33RD ANNUAL
PRIVACY AND TECHNOLOGY
LAW INSTITUTE

8 CLE Hours, Including
1 Ethics Hour | 1 Professionalism Hour

Sponsored By: Institute of Continuing Legal Education
Who are we?

SOLACE is a program of the State Bar of Georgia designed to assist those in the legal community who have experienced some significant, potentially life-changing event in their lives. SOLACE is voluntary, simple and straightforward. SOLACE does not solicit monetary contributions but accepts assistance or donations in kind.

How does SOLACE work?

If you or someone in the legal community is in need of help, simply email SOLACE@gabar.org. Those emails are then reviewed by the SOLACE Committee. If the need fits within the parameters of the program, an email with the pertinent information is sent to members of the State Bar.

What needs are addressed?

Needs addressed by the SOLACE program can range from unique medical conditions requiring specialized referrals to a fire loss requiring help with clothing, food or housing. Some other examples of assistance include gift cards, food, meals, a rare blood type donation, assistance with transportation in a medical crisis or building a wheelchair ramp at a residence.

Contact SOLACE@gabar.org for help.
The purpose of the SOLACE program is to allow the legal community to provide help in meaningful and compassionate ways to judges, lawyers, court personnel, paralegals, legal secretaries and their families who experience loss of life or other catastrophic illness, sickness or injury.

**TESTIMONIALS**

In each of the Georgia SOLACE requests made to date, Bar members have graciously stepped up and used their resources to help find solutions for those in need.

A solo practitioner’s quadriplegic wife needed rehabilitation, and members of the Bar helped navigate discussions with their insurance company to obtain the rehabilitation she required.

A Louisiana lawyer was in need of a CPAP machine, but didn’t have insurance or the means to purchase one. Multiple members offered to help.

A Bar member was dealing with a serious illness and in the midst of brain surgery, her mortgage company scheduled a foreclosure on her home. Several members of the Bar were able to negotiate with the mortgage company and avoided the pending foreclosure.

Working with the South Carolina Bar, a former paralegal’s son was flown from Cyprus to Atlanta (and then to South Carolina) for cancer treatment. Members of the Georgia and South Carolina bars worked together to get Gabriel and his family home from their long-term mission work.

Contact SOLACE@gabar.org for help.
Dear ICLE Seminar Attendee,

Thank you for attending this seminar. We are grateful to the Chairperson(s) for organizing this program. Also, we would like to thank the volunteer speakers. Without the untiring dedication and efforts of the Chairperson(s) and speakers, this seminar would not have been possible. Their names are listed on the AGENDA page(s) of this book, and their contributions to the success of this seminar are immeasurable.

We would be remiss if we did not extend a special thanks to each of you who are attending this seminar and for whom the program was planned. All of us at ICLE hope your attendance will be beneficial, as well as enjoyable. We think that these program materials will provide a great initial resource and reference for you.

If you discover any substantial errors within this volume, please do not hesitate to inform us. Should you have a different legal interpretation/opinion from the speaker’s, the appropriate way to address this is by contacting him/her directly.

Your comments and suggestions are always welcome.

Sincerely,

Your ICLE Staff

Jeffrey R. Davis
Executive Director, State Bar of Georgia

Tangela S. King
Director, ICLE

Rebecca A. Hall
Associate Director, ICLE
AGENDA

Presiding:
Jennifer Ruth Liotta, Program Chair; Vice Chair, Privacy and Technology Law Section of the State Bar of Georgia; Managing Attorney, Tanager Legal, LLC, Atlanta, GA

7:15 REGISTRATION AND CONTINENTAL BREAKFAST
(All attendees must check in upon arrival. A jacket or sweater is recommended.)

7:55 WELCOME AND PROGRAM OVERVIEW

8:00 MORNING KEYNOTE: PRIVACY IN A POST-GDPR WORLD

9:00 BREAKOUT SESSIONS

PRIVACY TRACK
PRACTICAL CONTRACTING: PRIVACY AND SECURITY CLAUSES
Jason A. Bernstein, Partner, Barnes & Thornburg LLP, Atlanta, GA

TECHNOLOGY TRACK
COMPLEX CUSTOMER ISSUES IN TECHNOLOGY CONTRACTING
Janine Anthony Bowen, Partner, BakerHostetler LLP, Atlanta, GA

10:00 BREAK

10:15 BREAKOUT SESSIONS

PRIVACY TRACK
GDPR IMPLEMENTATION PANEL
Moderator: Christina D. McCoy, Associate Counsel, Calero Software LLC, Atlanta, GA
Panelists:
Amanda M. Witt, Partner, Kilpatrick Townsend & Stockton LLP, Atlanta, GA
Aruna Sharma, Associate General Counsel, Turner Broadcasting System, Inc., Atlanta, GA
Toby Spry, Principal - Cybersecurity & Privacy, Price Waterhouse Coopers, Atlanta, GA

TECHNOLOGY TRACK
BLOCKCHAIN: IMPLEMENTATION RISKS
Paul H. Arne, Partner, Morris Manning & Martin LLP, Atlanta, GA

11:15 LUNCH: PROFESSIONALISM—AI & THE LAW
Al Leach, Alston & Bird, Atlanta, GA
Will Bracker, Corporate Counsel, Privacy, Cox Communications, Atlanta, GA

12:15 BREAK
12:30  BREAKOUT SESSIONS

PRIVACY TRACK
BIG DATA MONETIZATION
Moderator: Theodore F. “Ted” Claypoole, Partner, Womble Bond Dickinson (US) LLP, Atlanta, GA
Panelists:
Forrest Pace, AIG, Atlanta, GA
Jeff Reynolds, Daugherty Business Solutions, Atlanta, GA
JP James, Octane Systems, Atlanta, GA

TECHNOLOGY TRACK
CYBER PANEL
Moderator: Jennifer Ruth Liotta, Program Chair; Vice Chair, Privacy and Technology Law Section of the State Bar of Georgia; Managing Attorney, Tanager Legal, LLC, Atlanta, GA
Panelists:
Chad Hunt, Supervisory Special Agent, Federal Bureau of Investigation, Atlanta, GA
Johnny Lee, Principal - Forensic Advisory Services, Grant Thornton LLP, Atlanta, GA

1:30  BREAKOUT SESSIONS

PRIVACY TRACK
CCPA AND BEYOND—WHERE IS PRIVACY HEADED
Jonathan A. “Jon” Neiditz, Partner, Kilpatrick Townsend & Stockton LLP, Atlanta, GA

TECHNOLOGY TRACK
ADTECH
Jodi Daniels, Founder, Red Clover Advisors, Atlanta, GA

2:30  BREAK

2:45  AFTERNOON KEYNOTE: ROYALTY AND PAYMENT TERMS, AUDITS AND ALTERNATIVE STRUCTURES
Peter J. Kinsella, Partner, Perkins Coie LLP, Denver, CO

3:45  BREAKOUT SESSIONS

PRIVACY TRACK
ETHICS
David C. Hricik, Professor of Law, Mercer University School of Law, Macon, GA

TECHNOLOGY TRACK
BIG DATA AND PROTECTED DATA: LEGAL ETHICS ISSUES AROUND THE HANDLING BY AND FOR CLIENTS
Ann Moceyunas, General Counsel, Surgical Information Systems, LLC, Alpharetta, GA

4:45  ADJOURN
## TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Page</th>
<th>Chapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>v</td>
<td>Foreword .................................................................</td>
</tr>
<tr>
<td>vi</td>
<td>Agenda ...........................................................................</td>
</tr>
<tr>
<td>1</td>
<td>Morning Keynote: Privacy In A Post-GDPR World......................... Daniel J. Solove</td>
</tr>
<tr>
<td>2</td>
<td>Practical Contracting: Privacy And Security Clauses .................... Jason A. Bernstein</td>
</tr>
<tr>
<td>3</td>
<td>Complex Customer Issues In Technology Contracting ..................... Janine Anthony Bowen</td>
</tr>
<tr>
<td>4</td>
<td>GDPR Implementation Panel ................................................ 1-11 Moderator: Christina D. McCoy</td>
</tr>
<tr>
<td></td>
<td>Panelists: Amanda M. Witt</td>
</tr>
<tr>
<td></td>
<td>Panelists: Aruna Sharma</td>
</tr>
<tr>
<td></td>
<td>Panelists: Toby Spry</td>
</tr>
<tr>
<td>5</td>
<td>Blockchain: Implementation Risks ............................................. Paul H. Arne</td>
</tr>
<tr>
<td>6</td>
<td>Professionalism—AI &amp; The Law ................................................ Al Leach</td>
</tr>
<tr>
<td></td>
<td>Will Bracker</td>
</tr>
<tr>
<td>7</td>
<td>Big Data Monetization ......................................................... Moderator: Theodore F. “Ted” Claypoole</td>
</tr>
<tr>
<td></td>
<td>Panelists: Forrest Pace</td>
</tr>
<tr>
<td></td>
<td>Panelists: Jeff Reynolds</td>
</tr>
<tr>
<td></td>
<td>Panelists: JP James</td>
</tr>
<tr>
<td>8</td>
<td>Cyber Panel .................................................................... Moderator: Jennifer Ruth Liotta</td>
</tr>
<tr>
<td></td>
<td>Panelists: Chad Hunt</td>
</tr>
<tr>
<td></td>
<td>Panelists: Johnny Lee</td>
</tr>
</tbody>
</table>
CCPA And Beyond—Where Is Privacy Headed................................................................. 1-86 9

Jonathan A. “Jon” Neiditz

Adtech............................................................................................................................................................. 1-29 10

Jodi Daniels

Afternoon Keynote: Royalty And Payment Terms, Audits And Alternative Structures.................................................................................................................... 1-30 11

Peter J. Kinsella

Ethics................................................................................................................................................................ 1-20 12

David C. Hricik

Big Data And Protected Data: Legal Ethics Issues Around The Handling By And For Clients.................................................................................................................... 1-37 13

Ann Moceyunas

Appendix:
ICLE Board ............................................................................................................................................................ 1
Georgia Mandatory ICLE Sheet .................................................................................................................... 2
Morning Keynote: Privacy In A Post-GDPR World

Presented By:

Daniel J. Solove
George Washington University Law School
Washington, D.C.
Why I Love the GDPR: 10 Reasons

Daniel Solove, Professor, George Washington University Law School

In the United States, a common refrain about GDPR is that it is unreasonable, unworkable, an insane piece of legislation that doesn’t understand how the Internet works, and a dinosaur romping around in the Digital Age.

But the GDPR isn’t designed to be followed as precisely as one would build a rocket ship. It’s an aspirational law. Although perfect compliance isn’t likely, the practical goal of the GDPR is for organizations to try hard, to get as much of the way there as possible.

The GDPR is the most profound privacy law of our generation. Of course, it’s not perfect, but it has more packed into it than any other privacy law I’ve seen. The GDPR is quite majestic in its scope and ambition. Rather than shy away from tough issues, rather than tiptoe cautiously, the GDPR tackles nearly everything.

Here are 10 reasons why I love the GDPR:

(1) Omnibus and Comprehensive

Unlike the law in the US, which is sectoral (each law focuses on specific economic sectors), the GDPR is omnibus – it sets a baseline of privacy protections for all personal data.

This baseline is important. In the US, protection depends upon not just the type of data but the entities that hold it. For example, HIPAA doesn’t protect all health data, only health data created or maintained by specific types of entities. Health data people share with a health app, for example, might not be protected at all by HIPAA. This is quite confusing to individuals. In the EU, the baseline protections ensure that nothing falls through the cracks.

The GDPR is quite comprehensive in the scope of what it protects as well as comprehensive in the types of protections it offers. In contrast, with many other privacy laws, there are some glaring omissions. Many US privacy laws, for example, fail to address vendor management or have provisions for governance and accountability. These laws are quite incomplete; they are only a partial recipe for protecting privacy.

Additionally, there are many privacy laws with exceptions that open up gaping holes in the law. With the GDPR, I can’t find a lot that is missing or exceptions that swallow the rule.

(2) Requires Organizations to Know Their Data

To comply with GDPR, organizations must know their data. There’s no way to follow GDPR without knowing about the data that one collects and processes.
Knowing one’s data is essential to protecting it. An organization must understand the type of data it has, why it has it, how it is used, and with whom it is shared, among other things. This is the first step to getting a handle on data protection.

(3) Governance and Accountability

The GDPR has extensive requirements for governance and accountability – requiring data protection officers (DPOs), policies and procedures, data protection impact assessments (DPIAs), workforce training, and other key components of an effective privacy program. These requirements are essential for a law to be effectively followed by organizations.

Laws that lack governance requirements are often ignored. Someone at an organization must own the task of compliance; without any owner, compliance will be adrift. There must be policies and procedures, and there must also be training. The best policies are meaningless if nobody knows about them or how to follow them.

(4) Broad Definition of Personal Data

The GDPR defines personal data quite broadly. According to the GDPR Article 4, personal data is “any information relating to an identified or identifiable natural person.”

Many privacy laws cover identified people but fail to adequately cover identifiable people. In contrast, the GDPR has a broad definition of identifiable: “[A]n identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.”

It is alarming how much data that we think isn’t linkable to a person can actually be linked to that person. The GDPR understands this; many other privacy laws don’t.

(5) Rights and Redress for Individuals

The GDPR provides quite a number of important rights to individuals:

- Right to be informed about the person data organizations have about them
- Right to access personal data
- Right to rectification – correct errors in personal data or add to incomplete records
- Right to erasure (aka “the right to be forgotten”)
- Right to restriction on processing of personal data
- Right to data portability
- Right to object to the processing of personal data

Few other privacy laws have all of these rights. Many laws omit rights such as erasure and data portability. Other laws provide a rather anemic right to rectification as well as not much ability to restrict processing of personal data.
The GDPR does more than just provide for rights, but it has provisions to ensure that the rights are meaningful. For example, the GDPR does more than just require a privacy notice; it specifies the types of things that organizations must disclose to people.

Additionally, individuals whose rights are violated under the GDPR have redress. There must be effective judicial remedies. In contrast, there is no such guarantee in US law. Some laws lack a private right of action. People can complain to regulators, but without any economic incentive to raise complaints, many people will just suffer in silence.

In instances where people can bring lawsuits, many US courts dismiss cases based on privacy or security violations based on a view that individuals haven’t been harmed. These courts have a very narrow view of harm and often require plaintiffs to establish physical, financial, or reputational harm. Privacy and security harms are often of a different nature. Many privacy harms are based on emotional distress, thwarted expectations, or betrayal of trust. Many security harms are based on increased risk rather than actual materialized injury. US courts struggle to recognize these types of harms. The U.S. Supreme Court in Clapper v. Amnesty International and Spokeo, Inc. v. Robins further muddied the waters.

The GDPR avoids falling into this muddy morass by declaring that individuals must have a right to receive compensation when they have “suffered material or non-material damage.” This ensures that important provisions of the GDPR aren’t ignored or deliberately violated because plaintiffs will have a tough time proving harm.

(6) Meaningful Consent

Consent is one of the lawful bases by which organizations can process personal data. The GDPR requires affirmative consent, which must be freely given, specific, informed, and unambiguous. Consent can’t be assumed from inaction. Pre-ticked boxes aren’t sufficient to constitute consent.

This approach is an improvement over the opt-out approach, common in US privacy laws that infer consent from inaction. As most people don’t read privacy policies, inaction doesn’t really mean consent.

The GDPR also imposes a presumption that consent isn’t freely given if there is “a clear imbalance between the data subject and the controller.” This provision prevents the use of the fiction that highly-coerced “consent” is valid consent.

Another good thing that the GDPR does is to not allow organizations to require people’s consent to certain uses of data order to obtain a service unless necessary for the service. HIPAA has such a requirement too – an authorization to use protected health information for marketing can’t be required in order to obtain medical treatment.

The GDPR also has a purpose specification requirement: If a data subject consents to the use of personal data for one purpose, then the data can’t be processed for a different unrelated
purpose without obtaining a new consent. In contrast, many other privacy laws omit purpose specification, one of the fundamental Fair Information Practice Principles (FIPPs).

(7) Follows the Data

The GDPR follows the data. This is a very important component of a privacy law. Organizations often transfer personal data to other entities.

Many privacy laws focus just on the contracts vendors make with these entities, making sure that the contracts include some provision assuring compliance with the law. But this isn’t good enough. Many organizations just sign these contracts but don’t comply. Their only penalties for failing to comply are contractual — the regulators often lack the ability to enforce against these organizations.

The GDPR covers the entities that are the controllers of the data (“data controllers”) and also the entities that receive data from controllers to perform functions for the controllers (“data processors”). Enforcement thus follows the data.

When a law fails to follow the data, the data readily falls outside the enforcement ambit of the regulator. These are leaky laws that expose data to a lot of risk in today’s world where data is often outsourced to third party vendors for various functions.

(8) Vendor Management and Data Transfer

The GDPR imposes significant obligations on controllers that contract with processors.

Many controllers have numerous vendor agreements with various companies that perform functions involving personal data. The GDPR requires that controllers perform due diligence in selecting vendors, that controllers have certain provisions in their contracts with vendors, and that controllers monitor vendors for compliance

Vendors – or “processors” under the terminology of the GDPR – also have obligations under the GDPR and can face penalties for failure to comply.

Under the GDPR Article 28, when selecting processors, controllers must make sure that the processors provide “sufficient guarantees” of their ability to comply with the GDPR.

There must be a contract between the controller and the processor. The GDPR sets forth a series of requirements for these contracts. This is an important thing to include, as many vendor agreements lack all of the essential elements.

The GDPR also restricts the transfer of personal data to other countries. There must be an “adequate level of protection” in order for data to be transferred to these countries. The US has no such requirement.
These provisions of the GDPR ensure that data doesn’t start losing protection as it flows from one organization to another and from one country to another.

(9) Attention-Grabbing Penalties

The GDPR has penalties that make upper management pay attention. Fines for the most serious violations can be as high as either 20 million euros or 4% of total annual worldwide turnover, whichever is higher. Less serious violations can involve fines as high as either 10 million euros or 2% of total annual worldwide turnover, whichever is higher. Overall, under Article 83, administrative fines are to be “effective, proportionate and dissuasive.”

These fines are very hefty. For many organizations, upper management will not devote significant attention or resources unless there’s a significant risk. The GDPR penalties create such a risk, and they drive greater resources. Good privacy protection depends upon upper management caring and devoting the necessary resources.

Far too many privacy laws lack strong enough penalties to make organizations take compliance seriously. The penalties must ensure that organizations are never be better off for having violated a privacy law.

(10) Data Protection by Design and Default

Unlike many privacy laws, the GDPR directly addresses design. As Professor Woodrow Hartzog demonstrates persuasively in his book, Privacy’s Blueprint, technological design plays an essential role in privacy protection, and laws often fail because they don’t address design.

Article 25 of the GDPR mandates that data protection be built in starting at the beginning of the design process. This means that data protection cannot be an afterthought and must be documented.

By default, only personal data necessary for each specific purpose of the processing should be processed. Default settings should be set so that personal data isn’t accessible to an indefinite number of people.

For a long time, privacy has been a vague consideration for organizations. The result of this was that for many organizations, what it meant to protect “privacy” was just doing a handful of things, often easy things. There was no recipe for privacy, so one just threw in some ingredients and claimed it was done. But, in fact, it was only partially baked.

The GDPR supplies a recipe, one that is clear enough to get upper management to avoid leaving out key ingredients.

My main hope is that the EU regulators don’t snatch defeat from the jaws of victory by failing to effectively enforce the GDPR. Enforcement should be strong without being crippling, consistent and not arbitrary, rewarding of reasonable efforts and good faith, practical and strategic, and sufficiently frequent so as not to appear as a remote risk.
The GDPR is a great achievement, a major step forward for privacy protection. Time will ultimately supply the full verdict on the GDPR, but at this time, the GDPR sets the standard.

With so much worry and stress over GDPR, I think it is important to take a moment and admire it as a grand legislative achievement. It is an immensely intricate law, and it addresses an incredibly challenging set of problems. So, let’s pause in the freak out about May 25 and offer a toast to the GDPR – it deserves our praise and admiration.
Carpenter v. United States, Cell Phone Location Records, and the Third Party Doctrine

Daniel Solove, Professor, George Washington University Law School

The U.S. Supreme Court recently issued a decision in Carpenter v. United States, an important Fourth Amendment case that was eagerly awaited by many. The decision was widely cheered as a breakthrough in Fourth Amendment jurisprudence — hailed as a “landmark privacy case” and a “major victory for digital privacy.” In the NY Times, Adam Liptak referred to Carpenter as a “major statement on privacy in the digital age.”

Although I agree with the outcome of the decision, I ultimately find it to be disappointing. True, the Supreme Court finally took a step forward to bring the Fourth Amendment more in line with the digital age. But this was only a step in the year 2018, when the Court should have walked more than a mile.

Despite the fact that the various opinions in Carpenter total 119 pages, Carpenter only resolves a narrow issue and leaves many open questions. When something is the length of a Tolstoy novel, the plot should advance quite a lot more. The basic holding of the case is that the Fourth Amendment applies when the government “accesses historical cell phone records that provide a comprehensive chronicle of the user’s past movements.” But a lot more was at stake in the case. This was the prime opportunity of the Court to overrule the Third Party Doctrine, under which the Court has held that that there is no reasonable expectation of privacy for information known or exposed to third parties. The Third Party Doctrine was forged in the 1970s in cases involving bank and phone records. In United States v. Miller, 425 U.S. 435 (1976), the Court held that there is no reasonable expectation of privacy in financial records maintained by one’s bank because “the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.” In Smith v. Maryland, 442 U.S. 735 (1979), the Court concluded that there was no reasonable expectation of privacy when the government obtained a list of phone numbers a person dialled from the phone company because people “know that they must convey numerical information to the phone company” and cannot “harbour any general expectation that the numbers they dial will remain secret.”

As I argued in an earlier post about Carpenter, the Third Party Doctrine is deeply flawed and eviscerates Fourth Amendment protection in today’s digital age where so much of our information is in the hands of third parties. Carpenter would have been the ideal case to get rid of the Third Party Doctrine. Instead, the Supreme Court did what it has often done in recent years — tiptoe weakly like a mouse, nibbling around the edges of issues rather than directly resolving them. Rather than overrule Smith and Miller, the Carpenter Court just stated that these cases don’t apply to cell-site location records: “We decline to extend Smith and Miller to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user’s claim to Fourth Amendment protection.” This is a partial victory, as the Third Party Doctrine finally has a stopping point, but there are an endless series of situations involving the Third Party Doctrine, and the Court has provided scant guidance about when the Third Party Doctrine will apply.
The majority opinion goes out of its way to emphasize its narrowness:

Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or “tower dumps” (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of Smith and Miller or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security. As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not “embarrass the future.”

But in its fear of embarrassing the future, the Court embarrasses the present. The Court treats these issues as if they were cutting-edge technological issues. In fact, they are rather old technological issues. A larger problem with the decision is that it fails to provide much guidance about when the Third Party Doctrine would apply in other contexts. What test, if any, can be derived from the decision as to when the Third Party Doctrine doesn’t apply? Perhaps a statement toward the end of the decision will help: “In light of the deeply revealing nature of CSLI, [cell-site location information] its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.” Thus, the test seems to be one of extensiveness of the information and the difficulty of avoiding its collection. But how extensive? What if the information is extensive but collection is more avoidable?

So while I am pleased that the majority opinion finally indicated a limit to the Third Party Doctrine, this opinion is just a baby step in the right direction that leaves far too many unanswered questions. Such a cautious approach might have been warranted 20 years ago — or even 10 years ago — but certainly not now.

The dissents are all over the place. Several focus on property, with Justice Thomas stating: “The organizing constitutional idea of the founding era, by contrast, was property.” Justice Gorsuch (writing in dissent, though it should probably be a concurring opinion) wants to do away with Katz as well as the Third Party Doctrine and replace it with something else — a test that is property-based yet understands “property” in a broader manner:

It seems to me entirely possible a person’s cell-site data could qualify as his papers or effects under existing law. Yes, the telephone carrier holds the information. But 47 U. S. C. §222 designates a customer’s cell-site location information as “customer proprietary network information” (CPNI), §222(h)(1)(A), and gives customers certain rights to control use of and access to CPNI about themselves.

I don’t think property is the right thing to focus on. The Fourth Amendment limits the government to reasonable searches and provides judicial oversight not to vindicate property interests, but to regulate government power. The Framers were most concerned with general
warrants that authorized dragnet-like searches. With government searches, they were worried about excessive government power to pry into their activities. The fact that the Fourth Amendment mentions physical things (“persons, houses, papers, and effects”) is because there weren’t digital records at the time. The list of “persons, houses, papers, and effects” is meant to be a broad inclusive list, not a way to narrow the scope of the Fourth Amendment. The key part of the Fourth Amendment is its prohibition on “unreasonable” searches and seizures. The Fourth Amendment uses reasonableness as its focus, a concept that is flexible and widely-encompassing.

In an essay I wrote a number of years ago, Fourth Amendment Pragmatism, 51 Boston College Law Review 1511 (2010), I argued:

We should sidestep the contentious debate about expectations of privacy — or about any other specific value as a trigger for Fourth Amendment protection. Instead, whenever a particular government information gathering activity creates problems of reasonable significance, the Fourth Amendment should require regulation and oversight. These problems not only involve invasion of privacy, but also chilling of free speech, free association, freedom of belief, and consumption of ideas. They can involve inadequately constrained government power, lack of accountability of law enforcement officials, and excessive police discretion, among other things. The Fourth Amendment should provide coverage whenever any of these problems might occur.

The Third Party Doctrine has plagued Fourth Amendment jurisprudence for roughly 40 years. The Supreme Court should have overruled the Third Party Doctrine or at least carved out a greater chunk of it. Carpenter leaves open the door for more curtailment of the Third Party Doctrine in the future, but for now, it has left Fourth Amendment law needlessly unresolved and uncertain.
For the first half of 2018, all eyes were focused eastward on the EU with the start of GDPR enforcement this May. Now, all eyes are shifting westward based on a bold new law passed by California. By January 1, 2020, companies around the world will have to comply with additional regulations related to the processing of personal data of California residents. Pursuant to the California Consumer Privacy Act of 2018, companies must observe restrictions on data monetization business models, accommodate rights to access, deletion, and porting of personal data, update their privacy policies and brace for additional penalties and statutory damages. The California Legislature adopted and the Governor signed the bill on June 28, 2018 after an unusually rushed process in exchange for the proposed initiative measure No. 17-0039 regarding the Consumer Right to Privacy Act of 2018 (the “Initiative”) being withdrawn from the ballot the same day, the deadline for such withdrawals prior to the November 6, 2018 election.

Below is an interview with Lothar Determann, a leading expert on California privacy law. He has a treatise on the topic: California Privacy Law (3rd Edition, IAPP 2018).

In addition to being a partner at Baker & McKenzie, Lothar has taught data privacy law at many schools including Freie Universität Berlin, UC Berkeley School of Law, and Hastings College of the Law, Stanford Law School, and University of San Francisco School of Law. He has written more than 100 articles and 5 books, including a treatise about California Privacy Law.

This October 3, Lothar will be leading a California Privacy Law Workshop at my event, the Privacy+Security Forum.

SOLOVE: In what ways is this law significant and innovative?

DETERMANN: With this law, California responds to growing public concerns regarding trading of personal data and data security breaches. The Internet as we know it today – with a large ecosystem of charge-free services, funded through behavioural advertising and data commercialization – was born and raised in California. Perhaps it will die here too.

Free bicycle maps, mobile navigation services, social networks and much more — all innovative online services that could never have scaled to critical mass if companies were forced to rely on subscription fees for and after the initial launch. Other established pay services, such as news and email were quickly replaced by charge-free offerings. Let’s face it, consumers like free stuff and have never actually cared much about privacy in the past. See Lothar Determann, Social Media Privacy: a Dozen Myths and Facts, 7 Stanford Technology Law Review (2012). Based on user statistics and company earnings reports, I do not believe this has changed today – the new law hardly came from “the people.”
Perhaps the most significant and innovative component of the Act is its anti-discrimination provisions. Few, if any, U.S. privacy laws – or any other U.S. law for that matter – dictate how companies may calculate prices or allocate costs. The new law will prohibit companies from charging California residents for the costs of data access, deletion and mobility requests, or discriminate against consumers who make such requests or opt-out of data trading. This may effectively doom charge-free services, as companies may no longer be able to rely on data monetization revenue to scale their business, *e.g.*, from behavioural advertising on news sites, retargeting for online stores, or mobility data from apps.

Significant also is the breadth of the statute: Companies in all industry sectors, anywhere in the world, are required to comply and with respect to any categories of persona data. This feature of the law, though, is not particularly innovative, as it largely catches up with European data protection regulation, which is also extremely broad in scope and definitions.

Also significant are additional statutory damages for data security breaches. For more details, see Lothar Determann, *Be Wary of Liability for Statutory Damages under California Consumer Privacy Act*, Bloomberg BNA Privacy Law Watch (July 09, 2018). These will have a huge impact on companies that find themselves victims of a cyber-attack or data theft and that under this new law may now face class action lawsuits containing claims for statutory damages of up to $750 per consumer – even if no consumer suffered any actual harm. This concept is not entirely new. California included similar provisions in a data security law pertaining specifically to automated license plate scanners back in 2016.

Innovative, but of significance only to a limited subset of companies, are new thresholds exempting companies with lower revenues and who do not trade user data. Few other, if any, privacy laws exempt smaller companies in this manner, given that consumer privacy interests can be harmed equally by small and large companies alike. Still, the new law also contains broad regulatory restrictions, beyond what is necessary to protect individual privacy so it seems appropriate to exempt smaller companies and in fact the thresholds in the new law may not too low.

Finally, new rules pertaining to dual public / private enforcement are noteworthy: Plaintiffs’ attorneys will have to notify companies of violations first and then offer the case to the California Attorney General, who can either prosecute the case, veto private litigation, or let the private litigation proceed. Additionally, the California Attorney General is financially incentivized to enforce the new law through the establishment of a “Consumer Privacy Fund” which will offset costs incurred by State Courts and the Attorney General in the course of enforcing the law, financed by 20% of all penalties that the Attorney General collects. The new system seems intended to curb the worst consequences of enforcement by class action lawsuits. At the same time, it also provides for private rights of action, statutory damages and penalties, all of which are expected to maintain pressure on companies through an active plaintiff’s bar.

**SOLOVE: The law was very hastily drafted and has many areas that are confusing and unclear. What are some of the problems you have identified with the law?**
DETERMANN: The law has numerous inconsistent and unclear provisions, which will hopefully be addressed in corrections during the next few months.

For example, instead of referring to the established definition of “security breach” as codified in other parts of the California Civil Code, the new Section 1798.150(a)(1) refers to “unauthorized access and exfiltration, theft, or disclosure.” While the qualifier “unauthorized” makes sense to limit “access, exfiltration and disclosure” it does not in the case of “theft.” Also, grammatically, “unauthorized” could be read to qualify only “access and exfiltration.” If this were the case though, any disclosure, even if authorized, could trigger statutory damages. Also, the concept of precluding statutory damages if a breach is cured (as in California Civil Code §1798.150(b)(1)), while a good idea in principle, does not seem appropriate in the context of data security breaches, which can hardly ever be undone.

Perhaps an even bigger problem is that the new requirements are duplicative or inconsistent with disclosure and other requirements contained in the numerous existing California data privacy laws. The California Legislature should immediately revisit all existing California data privacy laws and abolish, or at a minimum, align and simplify sector and harm-specific privacy laws that require notice and consent in various forms and with nuanced requirements. In my practical guide and commentary, California Privacy Law (3rd edition, 2018), I cover hundreds of California and Federal privacy laws and my initial sense is that many of these can and should be repealed or simplified to align with the new provisions in the California Consumer Privacy Act.

SOLOVE: Are there any parts of the law that you find particularly praiseworthy or problematic?

DETERMANN: My personal view is that the broadened requirement for all companies and industries to provide notices regarding their data handling practices is appropriate and could simplify compliance if California repeals all the sector and situation-specific notice requirements, e.g., regarding website privacy policies (California Online Privacy Protection Act), direct marketing (Shine the Light Law), automated license plate scanners, etc.

I am not sure that data access and portability requirements are as crucial and worth the cost to society and consumers as a whole. If companies are forced to offer such rights, they should be able to charge those who make requests for the resulting costs. Companies should not be forced to abandon charge-free service offerings or raise prices for all customers to accommodate a subset population with special interests in data privacy or unrelated agendas. Most data access requests I have seen clients subjected to since GDPR came into effect were initiated by journalists, activists, IT contractors, disgruntled employees and consumers who had an entirely unrelated beef with the company, such as overdue bills being handed off to collection agencies or limitations on the use of gift cards across physical and online stores.

Besides the statutory damages and “anti-discrimination” regulations we already covered earlier in this interview, perhaps the most problematic provision is the right to data deletion. The “right to be forgotten” is a conceptually pathetic obsession of politicians, who should strive to be remembered. Most people are sufficiently protected against harmful speech by existing laws prohibiting defamation, copyright infringement and various other forms of illegal
communications. Granting broad deletion rights creates a slippery slope to “data minimization” as a principle.

The European goal of “data minimization” is hopelessly outdated – from the 1970s – irrespective of it being regurgitated in the GDPR. We need more – not less – information to make sound policy decisions, train artificial intelligence, enable autonomous cars to recognize people, improve medicine, etc. Where abusive data handling practices cause actual harm, governments should pass laws to address such harm and prohibit abusive practices. But, it is far too simplistic to prohibit all processing of personal data as a default position – as the GDPR does – or grant broad deletion rights – as the GDPR and now also the California Consumer Privacy Act both do.

The data genie is already out of the bottle, we cannot put it back in. If we are worried about bad things that companies or governments might do with personal data, then we need to tackle such bad things whatever they may be – undesirable differentiation in insurance tariffs, hiring practices, service offerings, etc. Data processing and trading as such is neutral and can have positive effects for data subjects, such as better planning, product development, anti-discrimination efforts, more relevant marketing, etc.

If we overly restrict data processing simply because it is in some way related to these bad practices, then we act like the drunk who searches for his key under a street lamp, even if he lost it somewhere else, because he thinks it is easier to search with light. If we attempt to prohibit personal data processing altogether as a default, we are tilting at windmills instead of tackling today’s real problems.

**SOLOVE: What advice would you give to companies regarding compliance with the law?**

**DETERMANN:** First of all, I would refer companies back to the point I made in our last interview (Beyond GDPR): Businesses need to assess holistically how they can align or combine compliance efforts to address the new California law with the same efforts they make to comply with EU GDPR and other countries’ laws.

Secondly, companies have to conduct a detailed assessment of whether and how they are affected. They should start now, because some provisions require potentially significant changes to business models and technical implementations.

Thirdly, companies should follow legislative developments closely. The California Legislature has a lot of clean-up to do, and there is also potential for federal pre-emption.

Last but not least, companies should consider whether they can and should treat Californians differently from people in other U.S. states and other countries going forward. Under the new law’s anti-discrimination provisions, companies have to treat all Californians the same. But, they are free to levy or increase charges only for Californians, set up California-only websites or stop doing business in California. Many options are theoretically available, although companies will of course need to bear in mind that California’s economy is now the 5th largest in the world, behind only the USA as a whole, China, Japan and Germany.
SOLOVE: What kind of impact do you think that this law will have?

DETERMANN: Companies face significant additional penalties, statutory damages, compliance costs, technical complexities and administrative burdens. Smaller companies will struggle. As a result of the law, we may see fewer start-ups founded and based in California, fewer innovative charge-free service offerings, higher prices for online services, and a greater number of nuisance requests and lawsuits.

Consumers will see more charges, even longer and more detailed privacy notices, including different versions for different jurisdictions, and perhaps different websites and interfaces to accommodate local compliance requirements and enable differentiated pricing.

Politicians may again now see a need to push for a federal privacy law that streamlines and simplifies the highly divergent state laws in this field – provided it were to pre-empt state privacy laws. If that happens, we may see an ossification of privacy laws, as federal law is more difficult to change, and U.S. privacy laws may follow the fate of EU data protection laws which took 23 years to update and in principle still look very much like laws from the 1970s.

SOLOVE: What do you think the reaction of the EU will be to this law?

DETERMANN: Different groups in Europe will have different reactions:

The European Commission should consider an adequacy finding for California based on this law. The new California Consumer Privacy Act protects directly only residents of California, but it furthers what is already a relatively strong level of privacy protections in California that meets or exceeds the de facto level in many European countries as well as other countries that have received adequacy findings, such as Argentina, Canada, Israel, New Zealand and Uruguay. But, it would take quite a political effort to conduct an honest comparative assessment, a concept that has been less popular at the EU level than the reflexive U.S. privacy-bashing more common in the EU Parliament. See Lothar Determann, Adequacy of data protection in the USA: myths and facts, International Data Privacy Law, 2016; doi: 10.1093/idpl/ipw011.

European companies, on the other hand, may to some extent welcome a levelling of the playing field: California laws tend to be enforced first and foremost against California and U.S.-based companies (even if they technically apply worldwide), which will disproportionately affect companies in Silicon Valley and elsewhere in the United States. This, in turn, may create opportunities for companies in Europe, which have been hampered by excessive data regulation for the last several decades, and even more so in Asia, where data privacy laws have been far less restrictive to date.

The German government may reconsider its recent initiative to create data ownership rights in furtherance of efficient data trading (see my paper ‘No one owns data’) given that Germany is proud of its particularly strict national laws and history. My home state Hessen passed the first-ever data protection law in 1970 and started the trend worldwide.
Practical Contracting: Privacy And Security Clauses

Presented By:

Jason A. Bernstein
Barnes & Thornburg LLP
Atlanta, GA
1. Why is data security and privacy in agreements important to think about?
   A. Risk management

2. Types of agreements where DSAP is often an issue
   A. Software license/SaaS
   B. Outsourcing
   C. Manufacturing
   D. Service level agreements
   E. Data processing
   F. Purchase T&C
   G. Mobile app EULA
   H. Website TOU/PP
   I. M&A
   J. Anything involving data

3. Contracting goals (vendor’s perspective)
   A. Protect data
   B. Impose appropriate obligations
   C. Close the deal quickly
   D. Maximize profitability
   E. Minimize risk
   F. Minimize the cost of the deal

4. Consequences of poor negotiation
   A. Profit killers
      i. Increased cost for implementing required infrastructure improvement (hardware, software, network)
      ii. Cost of obtaining new certifications, and annual re-certification cost
      iii. Training costs
      iv. If offshoring prohibited, the cost of on-shore personnel will be higher
      v. Increased workload to implement and maintain compliance
      vi. Increased reporting requirements
      vii. Increased annual audit work
      viii. Increased burden to ask customer for consents for contractors, moving data location, to offshore data
      ix. Cost of increased cyber insurance
   B. Longer time to close a deal and get revenue or product
   C. Increased liability exposure
   D. Increased obligations

5. Negotiation strategy
   A. Negotiation of DSAP issues is all about risk management

---

Data Security and Privacy in Agreements
Jason A. Bernstein
© Barnes & Thornburg LLP 2018 All Rights Reserved

\(^1\) Sample language (pro-customer): Service Provider will provide Customer with at least three (3) months written notice of any change to a hosting provider that is different than the hosting provider as of the Effective Date, including providing a written security audit of the new hosting provider by a reputable third party security specialist, which report shall identify any readily identifiable security vulnerabilities of the hosting provider and suggested remedies to address the vulnerabilities. Service Provider will provide Customer a reasonable opportunity to inspect the operations of the new hosting provider and if not acceptable to Customer, Customer shall have the right to terminate this Agreement upon notice to Service Provider. Any new hosting provider shall be subject to the terms and conditions of this Agreement.
Data Security and Privacy in Agreements

Jason A. Bernstein
© Barnes & Thornburg LLP 2018 All Rights Reserved

1. I-D-A-T-A

B. Assess whether the other side is monolithic and unyielding in DSAP, or willing to negotiate.

C. If no PI is involved, get early acknowledgement by customer so that onerous ISR can be avoided. Same with GDPR requirements.

D. Understand how data and privacy fit into the transaction

E. Vendor: avoid getting identifiable PI, especially during the trial/proof-of-concept phase of the relationship.

F. Scale liability cap to match exposure

G. Anticipate what could go wrong and what can change

6. Enforceability

A. Forming binding agreement

B. Signed or click-through?

Main provisions

1. Definitions

A. Vendor wants definitions narrow, customer wants them broad

B. Personal Information

   i. Does statutory definition apply (GLBA, HIPAA, FERPA, GDPR…)? GDPR is broader than the others. Have GDPR definition apply only to data which requires compliance with GDPR.

   ii. Separate PI and general confidential information. Vendor wants data breach response requirements to be just for PI, not all confidential information.

   iii. Vendor should limit definition of PI to nonpublic information because some information is publically available, e.g., name and address

C. Customer data

---

2 Sample language (pro-vendor—prohibition on Customer sending Service Provider PI): Customer shall not disclose or transmit Personal Information to Service Provider unless specifically agreed to by Service Provider in advance in writing, and Service Provider will not attempt to identify any person from any such Personal Information if so provided. In the event Customer inadvertently provides to Service Provider or uploads to the Platform any Personal Information (“Inadvertent Personal Information”), Customer shall immediately notify Service Provider in writing. Service Provider shall use commercially reasonable efforts to secure Inadvertent Personal Information according to its then-current information security policies, but Service Provider shall not be liable for any unauthorized access, loss, or use of Inadvertent Personal Information. Service Provider shall promptly delete all Inadvertent Personal Information it receives, and shall not process (as such term is defined under GDPR) and shall not process any Inadvertent Personal Information. In the event that Service Provider agrees to receive or access Customer’s “personal data” of European residents (as defined under GDPR), Customer is deemed to be the “Data Controller” for the purposes of GDPR compliance. Customer shall at all times during this Agreement comply with all applicable provisions of GDPR, including, but is not limited to, regarding collection of personal data, obtaining consent, providing required notice, securing collected personal data, allowing access by the individuals whose personal data is collected (and allowing for correction of inaccuracies), maintaining the confidentiality of collected personal data, and, using the collected personal data only for purposes stated in required notices.

3 Sample language (pro-vendor, for financial-type data): “Personal Information” means (i) “nonpublic personal information” as defined under the Gramm-Leach-Bliley Act (“GLBA”), or (ii) if and to the extent compliance under the European General Data Protection Regulation (“GDPR”) is required, “personal data” as defined under the GDPR, but only as to data of European residents collected in the European Economic Area (GLBA and GDPR as implemented and amended during this Agreement).

Data Security and Privacy in Agreements
Jason A. Bernstein
© Barnes & Thornburg LLP 2018 All Rights Reserved
D. Data breach/security incident
   i. “actual” vs “suspected”
E. Material: define since vendor doesn’t want to be in breach for a trivial failure/default
F. Confidential Information includes vendor’s security logs, audit information, assessments, etc.
G. Damages/Limitation of liability
   i. Exclusions to cap
   ii. Define direct damages for data breach
   iii. Supercap for data breach
   iv. Scale cap for data breach (increase cap based on the number of customer records or revenue that vendor gets)

Sample language (pro-customer—broad, covers data developed by Service Provider from inputted data):

“Customer Data” means the data: (i) gathered, transferred, or inputted by or on behalf of Customer, Authorized Users, or by Service Provider on the Customer’s behalf into the Software or otherwise for the purpose of using or facilitating Customer’s use of the Services, (ii) derived or generated from the data described in the preceding clause (i); (iii) resulting from the processing of data described in the preceding clause (i); or, (iv) derived or generated from Customer’s or Authorized Users’ access to or use of the Software or the Subscription Services.

Sample language 1: “Security Breach” means any unlawful, unauthorized or accidental access, review, viewing, use, loss, transfer, acquisition or disclosure of any unencrypted or unredacted Personal Information or protected elements thereof (or encrypted Personal Information or protected elements thereof along with the confidential process or decryption key) which compromises or may be reasonably expected to compromise the security, integrity or confidentiality of the Personal Information or which creates a risk of harm to a person. A Security Breach does not include any of the above activities involving encrypted Personal Information, so long as the encryption key for that data is not also accessed.

Sample language 2 (pro-customer, but balanced, HIPAA-data focused): “Data Breach” means (i) any actual unauthorized or accidental, access, acquisition, use, loss, or disclosure of any Customer Data which could reasonably be expected to compromise the integrity and confidential nature of such Customer Data or that would require breach notification to affected individuals under applicable state, federal or foreign Law, (ii) any actual breach of Service Provider’s (or its Subcontractors’) security or information systems or the systems of Customer under management by Service Provider that either (A) exposes any Customer Data to such unauthorized or accidental access or use or (B) cause harm, damage or negatively affect the function or performance of Customer Infrastructure, or (iii) with respect to Customer Data which also meets the definition of “protected health information” under HIPAA, a “breach of unsecured protected health information” as that term is defined under HIPAA.

Sample language: LIMITATION OF LIABILITY. EXCEPT FOR INSTANCES OF GROSS NEGLIGENCE OR INTENTIONAL MISCONDUCT, THIRD PARTY CLAIMS OF INFRINGEMENT, A BREACH OF DATA SECURITY, A BREACH OF CONFIDENTIALITY NOT INVOLVING CUSTOMER DATA, A PARTY’S INDEMNIFICATION OBLIGATIONS, OR CUSTOMER’S PAYMENT OBLIGATIONS, ...

See end of this doc.

Sample language: The Parties agree to an aggregate “Supercap” equal to twice the limitation of liability level set forth in Section ___ in the aggregate for direct damages related to any claims based on a Party’s obligations related to Data Breaches under Section __, the Business Associate Agreement, or compliance with applicable Laws.

Sample language: Limitation of Liability for Security Breach. The obligations of Service Provider and Customer as the Responsible Party to the other, respectively, under this Section ___ are subject to the following limitations (“Cap”): if the Security Breach occurs while there are less than 10,000 Payers registered to use the Platform, the maximum liability under this Section 13(a) is $3,000,000; if there are 10,000 - 30,000 Payers registered to use the Platform, the maximum liability is $6,000,000; and, if there are 30,000 or more Payers registered to use the Platform, the maximum liability is $10,000,000. This Section ___ sets forth the sole remedy of the Responsible Party in the case of a Security Breach related to or arising from the Services performed pursuant to this Agreement.

Data Security and Privacy in Agreements
Jason A. Bernstein
© Barnes & Thornburg LLP 2018 All Rights Reserved
v. Cap at insurance limits: customer wants this number to be regardless whether the carrier accepts coverage.

vi. Data breach liability trigger
   (1) If customer: any security incident at vendor’s end
   (2) If vendor: failure to comply with the requirements of the agreement (i.e., if vendor is hacked despite every defense effort [i.e., compliance with the ISR], vendor not liable, or liable only to capped limit); this create reasonable apportionment of risk

H. Indemnification
I. Limit to third party claims
   i. Vendor wants to limit to what is in its control, limit to the extent not caused by or the result of vendor’s negligence or omissions or acts, including data breach at vendor.
   ii. Include as part of “losses”: fines (HHS), penalties, assessments (PCI). Customer wants allegations covered, not just awards.
      (1) If you handle PCI info, become familiar with the credit card reporting requirements and how to do it. Very short time lines. You will need to send them the list of card numbers affected.
      (2) Idea: increase liability cap if vendor does not timely notify customer of a breach (resulting in customer’s increased costs, fines, etc.), fails to provide all info vendor knows at the time.

2. Data security measures and “information security requirements”
   A. Customer wants vendor to have written infosec policy, disaster recovery and business continuity plan

---

10 Sample language: Service Provider agrees to indemnify, defend and hold harmless (collectively referred to as “indemnify” or its derivatives) Customer and its affiliates and their respective employees, directors, officers and agents harmless against any liability, damages, losses, judgments, fines, penalties, assessments, and other expenses (including, but not limited to, reasonable attorney’s fees and litigation costs) (collectively, all of the foregoing referred to as “Losses”) arising out of or resulting from any third party claims made or proceedings brought against Customer to the extent such Losses arises in the execution or performance of this Agreement or from Service Provider’s negligence or willful misconduct, provided however, that such Losses are other than to the extent of any negligence of the part of Customer that would have reasonably been expected to have avoided such Losses.

11 Sample language: Inatech will use commercially reasonable efforts: (a) to preserve the security of the Personal Information; (b) to prevent unauthorized access to or unauthorized modification of any Personal Information or a Inatech system (including all associated interfaces, hardware and software); (c) to establish and maintain environmental, safety, facility and data security procedures and other safeguards designed to ensure against destruction, loss, alteration or theft of, or unauthorized access to, any Personal Information; and (d) to establish and maintain an appropriate disaster recovery plan designed to ensure Customer will be able to continue receiving the Services in the event of a disaster (but may be temporarily below normal performance levels). Such measures will include, at a minimum, using firewalls, password protection and virus protection software, and performing periodic, but in any event at least annual, internal security audits of Service Provider’s systems and Services and tests of such disaster recovery plan. Upon request, Service Provider will provide Customer with written reports summarizing the results of such audits and tests and will take appropriate measures designed to resolve issues thereby identified. If Inatech detects any unauthorized access Personal Information or any security breach involving the unauthorized release of Personal Information, or any other actual breach of security with respect to the Personal Information or any Inatech system, then Service Provider’s will promptly (upon verification and internal investigation, and taking into consideration any delay required by law enforcement) notify Customer. Service Provider’s will fully cooperate with Customer in investigating such breach.
B. Cite to standards or laws where there are existing security requirements for the type of data handled (NIST, FIPS, etc.)
   i. Standard/level of effort: Customer wants “best practices.” Vendor wants (a) reasonable for businesses similarly sized in similar area (can’t expect small company to have same cyber security procedures as large company) or (b) standard in the industry. Vendor to continually improve measures to meet new threats.

C. Does customer itself meet the requirements it puts on vendor?

D. Does vendor have to request approval to change data storage location, contractors, or to offshore data?

E. Vendor should try to require customer to be compliant with the info sec requirements required of vendor

3. Infosec requirements exhibit
   A. Security technology changes rapidly and customer has to keep its security measures dynamic.
   B. Can customer change at will? On mutual agreement?
   C. Can vendor object?
   D. Time and cost to implement? Vendor wants a reasonable time to implement required changes. Idea: Make vendor responsible if there’s a breach before the new changes are implemented, but after they’re agreed upon, to give vendor incentive to implement quickly.
   E. Vendor should negotiate longer time to comply, ability to reprice the services if cost increase
   F. Best practice vs standard in the industry vs commercially reasonable
   G. Comply with ISO, NIST or other standards
   H. How vendor can handle numerous DSAP audit questionnaires
      i. Provide template response and tell customer to ask any additional questions
   I. Customer wants vendor to comply with IRS, vendor can avoid if it can show it does not access any PI, including via screen share (Akkadian)
   J. Customer should not be monolithic or too stubborn on ISR requirements where the risk is low. E.g., where the only access to customer’s info is via screen sharing during support session, just require vendor to not copy, print, or screen scrape any screens with PI being shown.

---

12 Sample language: (pro-customer): You must exercise and maintain and ensure that your staff, affiliates and subcontractors exercise and maintain “Good Industry Practice” (defined as the exercise of that degree of skill, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced company engaged in the same type of undertaking under the same or similar circumstances seeking to meet its obligations to the fullest extent possible (for clarity, such standards may include, without limitation, NIST, ISO 27001, SOC 1 SSAE 18 Type II, SOC 2 and/or PCI DSS).

13 Sample language (pro-vendor): The parties agree that Service Provider shall have a reasonable period of time, but less than thirty (30) days after notice to Service Provider in writing, to implement any new requirements based on revisions to Customer’s Information Security Requirements. Customer shall promptly reimburse Service Provider for the reasonable cost of any requirements imposed by Customer after the Effective Date which necessitate Service Provider having to modify its existing software or hardware, systems, network, infrastructure or procedures, or having to purchase new software or hardware, beyond those measures which are commercially reasonable in Service Provider’s industry at the time of such notice.
4. Data ownership/usage rights
   A. Who owns what data?
      i. Data customer uploads vs data generated by vendor
      ii. Does vendor own data it generates based on customer data?
   B. Can vendor use and disclose deidentified customer data?
   C. Can vendor aggregate customer’s data with other customer’s data and use for any purpose? Vendor may want to combine data from customers and sell back to customers (only) as benchmark and comparison data of others in customer’s industry.

5. Cross-border data movement (transfer, access, storage)
   A. If data of EU residents collected in the EU is being shared outside of the EU, GDPR will apply.
   B. Customer should prohibit ex-US transfer or access if important to customer\textsuperscript{14}
   C. Vendor wants right to flow data ex-US, e.g., if vendor has service provider in another country, e.g., tech support
   D. Try to include evaluation criteria so that vendor can show that it’s data movement is within the criteria

6. Know what DSAP laws and standards bodies (e.g., PCI) must be comply with
   A. GDPR
   B. Will need data processing agreement. Vendor wants customer to warrant that all GDPR data was collected in compliance with GDPR.

7. Customer’s responsibilities
   A. Security is shared responsibility\textsuperscript{15}
   B. Install updates and patches promptly (Equifax)
   C. Responsible for unauthorized use of login ID due to its own negligence (Sony)

8. Data breach
   A. Reporting threshold: Must be an incident where customer’s data was accessible.
   B. Customer wants requirement to notify be after discovery AND verification
   C. Notification deadline\textsuperscript{16}
      i. What foreign, state, PCI deadlines apply. GDPR is 72 hours after the data controller becomes aware. If PCI data involved, customer wants vendor to use a PCI forensics investigator, and report within 24 hours (to avoid credit card company assessments)

\textsuperscript{14} Sample language (pro-customer): Service Provider shall store and process Customer Data only in the continental United States in the locations specified in the applicable Term Sheet. Service Provider shall not transfer Customer Data to any other locations, nor change the locations for storage and processing of such Customer Data, nor, for clarity, change the locations from which Customer Data is accessed, except as expressly permitted in the applicable Term Sheet, or otherwise with the express written consent of Customer, which Customer may withhold in its sole discretion.

\textsuperscript{15} Sample language (pro-vendor): Service Provider shall not be responsible for any damage, loss, data breach, or any other liability to the extent based on Customer’s failure to timely install Updates to the Software within thirty (30) days of the Update being made available for installation.

\textsuperscript{16} Sample language: If Service Provider become aware of any actual unauthorized access, acquisition or compromise of the confidentiality, integrity or availability of Customer Data or Customer’s network, Service Provider must (i) immediately (but in any event with 24 hours) notify Customer in writing (by email to ___), (ii) consult and cooperate with Customer’s investigations and notices reasonably elected by Customer, (iii) provide any information reasonably requested by Customer, and (iv) execute common-interest and similar agreements reasonably requested by Customer.
D. Cooperation

E. Each party should not liable if a breach is due to the other party.\textsuperscript{17}

F. Communication responsibilities
   i. Customer usually wants to control
   ii. Vendor wants right to disclose where legally required to or if law enforcement can be notified – FBI notification may be a good idea for vendor, even if not required because insurance coverage may require it.\textsuperscript{18}
   iii. Vendor wants to require customer to keep vendor’s name out of announcements unless approved by vendor (PR, admissions, etc.)

G. Vendor required to preserve all docs and data. They may be needed for litigation, insurance, etc.

9. IOT (internet of things)
   A. Data security requirements
   B. Unique password out of the box or forced change at login
   C. Consider the new Calif. IOT law (device must have reasonable security; must require password change on setup)
   D. Part manufacturer required to pay for costs of implementing security update if a vulnerability is found in the manufacturer’s parts (e.g., software vulnerability in wireless circuit board for door lock—board manufacturer should pay for the lock manufacturer (who builds the locks) to update locks already in the field. Costs can be high if no ability to remotely update the software. Vulnerability in software is not necessarily a data breach.
   E. Vendor wants right to disclose to law enforcement data collected by a device that may be evidence of a crime (e.g., geolocation)
   F. Does manufacturer get access to user data being sent by device back to the manufacturer?

10. Insurance
   A. Customer wants cyber insurance mandatory

\textsuperscript{17} Sample language: Service Provider will be liable for any Security Breach of Customer Data successfully uploaded to the Software where caused by the acts or omissions of Service Provider or its agents, hosting services or other contractors, except to the extent due to any acts, omissions or negligence of Customer, its agents, or contractors. Customer shall be liable for Security Breach of Customer Data where caused by the acts or omissions of Customer, its contractors (other than Service Provider, its agents or contractors), its then-current employees, former employees who were previously Authorized Users, and not due to any negligence of Service Provider or its agents, hosting services and other contractors (“Customer Security Breach”). Notwithstanding the previous sentence, former employees or contractors of Customer whose Authorized User credentials have been properly deactivated by Customer, but who subsequently cause a Security Breach through methods that do not include the use of their Authorized User credentials, does not constitute a Customer Security Breach.

\textsuperscript{18} Sample language: Service Provider reserves the right, in its sole discretion, to report criminal acts relating to the use and disclosure of Personal Information to applicable Government Authorities and shall notify Customer as soon as practicable that such reporting has occurred. With respect to instances in which Service Provider is considering notifying Government Authorities concerning civil, but not criminal, acts, Service Provider shall notify Customer in writing and consult with Customer prior to making any such notification. The parties shall immediately endeavor in good faith to reach agreement on the need, nature, and timing of such notification. If such agreement cannot be reached within seventy-two (72) hours after Service Provider has provided Customer with written notice, Service Provider shall have the right to inform Government Authorities [solely to the extent required by applicable law <— Note: There may not be a legal requirement but vendor may want to report to avoid fines, or to ensure insurance coverage].
B. Coverage limit should reflect the potential exposure
C. Scale coverage limit as amount of data increases

11. Audit rights
   A. Frequency. Annually unless there’s been a breach within the past 12 months requiring notification of affected individuals.
   B. How done:
      i. Questionnaire or on site or self-audit?
      ii. Provide SSAE 16-type reports?
      iii. Self-assessment
      iv. Re-certification
   C. Vendor’s info (reports, investigation material, logs, etc.) is confidential
   D. Level of intrusion permitted: Penetration test permitted?
   E. Vendor wants copy of all customer’s findings
   F. Materiality threshold for customer requiring remediation of any weaknesses found
   G. Pre-contract audit? Customer has vendor complete a security assessment questionnaire before signing and warrant that it is accurate and it is in compliance and will remain in compliance.

12. Return/destruction of PI/CI
   A. Vendor wants right to retain for legally required period (e.g., HIPAA 7 years)
   B. Not always practicable to delete all confidential information vendor has. PI may be embedded in vendor’s system, archives, reports, etc.\(^{19}\)
   C. Require that any CI/PI retained after termination be kept confidential forever.

13. Termination. Breach of the agreement leading to a data breach is not curable and vendor has the right to terminate.

OTHER AREAS

14. Data processing agreements
   A. Not all are the same; it’s not a uniform template
   B. Look at requirements vendor has vs customer

15. Equitable relief. Exclude from mandatory arbitration any claim for breach or threatened breach of confidentiality. Going to a judge for a TRO is much faster than going through arbitration.

16. M&A thoughts
   A. What will the buyer of your company inherit?
   B. Data security and privacy due diligence

17. Service level agreement
   A. Include performance credits
   B. 3 strikes\(^{50}\)

\(^{19}\) **Sample language** (use in addition to the usual return/delete language): Notwithstanding the foregoing, Service Provider may keep a copy of the Confidential Information to the extent such is required: (a) to comply with applicable law or regulation, or (b) pursuant to Service Provider’s standard electronic backup and archival procedures if (i) personnel whose functions are not primarily information technology in nature do not have access to such retained copies and (ii) personnel whose functions are primarily information technology in nature have access to such copies only as reasonably necessary for the performance of their information technology duties (e.g., for purposes of system recovery), provided, in each case, that such Confidential Information is retained in accordance with this Agreement.

Data Security and Privacy in Agreements
Jason A. Bernstein
© Barnes & Thornburg LLP 2018 All Rights Reserved
18. Conflate force majeure and DR/BP. A Force Majeure event may still be anticipatable (e.g., annual monsoons in India, tornados in Midwest US) and should not be grounds for suspension of vendor’s performance. Vendor should have a DR/BC plan to handle. FM event service suspension is only if DR plan doesn’t cover the FM event.\textsuperscript{21}
Sample Language

Direct Damages for Data Breach. Service Provider’s indemnification obligations in this Agreement related to Data Breach also includes Losses by Customer and its personnel, patients, customers, and end users, shall include, but are not limited to (all of the following of which are deemed direct damages):

A. generally, the costs of responding to and mitigating the damages caused by a data breach;
B. reasonable costs of investigation, namely, forensics or data security consultant fees for investigating the cause of the breach;
C. cost of data reconstruction (or migration);
D. reasonable costs of providing notice to affected individuals as required by applicable law;
E. reasonable costs of providing required notice to government agencies, state and/or federal regulators or credit bureaus as required by applicable law;
F. reasonable costs of complying with an investigation conducted by a government agency and/or state or federal regulator;
G. the cost of providing affected individuals with credit monitoring services and credit protection services (e.g., credit freeze services), credit fraud alert services, as required by applicable law, or, if none, for twelve (12) months;
H. fines and penalties assessed by government agencies, or state and/or federal regulators for the Security Breach due to Service Provider’s acts or omissions (to the extent that such fines and penalties are due to the Service Provider’s actions or inactions);
I. security audits or reviews of Service Provider’s systems reasonably requested by Customer;
J. the cost of recertification of Customer for any required certifications (such as, but not limited to, PCI, HIPAA, etc.);
K. Customer’s reasonable attorneys’ fees and costs relating to all of the foregoing, including, but not limited to, costs of litigation, legal data holds, public records requests and similar fees and costs;

ADDITIONAL ITEMS - FOR PAYMENT CARD BREACH INCIDENTS:

L. the costs of cancelling and reissuing replacement credit cards;
M. the costs of an investigation by a payment card industry forensic investigator;
N. the costs of PCI recertification;
O. the costs of fines, penalties, fees, and assessments imposed by the payment card brands/networks and/or payment card processor;
P. the costs of defending and settling litigation and regulatory agency actions, including, but not limited to, consumer claims and consumer class actions;
Q. the costs of a toll free hotline to answer questions about the Data Breach;

This list is likely more comprehensive than any vendor will tolerate, but is provided to illustrate what costs are potentially involved if there is a data breach.

(ALTERNATIVE-BROADER: providing identity theft monitoring and resolution services (including credit monitoring services))
R. the amount of the deductible or retention under Customer’s cyber insurance program or the costs of the deductible or retention under Service Provider’s cyber insurance program in which Customer is named as an additional insured;  
OPTIONAL ADDITIONAL ITEMS, USUALLY NOT REIMBURSABLE, BUT INCLUDED TO SHOW THE ENTIRE “COST” OF A BREACH:  
S. consulting/legal fees for developing improved data security policies, procedures and compliance;  
T. IT consultant fees for revising software to eliminate the hole, opening or vulnerability which was related to the Data Breach and improve software, network and hardware security;  
U. reasonable costs of repair or replacement of any computer hardware or software damaged as a result of the Data Breach;  
V. reasonable fees and costs associated with retaining crisis management, public relations, accounting, auditing, consulting, and similar professional services firm assistance attributable to the Data Breach;  
W. reasonable costs of providing customer hotline and other customer service support relating to any Data Breach; and,  
X. cost of cancelling and issuing replacement credit/debit cards.
Data Security and Privacy in Agreements

Jason A. Bernstein
Barnes & Thornburg LLP

October 19, 2018
Privacy & Technology Law Institute

Why is This Important?

Risk Management
Types of Agreements

- Software license/SaaS
- Outsourcing
- Manufacturing
- Service level agreements
- Data processing
- Purchase T&C
- Mobile app EULA
- Website TOU/PP
- M&A
- Anything involving data

Contracting Goals

- Protect data
- Impose appropriate obligations
- Close the deal quickly
- Maximize profitability
- Minimize risk
- Minimize the cost of the deal
Consequences of Poor Negotiation

• Profit killers
• Delay in receiving revenue or product
• Increased liability and risk exposure
• Increased obligations

Negotiation Strategy for DSAP

• Risk management
• Willingness of the other side to be flexible
• Know how PI fits into the transaction
• Find out if the other side had a public data breach recently
• Anticipate what can go wrong or change
### Handling Risk In Agreements

<table>
<thead>
<tr>
<th>I</th>
<th>Insure</th>
</tr>
</thead>
<tbody>
<tr>
<td>D</td>
<td>Diminish</td>
</tr>
<tr>
<td>A</td>
<td>Avoid</td>
</tr>
<tr>
<td>T</td>
<td>Transfer</td>
</tr>
<tr>
<td>A</td>
<td>Accept</td>
</tr>
</tbody>
</table>

### Enforceability

- Signed
- Click-through
Definitions

• Personal Information
• Customer Data
• Data Breach
• Material
• Confidential Information

Damages/Limitation of Liability

• Exclusions to cap
• Define direct damages for data breach
• Supercap for data breach
• Scaled cap
• Insurance cap
• Liability trigger
Indemnification

- Limit to third party claims
- Vendor wants to limit to what is in its control, and exclude any acts/omissions by customer
- Include “penalties, assessments...” in list of losses

Data Security Measures

- Written requirements:
  - Customer wants vendor to have written infosec, disaster recovery, and business continuity policies
  - Vendor wants req’ts limited to what’s required by law, not by NIST or recommended standards
- Standard:
  - Customer wants “best practices”
  - Vendor wants “reasonable” or “standard” in the industry
Infosec Requirements Exhibit

- Vendor wants its ISR included, and any updates it wants
- Customer wants
  - right to object
  - have time to implement
  - reprice

Data Ownership and Usage

- Who owns what data?
- Data uploaded by customer vs data generated by vendor
- Restrictions on use and disclosure
Cross-Border Data Movement

- Customer wants to restrict movement
- Vendor needs right to have data accessed or moved offshore
- Customer’s consent needs to be short deadline and according to criteria.

Applicable laws

- Know what applicable laws (e.g., GDPR) and standards (e.g., PCI) apply
- Data processing agreement
Customer’s Responsibilities

• Security and privacy is a shared responsibility
• Requirement to install updates promptly
• Customer responsible for unauthorized use of login credentials due to its negligence

Data Breach

• Event threshold
• Notification deadline
• Communication responsibilities
• Vendor to preserve all data and documents
IOT

- Data security requirements
- Password reset
- New California IOT law
- Responsibility for implementing an update

Insurance

- Customer want cyber insurance mandatory
- Limits should reflect potential exposure
- Idea: scale coverage limit up as amount of data (and damages exposure) increases
Audit Rights (1)

- Frequency
- How done?
  - Customer questionnaire
  - Third party auditor
  - Self-assessment
  - Sharing SSAE-type reports
  - Certification
- Vendor’s info is confidential

Audit Rights (2)

- Level of intrusion permitted (pen test)
- Vendor wants copy of findings
- Remediation for “material” failures
Return/Destruction of Data

- Vendor must retain data for legally required time
- Often impracticable to force complete deletion
- Provide language to permit post-term storage

Other Areas

- Data processing agreements
- Equitable relief
- M&A
- Service level agreements
- Force majeure and disaster recovery
Questions?

Please feel free to contact me.

Jason A. Bernstein
Partner, Intellectual Property Group
• Data Security and Privacy (co-chair)
• Technology Agreements
• Patent, Trademark, Copyright Law

Phone: (404) 264-4040
Fax: (404) 264-4033
jason.bernstein@btlaw.com
3475 Piedmont Road, N.E.
Suite 1700
Atlanta, Georgia 30305-3327
www.btlaw.com
Complex Customer Issues In Technology Contracting

Presented By:

Janine Anthony Bowen
BakerHostetler LLP
Atlanta, GA
Complex Customer Issues in Technology Contracting

Janine Anthony Bowen, Esq., CIPP/US
jbowen@bakerlaw.com
(404) 946-9816
Atlanta, GA

Agenda

• Tech Contracting Landscape
• The Complex Issues
• Wrapping it up
Technology Contracting Landscape

The Issues of the Day
The more things change...

- Contractual risk vs. actual risk
- Security/Control issues
- Managing the complex business environment
- Data risk
- IP ownership

The more they stay the same...

- Lock-in
- Cost Control
- Time to deploy
- Transition planning
Understand the legal risk profile

Negotiating the Complex Contract Issues
Transition Assistance

- Lock-in is real
- Under what scenarios do I need time and help moving to another provider?
- Under what scenarios do I get no assistance?

Termination Rights

- What are the scenarios under which a vendor can terminate the agreement?
- When is termination for convenience appropriate?
- When is suspension appropriate?
Ownership of Work Product

- Contingency on payment?
- Contribution to the continuation and growth of the product?

Damages for Data Breach/Generally

- The harm is real, the expense is real – who pay?
- Are there any damages that are uncapped?
Privacy Generally

• GDPR
• HIPAA
• CCPA
• Confidential Info vs. Customer Data

Wrapping it Up/Q&A

• Janine Anthony Bowen, Esq., CIPP/US
  jbowen@bakerlaw.com
• www.linkedin.com/in/jdabowen
• (404) 946-9816
• www.bakerlaw.com
GDPR Implementation Panel

Presented By:

Moderator: Christina D. McCoy
Calero Software LLC
Atlanta, GA

Panelists:
Amanda M. Witt
Kilpatrick Townsend & Stockton LLP
Atlanta, GA

Aruna Sharma
Turner Broadcasting System, Inc.
Atlanta, GA

Toby Spry
Price Waterhouse Coopers
Atlanta, GA
October 19, 2018
EU GDPR Best Practices & Updates

Presentation by:
Christina McCoy, Associate Counsel, Catero Software, LLC
Aruna Sharma, Assistant General Counsel & Data Protection Officer, Turner Broadcasting System, Inc.
Toby Spry, Principal, PwC
Amanda Witt, Partner, Kilpatrick Townsend & Stockton LLP

Agenda
1. GDPR Best Practices
2. GDPR Enforcement Updates
3. Looking Ahead
Assessing Whether the GDPR Applies

General Data Protection Regulation 2016/679 applies to:

1. The processing of personal data in the context of the activities of a data controller or data processor established in the EU, irrespective of where the processing takes place.

2. The processing of personal data of data subjects who are in the EU by a data controller or data processor not established in the EU, where the processing activities are related to:
   • The offering of goods or services to those data subjects; or
   • The monitoring of their behavior in the EU.
GDPR Best Practices

- Clear Roles & Responsibilities (organization)
- Data Mapping for Article 30 Registry
- Data Processing Addenda (DPAs)
- Data Subject Access Request (DSAR) Policy
- Incident Response Policy (Update or Preparation)
- Update Privacy Notice
- Update Consents (and knowledge of “other grounds”)
- Remove Consents from Employment Agreements & Policies
- Appoint DPO
- Data Protection & Retention Policy
- Training
- Change Management Capabilities
- Demonstrating Accountability (“paper trail”)

Challenges of Implementation

- **Data Mapping** – Cross-team Cooperation
- **DPA Challenges** – pushback on processor / controller designations, indemnification / liability struggles
- **Privacy Notice** – struggle to be clear / layered and provide the required information
- **Marketing Communications** – to opt in or not
- **Resource Challenges** – who serves as DPO, organizational implementation challenges
- **Consent Quandaries** – updating old consents, deciding when to rely on consent, etc.
- **Data Subject Rights** – resources / technically enabling access and deletion.
GDPR Enforcement Updates

Early Challenges – Forced Consent

• The first major challenges filed under GDPR relate to “forced” consents from major tech companies such as Google, Facebook and Amazon.

• Max Schrems’ non-profit organization, NOYB, challenged these companies and asserts that under the GDPR, when users are asked to consent, they should be given a free choice – which means that consent should not be a condition of using the service.

• Complaints have been filed in France, Austria, Belgium and Germany and request that regulators impose fines of up to $4.3 billion – roughly 4 percent of each company’s revenue for 2017, the maximum penalty allowed under the GDPR.
Brave Complaint vs. AdTech

- Privacy-friendly browser, Brave, filed GDPR complaints against Google, IAB & other advertisers, in the UK and Ireland in September 2018.
- Complaints relate to the ad tech industry’s practice of disseminating personal data such as location data & browsing history to large amounts of other companies in order to solicit bids from these third parties for behavioral / targeted advertising purposes.
- Referring to such practices as a “massive & systematic data breach”, the complaints allege that real-time bidding practices, violate Article 5 of the GDPR, which requires personal data belonging to EU data subjects be “processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss.”

DPAs Drowning in Breaches

- The UK regulator (ICO) reported in September 2018 that it receives 500 breach reports per week.
- As of Sept. 2018, 1 in 5 breaches reported in the UK involves cyber incidents, of which nearly half concern phishing.
- Laura Middleton, head of the ICO’s personal data breach reporting team, revealed that there were 1,792 breaches notified to the ICO in June 2018, which was a 173% increase from the 647 reports received in May 2018.
- In April 2018, there were only 367 notifications in the UK.
- In Sept. 2018, the French regulator (CNIL) announced that it had received more than 600 notifications of data breaches, involving about 15 million people.
- Since May 25, CNIL has received 3,767 complaints (vs. 2,294 complaints over the same period in 2017, which was already a record year). This represents an increase of 64%. 
Ireland Sees Significant Increase in Reporting

- As of June 6, 2018, the Irish regulator (DPC) had received more than 1,300 “concerns or complaints” since 5/25/18.
- 60 breaches of people’s personal data were reported between 5/25/18 – 6/6/18.
- Between May 25 and May 31, the DPC received around 700 telephone calls and over 650 emails to its information service.
- These included contacts from both individuals raising concerns or making complaints to the DPC and questions from organizations.
- Irish DPC has indicated that it is “unlikely” that contractual necessity would pass muster for “collection and processing of personal data arising from tracking off-platform”—that is, on sites or apps other than those belonging to a particular service provider.

Empowered Data Subjects

- According to a SAS survey, 27% of UK and Irish consumers have already exercised their newfound personal data rights under GDPR.
- 56% of the 2,000 people surveyed in the UK and Ireland reported that they planned to exercise their personal data rights within the next year.
- 76% of UK and Irish survey participants who were aware of the Facebook/Cambridge Analytica story have either activated their GDPR rights or at least reassessed the information they share and how organizations use it.
- Companies can win customers back through respecting data privacy and consent. Customers are most trusting of organizations that promise they will not share data with third parties (38%) or misuse their data (37%).
The French regulator (the CNIL) intends to conduct over 300 investigations (onsite, online or per request of documentation or formal hearing) and will focus on the following areas:

- **Verifying GDPR Compliance** with leniency to be shown to companies with evidence of being dedicated to implementing a compliance program.
- Initiation of **Inspections** with special focus on the following:
  - Processing for *recruitment* activities – especially when using big data & algorithms
  - Adequacy and proportionality of documentation required by *real estate agencies* from applicants – concerns over requiring too much personal data
  - **Outsourcing** to private companies of the fining for paid parking services in public areas

---

**Dutch’s DPA Inspections**

- In July 2018, the Dutch Data Protection Authority (AP) launched "ex officio" investigations into compliance with the GDPR in the private sector.
- The AP intends to verify compliance with GDPR Article 30 (the data registry) in 30 randomly selected large companies (more than 250 employees) in 10 different sectors: industry, water supply, construction, retail, hospitality, travel, communications, finance, business services, and health care.
- Because preparing the registry is a company’s first step towards compliance, logical for AP to focus on it.
- Timing is interesting too because many of employees who would likely be tasked to handle such inquiries may be on summer vacation. Perhaps the AP is hoping to also test the maturity and effectiveness of each organizations’ GDPR compliance programs as required under Article 24 of the GDPR.
Italy’s Inspection Plan

- In August 2018, the Italian regulator (the Garante) announced an approved Inspection Plan for the second half of 2018.
- The Garante intends to focus its inspections on large-scale data processing by companies and national public administration entities.
- The initial two industries of focus will be banking and telemarketing.
- The Garante will put a special emphasis on what data protection measures have been put in place, and in particular, data breach reporting policies.

Early Fines & Enforcement Actions

- In Sept. 2018, the UK ICO’s sent its first GDPR enforcement notice to AggregateIQ, a data analytics company with ties to pro-Brexit groups.
- On Aug. 9, 2018, the Dutch DPA (AP) announced that it had fined Theodoor Gilissen Bankiers N.V. €48,000 for violation of a data subject's right of access.
- The AP found that the bank did not give the customer access to his personal data, and directed it to comply within two months.
- To enforce access, the AP imposed an order subject to a penalty of €12,000 for each week that it did not fully comply with the inspection request, up to a maximum of €60,000.
British Airways’ Breach

- In September 2018, British Airways (BA) notified the UK ICO BA about the hack of its website and mobile app that went undetected between Aug. 21st and Sept. 5th, compromising 380,000 payments.
- Will be a significant test of what enforcement of a major breach under GDPR will look like.
- BA has promised to compensate customers for any financial hardship that they may have suffered.
- Also, SPG Law, the U.K. branch of U.S. class action law firm Sanders Phillips Grossman, said that it was planning to launch a 500 million GBP group action (UK version of a class-action) unless BA settles.

Breach Lessons Learned

- **Exercise caution** when contacting the regulator – not “off the record” with breach notifications.
- Have sound **incident response policy** in place with defensible tools to distinguish “risk” from “high-risk” breaches to determine when to notify data subjects.
- DPAs with **processors** need to require more than notice – need full cooperation to obtain required, detailed information from processors.
- **Cross-border** breaches will test validity of a company’s selection of a lead supervisory authority.
- Don’t get stuck in **silos** – most breaches are global and require cross-border and cross-office cooperation.
UK ICO Offers Breach Reporting Tips

- Mr. Dipple-Johnstone noted that the ICO doesn’t expect perfection, but will look for evidence of senior management and board level insight and accountability.
- When reporting, have authority & access to share necessary information – it is not helpful to be vague.
- Some data controllers are over-reporting – the ICO intends to work with organizations to try and prevent this.
- Treat cybersecurity as a boardroom issue, and demonstrate a robust culture with appropriate transparency, control and accountability for employee & customers’ data.

Looking Ahead

- Will we see changes to the GDPR?
- Brexit’s impact on data flows
- ePrivacy Regulation status?
- GDPR-inspired laws from California’s Consumer Privacy Act to Brazil’s “GDPR”
- Federal privacy law in the US?
- Where to focus next? China? Japan? South Korea? India?
Resilience for our clients and our firm through data management in the world’s most challenging regimes
Blockchain: Implementation Risks

Presented By:

Paul H. Arne
Morris Manning & Martin LLP
Atlanta, GA
Identifying and Managing the Risks of Blockchains:

A Guide for the Non-Technical Person

Paul H. Arne
Morris, Manning & Martin, L.L.P.

Suite 1600
3343 Peachtree Rd. NE
30326
404-504-7784
parne@mmmlaw.com

Copyright © Paul H. Arne, 2018. All rights reserved.
# Table of Contents

I. What is Blockchain?

A. Blockchain Innovations

B. Blockchain Basics

1. Controlling Records
2. Distributed Ledger
3. The Power and Range of Blockchain
4. Other Attributes

C. Consequences of Blockchain’s Basic Design

1. No One has to Control a Blockchain
2. If No One is in Charge, No One May Be Able to Help if Problems Occur
3. Storage is Limited
4. Blockchains Take a Lot of Processing Power

D. Questions to Ask

II. How Do They Do That? The Basic Technologies of Blockchain

A. Controlling Records

1. Encryption basics
2. Two Keys
3. Control and Transfer
4. A Few Other Items to Know
5. Consequences of Using Public Key Encryption and Authentication
   a) Blockchains Do Not Protect Private Keys
   b) Theft of Private Keys
6. Questions to Ask

B. Creating a Distributed Ledger

1. Secure Hash Algorithms
   a) Using Secure Hash Functions to Create Immutability
   b) Risks of Hash Functions
   c) Questions to Ask

C. Reaching Consensus

1. Identifying the Problems
2. Examples of Consensus Mechanisms at Work
   a) Bitcoin Proof of Work
   b) Example of Simplified Byzantine Fault Tolerance Consensus
c) Comparison in Light of DDOS Attack .................................................. 22
3. Performance Issues with Consensus Mechanisms ............................... 22
4. Examples of Consensus Mechanisms .................................................. 22
5. The Difficulty of Consensus Mechanisms .......................................... 25
6. Questions to Ask ................................................................................. 25

D. Governance ....................................................................................... 26
   1. Generally ......................................................................................... 26
   2. Questions to Ask ............................................................................. 27

E. Programming ..................................................................................... 27
   1. Questions ........................................................................................ 28

III. Conclusion ....................................................................................... 28
How risky is blockchain? If blockchain is so great, why is so much cryptocurrency being stolen or lost? Where do I look for these risks? What do they look like? How do I make sure that risks are identified, evaluated, and addressed?

Identifying the risks in blockchain implementations is hard. Once you get under the hood of blockchain, you are rapidly faced with concepts that are not fully understood by one who isn’t a seasoned programmer with experience in distributed systems or one without a math Ph.D. specializing in cryptography and game theory. To make matters worse, many of the risks arise from the details of the technologies used. Yet business people, and lawyers, who do not have technical backgrounds still need to understand the risks associated with blockchain implementations. Millions if not billions of dollars can be at stake in blockchain implementations. You want to make sure that your technical folks are thoroughly addressing the risks involved.

Unless you have a highly technical background, you are going to have to rely heavily on technically-skilled people to help you assess these risks. Even if you don’t understand blockchain, your role may still be to make sure that someone is considering and managing the risks.

This article is written for the non-technical business person or attorney who gets involved in a blockchain project and has the need to evaluate the risks involved. The purpose of this article is to help you identify potential sources of risk, as well as some of the questions you can ask that may help you evaluate the risks of a particular blockchain implementation. You may not know the answers, but at least you will be able to ask good questions. Even if you don’t know the answers, someone on the blockchain implementation team should.

This article has two broad parts.

- What is blockchain? A very general description of the basic framework of blockchain.
- How do they do that? A discussion of the technologies that implement the basic blockchain framework.

Throughout the article, we will focus on two issues:

---

1 Paul is the Senior Partner and Chair of the Technology Transactions Group of Morris, Manning & Martin, L.L.P. He is a member of the firm’s Blockchain and Cryptocurrency Group and is the founder and Chair of the firm’s Open Source Group. This article does not create an attorney/client relationship with you and does not provide specific legal advice to you or your company. Certain legal concepts have not been fully developed and certain legal issues have been stated as fact for which arguments can be made to the contrary, due to space constraints. It is provided for educational purposes only.

2 Special thanks to Rachel Neufeld for her contributions to this article.

3 People frequently distinguish between “blockchains” and “distributed ledger technologies.” For simplicity, in this article I use “blockchain” for both.
1. We will identify some of the risks that arise from the basic framework and technologies used in blockchain implementations.

2. We will provide a list of questions that you can ask the developers of a blockchain implementation to determine:
   - what risks are involved,
   - whether the developers have considered those risks, and
   - whether the developers have taken steps to address those risks.

I. What is Blockchain?

Blockchain implementations are exceedingly varied. Blockchains are being used or implemented for the following purposes, just to name a few:

- Keeping track of the distribution of produce, from farm to grocery store
- Voting systems
- Electronic money, or cryptocurrency
- College diplomas
- Shipping
- Logistics
- Cross-border payments
- Managing medical records
- Prediction markets (gambling?)
- The quality of journalism
- Settlement of stock trades
- Data storage
- Real estate deed records
- Supply chain management
- Data security
- Automotive repair recordkeeping
- Electric power distribution
- Real estate mortgage origination and processing
- Electronic collectibles
- Video games
- Advertising transparency
- Travel booking settlement
- Awards programs
- Music distribution
- Corporate stock records
- Running computer programs

Much of this breadth exists because so many different types of information can be put in digital form. Digital information is normally stored in databases in a grouping of bits (a string of ones and zeroes—the language of computers; we’ll call them “records”). Generally speaking, it is useful to think of the following types of digital information that can be stored and manipulated on a blockchain.
**Figure 1**

<table>
<thead>
<tr>
<th>Type of Record</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. The record itself has value.</td>
<td>Bitcoin and other cryptocurrencies.</td>
</tr>
<tr>
<td></td>
<td>Cryptokitties.</td>
</tr>
<tr>
<td>2. The record is the ownership of an asset that exists off of the blockchain.</td>
<td>A car title. Having your name on a paper car title is your actual ownership of the car. One can put car titles on a blockchain rather than relying on a paper title. Owning the title record on the blockchain becomes the equivalent to having your name on a paper car title. Transferring a record on the blockchain becomes the replacement for signing over a paper car title to another person.</td>
</tr>
<tr>
<td>3. The record gives one the ability to control something that is not on the blockchain.</td>
<td>One can create a “token” as a blockchain record, which gives the owner the right to do or use a certain thing off of the blockchain. Examples include:</td>
</tr>
<tr>
<td></td>
<td>• The right to vote on something, or</td>
</tr>
<tr>
<td></td>
<td>• The right to use a certain amount of data storage.</td>
</tr>
<tr>
<td>4. The record is the ability to run a computer program, which runs on the blockchain, and specify its inputs.</td>
<td>Ethereum is the most well-known of this kind of blockchain.</td>
</tr>
<tr>
<td>5. The record is information.</td>
<td>Keeping track of produce from farm to grocery is an example. Repair records for a car is another.</td>
</tr>
</tbody>
</table>

As you can see, there are a wide variety of uses for blockchains. Many blockchain implementations will fit into more than one category above. The flexibility of what the bits in a record are or represent is what allows blockchain technology to be used in a vast number of situations.

Blockchains can also vary depending on who has the ability to see what is on the blockchain and who can write information on the blockchain. Accordingly, some are known as “public” blockchains, others as “private” blockchains.

Blockchain can enable business models that have not existed before. This is especially true for real life assets that can be “tokenized” on a blockchain. The uncertainty and risk can be compounded by the newness, even strangeness, of the business models being implemented.
Because of this incredible breadth, the risks involved vary widely. A blockchain that keeps track of produce does not have to worry much about whether a country’s government can take it down; cryptocurrencies do.

**A. Blockchain Innovations**

The technologies used in blockchains are enabling companies to perform business processes in more efficient and at times novel ways.

1. Blockchains present a way of storing and manipulating data on a database that is different from the way data has been traditionally stored on databases. The interest in blockchains has increased the visibility of methods that can be used to enhance the privacy and security of traditional database records through the use of public key cryptography and secure hash functions, whether or not other blockchain technologies are used.

2. Tokenization—the creation of a blockchain record to grant rights in things that exist off of the blockchain—has been a source of substantial market innovation. For example, there are at least two companies that are “tokenizing” data storage, in essence creating a market where owners of excess data storage capacity, along with others, can sell that capacity to those who need more data storage. One can create tokens that allow for a return of a fractional piece of the electrical output of a solar panel. This “tokenization” of assets that exist off the blockchain has created new ways of creating, exploiting, and monetizing assets.

3. Blockchain’s ability to reach consensus about the content of a database, without the use of a central repository controlled by a single entity, is a potential source of substantial disruption in many industries.

4. By creating an asset that is in essence a computer program, blockchain can allow behaviors to be a part of the asset itself.

Combining these blockchain features has resulted in an explosion of creativity and new business models, not to mention efficiencies that have not historically been available.

**B. Blockchain Basics**

Not surprisingly, different blockchains have many different features, but all of them have two essential elements:

1. a way to allow a single person to control a record in a database, and

2. a distributed ledger database.

1. **Controlling Records**

Since the 1970s, technologies have existed that allow a single individual to have complete control over a database record or other set of digital information. The record can be publicly available to anyone, yet one individual can completely control that record. One individual can prevent anyone else from being able to manipulate that record. One individual controls to whom the record can be
transferred. Once transferred to another individual, the record can then be completely controlled by the recipient. The ability of a single person to completely control a record is one of the two most fundamental aspects of blockchains.

2. **Distributed Ledger**

Blockchains are a particular kind of database, called a “ledger.” Records posted in blockchain ledgers cannot be modified or deleted; records can only be added to the ledger. Ledgers are a familiar form of database. A check register is a form of ledger, as are many accounting databases. One enters information in the ledger and then adds additional information as time goes by, without changing or deleting what is already on the ledger.

In blockchains, an exact copy of this ledger is frequently stored in many, even thousands of, separate computers that are controlled by many different entities. All of the copies of the databases contain exactly the same information. All of the records in the blockchain are kept in each of these databases. The computers holding copies of the ledger are usually called “nodes.”

In blockchains, groups of records are assembled together in a “block.” Blocks are chained together on the ledger in a way that the information in the blocks cannot be changed. Thus, “blockchain.”

That’s it. **Records, each controlled by an individual, are grouped in blocks, all of which are stored on a ledger in many identical nodes.**

While this is easy to describe, how one goes about actually doing what was just described is much more complex. We will address the basics of this in Section II of this article. Before we get into some of the details, however, there are some attributes and consequences—and corresponding risks—of this basic structure that are important to address.

3. **The Power and Range of Blockchain**

Blockchains have a few key attributes that give it much of its power.

1. Once a record is put in a block on a blockchain, it is very, very difficult to change. This characteristic is called “immutability.”

2. Blockchains allow nodes to reach a common understanding about what records to put on the ledger and about the accuracy of those records. This is probably blockchain’s biggest innovation. Historically, if a database receives data from many sources, there is almost always a single source that determines which records are valid or not, and whether those records should be placed in the database. Having a single entity to determine the “truth” is not necessary in blockchains. The network of nodes and the technology itself is the source of truth, not a specific entity. Accurate information is available at each node, without a bank, credit card company or government—to name a few—being the ultimate arbiters of what is correct.

3. In many blockchain implementations, a key element in reaching this common understanding is that a significant percentage of nodes must agree for a record or block to be added to the
This makes the work of a hacker much more difficult, especially if resources (computer processing power, for example) must be expended to create the next block, if there is a time limit before the next block is created, and the resources to be expended must start over with each new block. In order to change transactions or records, the hacker must not only gain access to many computing systems rather than just one, the hacker must also expend resources that are multiplied by each node hacked. The hacker must also start over every time a new block is added to the blockchain. The distributed nature of blockchains is a key element to the security of the blockchain.

4. Other Attributes

Blockchains have other attributes that should be kept in mind.

1. While some blockchain technologies are mature, as bundled together the technologies used to create a blockchain are very new. They are immature. They can and must change over time.

2. While the basic technologies are the same, each of the basic technologies is actually a family of technologies. The choice of family member can impact the risk. Your developers should have considered the risks and benefits of the particular kind of basic technology chosen. You can ask (1) whether there are known vulnerabilities of the technology chosen and (2) why the particular technology was chosen. If you don’t get good answers, then maybe your company needs additional assistance with or review of the blockchain project.

3. One blockchain might use another blockchain to perform certain tasks. Blockchains can be made available as a service. They can be used in combination.

4. The blockchain itself is virtually never the whole story. Blockchains are normally a key element to a larger set of technologies that solves a particular business problem or addresses a particular business process. While much attention has been focused on the blockchain itself, many of the vulnerabilities of blockchain implementation are in the technologies that operate outside of the blockchain itself.

This description leaves a lot of important stuff out. It describes what a blockchain is rather than how it works, and the how is critically important. However, there are important risks of blockchains that can be derived from these basic elements.

C. Consequences of Blockchain’s Basic Design

Early in the process of helping to evaluate risk, it is critical to understand the basic design of a particular blockchain implementation.

1. No One has to Control a Blockchain

In many blockchain implementations, the code for the blockchain is licensed under one or more permissive open source licenses and made available to anyone who wants to use it. If you want to
operate a node, often you can simply download the software and set it up on a machine. There may be no restriction on who can create a node. This has three very important implications.

1. **There is no need for a data “owner.”** The network acts to create accurate records, rather than a bank, credit card company, healthcare provider, etc. If there is no central authority who determines the ultimate truth of records, the fees paid to those central authorities don’t need to be paid, either. The absence of a data “owner” or hub is a substantial source of the disruption that blockchain implementations can cause to existing business models.

2. **No one has to own a blockchain implementation.** Think about this for a moment. For some blockchain implementations, anyone can download the software and operate a node, and there is no need for a central entity that decides what data goes on the blockchain. If this is the case, who is the owner of it? The software developers may not be involved in the blockchain network at all. Owners of nodes only control their own nodes. No single entity controls the data. Analyzed from a traditional legal entity standpoint, there may be no individual, partnership, corporation, LLC, or other entity that actually has “ownership” of the blockchain. If there is a problem, who do you sue?

3. At least where anyone can get a copy of the software and anyone can operate a node, one can simply copy the software and the ledger and start a completely new blockchain implementation. Whoever is the owner of the records in the first blockchain are now also owners of the records in the new blockchain as well. Following the nomenclature in the open source community, this branching of a blockchain is called a “fork.”

4. If no one controls a blockchain, how does it evolve? As mentioned above, blockchains are immature at this point. They must evolve, improve. If different people control the nodes, then how do you get everyone to upgrade? **Governance is an outsized issue with blockchain implementations.**

2. **If No One is in Charge, No One May Be Able to Help if Problems Occur**

If someone steals your credit card and uses it to buy something, you can call your credit card company and get them to reverse the charges. If the credit card company is there to fix the problem. On a blockchain, because there is no data owner, database owner, or central decision-making authority for what data goes on the blockchain, there may be no one to fix problems that arise. If you lose the information that allows you to manipulate a record on a blockchain, it may be lost forever. If someone is able to steal your record, it may well remain stolen forever. Transacting on a blockchain can be a high wire act without a safety net. If information or a record is stolen, there may not be anyone who can fix the problem. It may even result in records that cannot be changed at all.

---

4 It doesn’t hurt that this is required by law.

5 This is a private key, as will be discussed below.
This has special consequences related to how private keys are stored and protected. More on this issue later.

3. **Storage is Limited**

If you have many, many nodes keeping the same information in database ledgers, **data storage becomes an issue as the blockchain grows.** The size of the database itself is limited by the storage capacity of each node. Since every record is stored on every node, a lot of storage is needed to enable a widely distributed blockchain.

Typically, normal database implementations outside of the blockchain world can store more information because complete copies of those implementations do not have to be stored in thousands of locations. Some kinds of records simply can’t be stored on a blockchain. No one, for example, is trying to store medical records on the blockchain itself. They are too big. This has a few important implications as well.

1. **Records stored on blockchains normally need to be limited in size.**

2. This is one of the reasons that people opt for model #3 in Figure 1—using blockchain to control something off of the blockchain.

4. **Blockchains Take a Lot of Processing Power**

Compared to regular databases, **blockchains take a lot of processing power.** The power required is basically the processing power needed to run a normal database, multiplied by the number of nodes.

Some blockchains use consensus mechanisms—discussed below—that need an extraordinary amount of processing power; however, the point here is a different one. Compared with an ordinary database, each node must process some data in order to add blocks on the blockchain. This need to process data on multiple nodes, maybe thousands of nodes, means that a database implemented on a blockchain necessarily uses more processing power than a database structure that has a single database of record.

The storage and processing limitations are reasons that blockchains frequently store information that is used to control information that resides off of the blockchain.

**D. Questions to Ask**

The description of the basics above is a good guide to the questions you should consider asking your development team. If your development team can’t answer these questions adequately, then further investigation may be warranted. Many of these items will be discussed in more detail in the second part of this article.

1. Since we know that blockchains themselves are usually only a part of any particular solution, you should **ask how the whole solution is put together.** People tend to focus on blockchains, but they are rarely the entire solution. Implementations using blockchain
methodologies frequently have the most risk in systems that operate outside the blockchain itself.

2. **Who will have access to read the records** that are placed on the blockchain?

3. **Who will have access to write the records** to be placed on the blockchain?

4. Is the blockchain technology licensed under open source licenses? If so, under what open source licenses?

5. **Who will be allowed to create a node** on the blockchain?

6. **How are changes to the blockchain accomplished?** Who has to agree? How is that agreement reached?

7. **How are issues addressed if things go wrong**, such as if someone’s record on the blockchain is stolen or is inaccurate?

8. **Are there technical limitations that must be overcome** before the implementation can achieve its intended use?

One final thought. Because many business processes implemented with blockchains are “new,” many companies are attempting to gain patent protection for these new business models. (E.g., cross-border payments + that fancy new blockchain stuff = a new patentable process!) Care should be taken to identify potential patent issues with blockchain implementations.

**II. How Do They Do That? The Basic Technologies of Blockchain**

We will need to get a little technical here, but the explanations below are still for non-technical people. You can always skip the details if you want; it is the conclusions and questions that arise from these details that you can use to identify risks.

It is easier to state what is in the first section of this article than it is to do it. How this could be done was first revealed by the publication of an article on October 31, 2008.⁶

**A. Controlling Records**

One of blockchains’ most important features is that a single person⁷ has the ability to control a record. This is done using cryptography, specifically public key cryptography. Public key cryptography isn’t just for encryption. It also allows you to securely control a database record, using a digital signature.

---


⁷ Actually, it doesn’t even need to be a person. One of the memes of blockchain is “On the blockchain, no one knows you’re a fridge.” The quote is ascribed to Richard G. Brown. See [https://www.linkedin.com/pulse/blockchain-one-knows-youre-fridge-eliot-mills](https://www.linkedin.com/pulse/blockchain-one-knows-youre-fridge-eliot-mills), last visited October 2, 2018.
Think of the role of signatures in a paper world. Let’s assume you have a blank check for your checking account. You fill out the check, made payable to someone else, and sign it. By signing the check, you are directing your bank to “Pay to the Order of” another person a specified sum of money. Your signature at the bottom of the check is your authorization to your bank for this transfer to occur. If the check is not signed by anyone, then your bank is not authorized to transfer funds from your account. If the check is signed by someone else—a forgery—then your bank is still not authorized to transfer funds from your account, because the check wasn’t signed by you.

Obviously, there are lot of things that could go wrong with this paper transaction. However, the principle is that you are directing someone—your bank—to do something through the use of your signature. Let’s see how this can be done electronically.

1. **Encryption basics**

The basic idea of encryption is to take a message that you don’t want most people to read, convert (i.e., encrypt) it into a form that can’t readily understood through the use of a “key” and some math, and send the encrypted message to the intended recipient, who in turn uses a key and some math to decrypt the message. Here’s a quick example.

| Unencrypted message: | 12 37 57 26 |
| Key = 20 (add): | 20 20 20 20 |
| Encrypted message: | 32 57 77 46 |
| Key = 20 (subtract): | 20 20 20 20 |
| Unencrypted message: | 12 37 57 26 |

Unless you know the key and the math used, anyone who intercepts the encrypted message will have a difficult time figuring out that 32 57 77 46 really means 12 37 57 26.

2. **Two Keys**

The encryption scheme above uses the same key (20) to encrypt and decrypt the message. This is known as a “symmetric” key. Symmetric key cryptography has many uses. One of the most popular kinds of symmetric cryptography is called AES265, which is frequently used in financial transactions.

There is another kind of cryptography that uses two keys rather than one: public key cryptography. It is the technology that allows one to transfer of things of value electronically.

Public key cryptography uses two keys to encrypt and decrypt messages. Let’s call them Key 1 and Key 2 for now. These two keys are created together, but it is almost impossible to determine what Key 1 is from Key 2 and vice versa.

If you encrypt information using Key 1, the information can only be decrypted using Key 2. Not even Key 1 can be used to decrypt the message. If you encrypt information using Key 2, only Key 1 can decrypt it. The encryption and decryption keys are “asymmetric.”
Let’s suppose that our friend Alice creates a key pair. Alice keeps Key 1 to herself (Alice’s Private Key) and doesn’t disclose it to anyone else. However, she publishes her Key 2 on the internet (Alice’s Public Key) so anyone can see Alice’s Key 2.

Now let’s suppose that Bob wants to send Alice a message that only Alice can read. Bob takes the message and encrypts it using Alice’s Public Key. He then sends the encrypted message to Alice. It doesn’t matter who else gets the encrypted message. The encrypted message can be sent to or intercepted by anyone, but only Alice can decrypt it, because only Alice has Alice’s Private Key. This is a huge innovation, because it allows for private messages to be sent over a public network without the parties having to exchange the decryption key first.

However, the reverse of this action is what is most important to understand here. Suppose instead that Alice encrypts a message using Alice’s Private Key. This action may seem silly at first, because anyone with Alice’s Public Key can read the message. However, only Alice could have sent this message. Encrypting with a private key is a very secure way of ensuring who created a message.

By Alice encrypting a message with Alice’s Private Key, she has effectively “signed” the message. The message can only have come from her. “Signing” a message with a private key can be the electronic equivalent to signing your name at the bottom of a check.

Encrypt with Public Key = Encryption
Encrypt with Private Key = Authentication

Figure 2 above can now be revised.

![Figure 3](image_url)

Importantly, there is a way to connect an unencrypted message with an encrypted message. This uses another technology called “secure hash functions,” which are addressed below. By encrypting with a private key and using a secure hash function, Alice can not only “sign” an

---

8 True authentication will also usually require a time stamp, the use of a secure hash function, and the use of a certificate, discussed below.
electronic document, she can also prove that the associated unencrypted message is unchanged from what she originally sent.

3. **Control and Transfer**

Having something encrypted with Alice’s Public Key means more than only Alice can decrypt it. In essence, it means that **Alice has complete control over the message** that was encrypted. No one else can do anything with it, since only Alice can decrypt it.

This gets more interesting when Alice and Bob both have key pairs. Using multiple key pairs allows one to transfer control of a record.

If Alice wants to transfer her encrypted record to Bob, she:

1. decrypts the record with Alice’s Private Key,
2. encrypts the record with Bob’s Public Key, and
3. signs the encrypted record with Alice’s Private Key to prove that she’s the one doing it.

Once the message is received by Bob, everyone with access to Alice’s Public Key knows that she has transferred the record, and now Bob is the only one who can do anything with that particular record.

**Public key cryptography allows a person to completely own a record and transfer it to another.**

Real world encryption and authentication schemes are more complex than this example, using multiple key pairs, as well as symmetric encryption.

4. **A Few Other Items to Know**

1. **Public key cryptography (in both directions) comes in strengths.** Generally speaking, the strength of an encryption key is a function of the length of the keys. The longer the key, the greater the difficulty in decrypting if you don’t have the appropriate key.

2. **Higher strengths of encryption are treated as a munition for the purposes of U.S. law.** Just as you can’t export nuclear material or fighter jets outside the U.S. unless you get permission from the government, you can’t export encryption technology above a certain strength. Unfortunately, it is much easier to inadvertently violate the law when you are dealing with encryption technology than with nuclear material. You can “export” encryption technology within the meaning of U.S. export laws simply making it available on the internet. Make sure that you and your company aren’t violating this law.

---

9 22 CFR 121.1, Category XII (B).
3. There is a really big hole in public key encryption technology that may, or may not, need to be filled. Suppose a malicious person, Mallory, decides to impersonate Alice. Mallory creates her own public/private key pair and publishes the public key, claiming that she is Alice. How does Bob know that a public key is actually Alice’s Public Key? Generally speaking, Bob can’t know. Of course, Alice could physically meet with Bob, provide lots of identification to prove who she is and personally give Bob her public key, but this is not usually practical on the internet.

   This hole is filled with something called a “certificate.” Certificates are normally held by a Certificate Authority, or CA. Instead of Alice and Bob physically meeting, Alice goes to a CA to get her public/private key pair. The CA requires Alice to provide sufficient identification to prove that she is Alice. Once the key pair is generated, Alice gets her private key, and the CA publishes a certificate on the internet that certifies that a certain number is Alice’s Public Key. Bob can make sure that he is communicating with the right person by looking up Alice’s Public Key at the CA’s website. However, many blockchain implementations DO NOT use certificates. Because one’s public key is normally available on the blockchain, blockchains that don’t use certificates are not completely anonymous; they are considered pseudonymous, meaning that the identity of the person may not be immediately self-evident, but one can frequently determine who the person is by comparing the blockchain records with other available sources of information.

4. Protection of private keys is critical. If Mallory instead steals Alice’s Private Key, Mallory can act just as if she is Alice. Mallory can use Alice’s Private Key to transfer Alice’s records on the blockchain. If Alice loses her private key, then the ability to do anything with a record that has been encrypted with Alice’s Public Key has been lost forever.

5. Public key encryption can be used in a variety of ways to accomplish an action. You don’t always have to distribute the public key. If I wanted only one person to be able to read what I encrypt with my private key, I could encrypt it with the recipient’s public key before sending it. Key pairs can be created for a single transaction only. The key pair may be set up to expire after a period of time, or after a number of uses. You can use multiple key pairs in tandem with each other to accomplish a specific result.

6. Relatively speaking, public key cryptography requires significantly more computing power than other forms of encryption. Accordingly, there is a processing and throughput cost to the use of public key encryption.

7. This use of a private key to “sign” something is called a “digital signature.” There is also something called an “electronic signature,” and it is important to distinguish between the two. A “digital signature” is something that has been encrypted with a private key for the purposes of signing something. An “electronic signature” is any action taken electronically with the intention of signing something. Signing your name to an email can be an electronic signature, if your intent is to sign the email, but it is not a digital signature. Digital signatures require the use of public key encryption. Digital signatures are a subset of electronic signatures.
Legally, electronic signatures are treated the same as their paper counterparts, and electronic records are treated the same as paper documents.¹⁰ A digital signature is just a really secure electronic signature.

5. Consequences of Using Public Key Encryption and Authentication

Public key cryptography has been around since the 1970s. It is a tried and true technology and is used routinely on the internet. Most of the readers of this article use public key encryption every day without knowing it. It is built into established protocols of the internet. Generally, its strengths and weaknesses are well known. While specific implementations of public key cryptography may be risky, public key cryptography itself is one of the strengths of blockchains. It is one of the main reasons that cryptocurrency blockchains themselves are rarely, if ever, compromised. However, just because the technology has been around for a long time doesn’t mean that you shouldn’t ask your developers questions about it. It also doesn’t mean that you don’t need to know some of the consequences of using it.

a) Blockchains Do Not Protect Private Keys

One of the biggest risks related to blockchain exists because of its use of public key cryptography. Records on a blockchain are typically the result of using a public or private key to encrypt something. Public keys frequently are stored on the blockchain, although that is not always true. Private keys are hardly ever stored on a blockchain, at least not in unencrypted form or in a manner that makes them available to third parties.

Where and how private keys are stored and protected is a paramount issue for many, if not most, blockchains.

The risk of loss or theft of private keys is compounded by the absence of a central authority that can “make things right.” If someone steals money from your bank account, or someone steals and uses your credit card, you can probably get your money back by working with your bank or credit card company. Having some organization make things right may not be available when blockchain is used.

Possession of a private key IS and should be treated as ownership of whatever that private key can decrypt. You can lose your “ownership” of something encrypted with your public key if any of the following occur:

- if your private key is only on your laptop’s hard drive, and your hard drive crashes with no backup,
- if the software at the website where your private keys are kept crashes and loses your private key,

- if the site where your private key is stored is hacked,
- if you misplace your private key,
- if you die and don’t leave your heirs access to your private key, or
- if your private key is stolen.

If that record represents a cryptocurrency, you may have done the equivalent of burning hundred dollar bills. You no longer own the record, and in many blockchain implementations, you can’t get it back.

b) Theft of Private Keys

Notorious bank robber Willie Sutton was reportedly asked by a reporter why he robbed banks, to which he responded, “That’s where the money is.” Any place that stores multiple private keys is a prime target of hackers. Exchanges, which allow you to trade money and cryptocurrencies, will frequently store private keys for your convenience. **Loss or theft of private keys at exchanges are responsible for some of the most spectacular losses of blockchain-enabled assets.**

The protection of private keys is paramount.

6. Questions to Ask.

1. What cryptography technology is being used?
2. How well-established is the cryptography technology? Does it comply with any standards established by standards organizations?
3. Why was that encryption technology chosen?
4. Have the vulnerabilities of the encryption technology been studied? How long has the encryption technology been used? These questions are especially important for new encryption technologies or ones that have not been adopted by standards organizations.
5. Has the encryption technology been used at scale before?
6. Has anyone checked to make sure that the encryption technology used is not a munition?
7. Does the blockchain use certificates to identify owners of public keys? If not, how are users identified?
8. How are private keys protected? You should expect a detailed answer to this question, which may involve “cold storage,” hardware wallets, multi-signature implementations, etc.
B. Creating a Distributed Ledger

The second major feature of most blockchains is the use of a ledger, exact copies of which are stored on multiple nodes. In order for this to be useful, the distributed ledger needs the following attributes:

- Once the records are posted to the blockchain, they need to be really hard to change. No one should be able to change records once they are put on the blockchain ledger. This is done by using secure hash algorithms. It also involves consensus mechanisms. Both of these are described below.

- Blockchains need mechanisms to ensure that records put on the blockchain are valid, as well as a mechanism to figure out what records go onto the blockchain, so all nodes have exactly the same data. This is done by using consensus mechanisms as well.

1. Secure Hash Algorithms

Secure hash algorithms are used to ensure that something in electronic form has not been changed. Sometimes also called cryptographic hash functions, they are mathematical algorithms, or formulas, with the following features:

- **You can run any length number through the function and you will always get a fixed length result.** For example, the 256 bit version of SHA2 always returns a 256 bit result, no matter how long or short the input number is.11

- **If you run the same number through the same secure hash algorithm, you always get the same number as the result.**

- **If you run a different number through a secure hash function, you will get a very different, seemingly random number,** no matter how slight the difference between the original two numbers. This isn’t completely random, because if you run the same input through the hash function, you get the same number. However, even if you change a single bit in a very large binary number, you cannot predict the resulting number.

- **You can’t predict what the different hash result will be based on the changes to the input number.** Even if you change a single bit in a million bit number, the output of the secure hash function will look completely different, and it is exceedingly difficult to determine how the hash result will change.

- **You can’t determine the original number input from the output number.** It is relatively easy to run a digital copy of a feature length movie through a secure hash function, but it is virtually impossible to use the hash result and turn it into the feature length movie.

---

11 If you want to try this out for yourself, go to https://passwordsgenerator.net/sha256-hash-generator/. Note that the output is in hexadecimal form, where the number 0-9 are just like their decimal counterparts and a-f are the numbers 10-15.
Secure hash functions can be used for any sequence of numbers, even if they represent different things. For example, an individual record in a blockchain may consist of multiple elements, but as long as the record as a whole can be set out in a single string of numbers, you can hash it. Similarly, a block of multiple records can consist of various parts: each individual record (with its various parts), one or more hash results, and even adding in some random numbers, yet you can hash the block as a whole.

a) **Using Secure Hash Functions to Create Immutability**

As you can see from above, secure hash functions can demonstrate whether a number, of any length, has changed. Secure hash functions are the key to immutable records on a blockchain. Here’s how it works.

**Figure 4**

Take three records and put them together in a block. The block is now a single string of bits, being the combination of the three records. Running that unique set of ones and zeroes through a secure hash function will create a fixed length result or “hash” of that block. For the next 3 transactions, which makes up the second block, add the hash result of Block 1 to the three records. To create Block 3, take the next three transactions and add the hash of Block 2.

After the creation of Block 2, if someone changes anything about Block 1, the hash of Block 1 will change. If the hash of Block 1 changes, the hash of Block 2 will also change. After creation of Block 3, if any change is made to either Block 1 or Block 2, the hash of Block 2 will change. Any change of any prior record will manifest itself in a change to the last hash result. A single number in the last block validates that no changes have been made to any records on the blockchain. Because complete copies of the blockchain are stored in multiple nodes, any node with a different last hash result will be easy to identify and can be corrected.

Now imagine that there are 10 separate nodes on 10 separate computers that have an exact copy of this blockchain. Once Block 3 is in place, someone who wants to falsify any transaction in Block 1 will have to change three blocks in each of 10 different systems. Depending on how many separate
nodes there are in a blockchain and how hard it is to create the hash of each block, this use of secure hash functions rapidly makes the blocks unchangeable, or “immutable.” (Immutability is not an absolute concept; generally you should consider “immutability” to mean “really hard to change.”)

Immutability will also be addressed in the discussion of consensus mechanisms below, since how quickly blocks in a blockchain become immutable is also a function of the consensus mechanism used.

Secure hash functions are the key to record immutability on blockchains.

b) Risks of Hash Functions

Not all secure hash functions are created equal. It used to be that one of the most used secure hash functions was Secure Hash Algorithm 1 (SHA1). Vulnerabilities were discovered in SHA1, so the technology industry has been migrating to SHA2 of varying bit lengths, the most popular of which is the 256-bit version, SHA256.

In addition, secure hash functions are frequently selected over other possible secure hash functions based on the frequency of “collisions.” Collisions are where two different inputs result in the same hash result. Not having too many collisions is a feature of a good secure hash function.

There are other attributes of secure hash functions that can also be important, but some of those will be addressed in the discussions below about consensus mechanisms.

c) Questions to Ask.

- For this blockchain, what hash algorithms are being used?
- What secure hash function do you use to chain blocks together?
- Other than chaining blocks together, what are the hash algorithms used for?
- Is the secure hash function approved by any standards organizations?
- Why were these hash algorithms chosen?
- What are the known vulnerabilities of these hash algorithms?
- Have the vulnerabilities of hash algorithm been studied? How long has the encryption technology been used?
- Has the hash algorithm technology been used at scale before?
- How are the risks associated with known vulnerabilities being addressed in the design and implementation of the blockchain?
C. Reaching Consensus

In order to have all the ledgers in all the nodes be exactly the same, there has to be a way for them to reach agreement on which records are valid and which should be included on the ledger. The means of reaching consensus are called “consensus mechanisms” or “consensus algorithms.”

As discussed earlier, databases have traditionally been controlled by a single entity. This single entity becomes the sole arbiter of what records should go on the database and their accuracy. In many ways, being able to reach a common understanding as to what records are valid and should go on the database without a central authority is the true cognitive leap of blockchain.

This is also the area where a non-technical person will need the most technical help. Unlike public key cryptography and secure hash functions, which have been used since at least the 1970’s, the consensus mechanisms in use are relatively new, can involve complex math (especially game theory), and are rapidly evolving, even though many of the challenges from a computer science standpoint have been studied for decades. In the choice of consensus mechanism, your developers should be relying on true experts.

Game theory is important here. Those who determine whether particular records are valid and those who choose which records should go on the blockchain must be motivated to do the right thing, through all the various situations that they find themselves in.

There are a myriad of consensus mechanisms. New consensus mechanisms are begin created all the time. Picking the right one for a particular blockchain requires considerable skill, experience and, probably, an understanding of game theory.

Consensus mechanisms can also have a very important impact the performance of the blockchain. There may be other reasons for selecting a particular consensus mechanism over another. For example, as of this writing, the Bitcoin and Ethereum blockchains both use a consensus mechanisms that are in the “proof of work” family, but they use different secure hash function algorithms for this purpose. The makers of Ethereum felt it important that the algorithm used can be more readily calculated using graphics processing chips (GPU’s) rather than application-specific integrated circuits (ASIC’s), so the Bitcoin and Ethereum blockchains use different algorithms.

In order to determine whether a consensus mechanism is appropriate for a particular blockchain, one should consider what problems need to be solved and what the tradeoffs are between different consensus mechanisms.

1. Identifying the Problems

Identifying the different types of bad things that can happen to a network is a good starting point for determining what consensus mechanism should be used to combat those problems. The level of risk of the problems may be different, depending on the type of blockchain.

---

12 Ethereum has announced its intent to move from a proof of work consensus mechanism to one called “proof of stake.”
• Attacks on the network itself. The most frequently discussed problem here is a distributed denial of service attack (DDOS), where many computers are taken over by a malicious agent and all send many requests to a server, seeking to overwhelm the server.

• Double Spending Problem. You don’t want someone who has an asset on a blockchain to sell it twice, like one might be able to do if you could quickly transfer the asset on two separate nodes.

• Byzantine Generals Problem. Some of the potential problems can be grouped into what computer scientists call the “Byzantine Generals Problem.” These problems are basically those that exist when a distributed database cannot be sure that the messages it gets about the data are correct or not. Generally speaking, these are:
  o The failure of one or more nodes.
  o The communications between nodes fails or is delayed.
  o Messages from one or more nodes are forged. One of the kinds of attacks in this context is called a “man-in-the-middle attack.”
  o False record or block provided by one or more participants on the blockchain.

• Changing an existing record or block by a malicious hacker.

• Changing a record or block by one or more participants on the blockchain.

One can simplify these potential problems into two different major categories:

1. Problems caused by the lack of availability of some of the nodes on the blockchain or the communications infrastructure and

2. Problems caused by unreliable pieces of information coming from different sources.

In order to reach a consensus around the correct information, the decision maker must be motivated to reach the proper consensus over all situations that may occur on the blockchain over time.

2. Examples of Consensus Mechanisms at Work

It may be useful to compare two different consensus mechanisms to show how they react differently to a potential problems: a DDOS.

---

a) **Bitcoin Proof of Work**

Bitcoin uses a type of consensus mechanism called “proof of work.” Bitcoin is designed in a way that a new block is created approximately every ten minutes. In Bitcoin, there are maintainers of nodes that participate in the creation of new blocks, called “miners.” The process is as follows:

- All proposed records are broadcast to all nodes.
- Each node collects records into a proposed block.
- Each node runs a hash calculation, using SHA256, against the combination of the proposed records in the block, the hash result of the prior block, and an arbitrary number called a “nonce.” Each miner has a different starting nonce.

At this point, a little math is needed to understand what is going on. Because the hash results are basically random, the chances of any hash calculation beginning with the number 0 instead of 1 is ½. The chances of a hash calculation beginning with two zeroes is 1/4 (or 1/2²). The chances of having 60 leading zeroes is 1/2⁶⁰. The number of leading zeroes, i.e., the upper threshold of the number that is acceptable, is called the “difficulty.”

- Once a miner calculates a hash result that is less than the difficulty, that miner gets to post the next block, which is then broadcast to all nodes. If the hash result is more than the difficulty, then the miner increments its nonce (i.e., prior nonce + 1) and then runs the hash calculation again. The process is repeated until one of the miners calculates a hash result below the difficulty.

Every miner is in a race to find a hash result that is below the difficulty level. This means that the likelihood of a particular miner calculating a hash result less than the difficulty is the ratio of the amount of that miner’s computing power applied to the task, as the numerator, divided by the total computing power of all nodes, as the denominator. While this ratio will work out on average, which miner gets to create any particular block is essentially random.

As of this writing, in order to get a new block every ten minutes, the number of hash calculations that are performed by all miners on the Bitcoin blockchain is about 57 million trillion hash calculations per second. This is not a typo. Fifty-seven times a million times a trillion. In Bitcoin proof of work, you have thousands of miners performing billions of hash calculations per second, and the one that achieves a hash result below the difficulty number wins.

b) **Example of Simplified Byzantine Fault Tolerance Consensus**

Another example of a consensus mechanism is one of the forms of the Simplified Byzantine Fault Tolerance (SBFT) consensus mechanism. In this example, one node is elected by the other nodes to make the decision of what records should be included in the next block. If a specified number of nodes accepts the proposed block, then it becomes the next block in the blockchain.
c) **Comparison in Light of DDOS Attack**

Now let’s suppose that someone brings a DDOS attack against the blockchain using the SBFT consensus mechanism. All the malicious actor needs to do is to shut down the node that has been elected the decision-maker, and then that blockchain can’t add new blocks.

On the other hand, if a DDOS attack is to work against the Bitcoin blockchain, the attacker has to figure out which of the thousands of miners is going to win the hash calculation lottery. If the DDOS attacker shuts down one miner, there are still thousands of other miners who can be the creator of the next block.

Unlike the blockchain that uses the SBFT consensus mechanism described above, the Bitcoin blockchain is virtually impervious to DDOS attacks. The consensus mechanism used in Bitcoin is one of the main reasons that it is so difficult to attack, even by very well-funded threats, such as governments. On the other hand, maybe the blockchain you are working with doesn’t have to worry about nation-state attacks.

The choice of consensus mechanism determines the risk posture of the various potential problems that may occur in creating valid new blocks. Each risk should be examined separately to determine the resilience of the particular choice of consensus mechanism to that particular risk.

3. **Performance Issues with Consensus Mechanisms**

The choice of consensus mechanism can dramatically impact how quickly the blockchain can create new blocks and therefore the overall performance of the blockchain. As can be seen in the comparison between the Bitcoin consensus mechanism and the SBFT consensus mechanism, Bitcoin has some very significant issues with scaling up the number of records that it can handle quickly.

4. **Examples of Consensus Mechanisms**

Here are a few examples of consensus mechanisms that may be used in blockchains.

<table>
<thead>
<tr>
<th>Type of Mechanism</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proof of Work</td>
<td>In Proof of Work (PoW), all the computers in the network that are tasked with maintaining the security of the blockchain work to find a hash result below a threshold difficulty. This task is extremely repetitive and computationally expensive. The computer that finds the answer first—the proof that they have done the necessary work—is allowed to add a new block of transactions to the blockchain. The validity of the calculation is easy to confirm, as it only requires a single has calculation by the other miners. In the Bitcoin blockchain, the first miner to achieve the threshold difficulty is rewarded with a tranche of newly-minted Bitcoins, plus all of the small transaction fees users have paid to post a record on the Bitcoin blockchain.</td>
</tr>
<tr>
<td>Proof of Stake</td>
<td>In Proof of Stake (PoS), the participant’s coin stake relative to the total of all coins determines its likelihood of creating the next block. That is, each network node is linked to an address, and the more coins that address holds, the more likely it is that they will mine (or ‘stake’, in this instance) the next block. It is like a lottery: the winner is determined by chance, but the more coins (lottery tickets) they have, the greater the odds. An attacker who wants to make a fraudulent transaction would need over 50% of all coins to process the required transactions reliably; buying these would push the price up and make such an endeavor prohibitively expensive. Stakers’ rewards typically consist only of transaction fees.</td>
</tr>
<tr>
<td>Leased Proof of Stake</td>
<td>In classic PoS, holders with small balances are unlikely to stake a block—just as small miners with low hash rates are unlikely to mine a block in Bitcoin. It may be many years before a small holder is lucky enough to generate a block. This means that many holders with low balances won’t run a node, and leave maintaining the network to a limited number of larger players. Since network security is better when there are more participants, it is important to incentivize these smaller holders to take part. Leased Proof of Stake (LPoS) achieves this by allowing holders to lease their balances to staking nodes. The leased funds remain in the full control of the holder, and can be moved or spent at any time (at which point the lease ends). Leased coins increase the ‘weight’ of the staking node, increasing its chances of being allowed to add a block of transactions to the blockchain. Any rewards received are shared proportionally with the lessors.</td>
</tr>
<tr>
<td>Delegated Proof of Stake</td>
<td>With Delegated Proof of Stake (DPoS), coin holders use their balances to elect a list of nodes that will have the opportunity to stake blocks of new transactions and add them to the blockchain. This engages all coin holders, though may not reward them directly in the same way as LPoS does. Holders can also vote on changes to network parameters, giving them greater influence and ownership over the network.</td>
</tr>
<tr>
<td>Proof of Burn</td>
<td>In a Proof of Burn (PoB) mechanism, value of one digital currency is exchanged for another. A node takes part in a lottery to choose the next block by burning (i.e., destroying) other cryptocurrencies they hold, for example, Bitcoin or Ether. To locate the following block, the node transfers Bitcoin, Ether or some other digital currency to an unspent address. In return, the node gets a reward in the coins of the applicable blockchain.</td>
</tr>
<tr>
<td>Proof of Importance</td>
<td>The Proof of Importance (PoI) consensus system is based on the idea that productive network activity, not just the amount of coins, should be rewarded. The odds of staking a block are a function of a number of factors, including balance, reputation (determined by a separate purpose-designed system), and the number of transactions made to and from that address. This provides a more holistic picture of a ‘useful’ network member.</td>
</tr>
<tr>
<td>Practical Byzantine Fault Tolerant</td>
<td>In a Practical Byzantine Fault Tolerant (pBFT) model all of the nodes are ordered in a sequence with one node being the primary node (leader) and the others referred to as the backup nodes. All of the nodes within the system communicate with each other and the goal is for all of the honest nodes to come to an agreement of the state of the system through a majority. Nodes communicate with each other heavily, and not only have to prove that messages came from a specific peer node, but also need to verify that the message was not modified during transmission. For the pBFT model to work, the assumption is that the amount of malicious nodes in the network cannot simultaneously equal or exceed ( \frac{1}{3} ) of the overall nodes in the system in a given window of vulnerability. The more nodes in the system, then the more mathematically unlikely it is for a number approaching ( \frac{1}{3} ) of the overall nodes to be malicious.</td>
</tr>
<tr>
<td>Cross-Fault Tolerance</td>
<td>The Cross-Fault Tolerance (XFT) protocol assumes a powerful adversary where the adversary is able to control the compromised nodes as well as the message delivery of the entire network. Being able to tackle such a powerful adversary brings in a lot of complexity in BFT protocols and therefore makes them less efficient. XFT relaxes the assumption of the powerful adversary and solves the state machine replication problem by simplifying it and providing an efficient solution that can tolerate Byzantine faults. XFT is designed to provide correct service as long as majority of the replicas are correct and can communicate with each other synchronously.</td>
</tr>
<tr>
<td>Ripple Protocol Consensus Algorithm</td>
<td>This protocol requires each node to define a Unique Node List (UNL). The UNL comprises of other Ripple nodes that are trusted by the given node not to collude against it. Consensus in the Ripple network is achieved by each node by consulting other nodes in its UNL. Each UNL has to have a 40% overlap with other nodes in the Ripple network. Consensus happens in multiple rounds where each node collects transactions in a data structure called “candidate set” and broadcasts its candidate sets to the other nodes in its UNL. Nodes validate the transactions, vote on them and broadcast the votes. Based on the accumulated votes, each node refines its candidate set and transactions receiving the largest number of votes are passed to the next round. When a candidate set receives a super-majority of 80% of votes from all nodes in UNL, the candidate set becomes a valid block or in Ripple terms a “ledger”. This ledger is finalized and considered the “Last Closed Ledger (LCL)” and added to the Ripple blockchain by each node. Next round of consensus is started with newer transactions and pending transactions that did not make it into the last round of consensus. Consensus in the entire network is reached when each individual sub-network reaches consensus.</td>
</tr>
</tbody>
</table>
Stellar Consensus Protocol

Using a variation of the Byzantine Fault tolerance model (Federated BFT), Stellar Consensus protocol algorithm uses the concept of quorums and quorum slices. A quorum is a set of nodes sufficient to reach an agreement. A quorum slice is a subset of a quorum that can convince one particular node about agreement. An individual node can appear on multiple quorum slices. These quorum slices and quorums are based on real life business relationships between various entities thereby leveraging trust that already exists in business models. To reach consensus in the entire systems, quorums have to intersect. Overall consensus is reached globally from decisions made by individual nodes. The consensus protocol works as follows. Each node first performs initial voting on transactions, also generically considered as statements. This is the first step of the federated voting process. Each node performs its selection of statements and will never vote for another statement contradicting its selection. It can however accept a different statement if its quorum slice has accepted a different one. Second step is the acceptance step. A node accepts a statement if it has never accepted a statement contradicting the current statement and each node in its v-blocking set has accepted that statement. A v-blocking set is a set of nodes one each from a quorum slice to which the current node belongs to. Quorum slices influence one another leading to quorums that agree on a certain statement. This step is known as ratification when all members of a quorum agree on a statement. Confirmation is the final step of the voting process and signifies system level agreement. This step ensures that nodes send each other confirmation messages so that all agree upon the final value of the state in the system.

5. The Difficulty of Consensus Mechanisms

Consensus mechanisms need to be able to have those who decide what records to add to the blockchain and what blocks to add to the blockchain do the right thing in spite of possible attacks on the blockchain from participants and outsiders to the blockchain, in spite of the possibility of false information being provided, and in spite of the absence of some normally available information. They must not only be motivated to do the right thing, they must have sufficient incentives to serve in these roles. These requirements must exist throughout the life of the blockchain.

Considerations must also be given to the impact the consensus algorithms have on the performance of the blockchain, as well the relationship between the performance and security of the blockchain.

Not surprisingly, choosing an appropriate consensus mechanism will frequently require experts in game theory and mechanisms for distributed database management. It is unlikely that someone without a technical background will be able to determine whether the consensus mechanism chosen is the right one for a particular blockchain implementation. Once again, however, you can still ask the questions that help to determine whether the development team has examined the issues and risks that should be considered when choosing a consensus mechanism.

6. Questions to Ask

1. What is the process for validation of records?
2. Why was that process chosen?

3. How are disagreements as to the validity of records resolved?

4. How is consensus reached on what blocks are added to the blockchain?

5. How are disagreements as to what blocks to add to the blockchain resolved?

6. How easy is it for someone who disagrees with a record or block to fork the blockchain?

7. What is the maximum throughput of the blockchain? How will throughput change as the blockchain grows in size?

8. What amount of throughput does the blockchain need?

9. Where does the validation of records occur? On chain or off chain?

10. What incentives exist to keep those who are responsible for creating consensus to act appropriately? How will the efficacy of those incentives change over time?

11. What incentives exist to encourage those who are responsible for creating consensus to participate in the consensus process?

12. How does the consensus mechanism manage false information that may be proposed for inclusion on the blockchain?

13. How does the consensus mechanism manage the possible unavailability of portions of the blockchain nodes?

14. How does the consensus mechanism prevent malicious attacks on the blockchain itself, such as a DDOS attack?

**D. Governance**

1. **Generally**

Blockchain technologies are immature. To remain viable, they must change over time. We have also established that some or all of the following may be true for many blockchain implementations:

- They may not be owned by anyone
- They may not be controlled by anyone
- They may be easy to “fork” when people don’t like the direction that the blockchain is moving

With those factors in mind, how do you go about changing blockchains over time? Disagreements over the direction of blockchains are the reason that we have a Bitcoin blockchain and a Bitcoin Cash blockchain, an Ethereum blockchain and an Ethereum Classic blockchain.
This is further complicated by having different stakeholders. In many blockchains, especially public blockchains, the software developers, those who operate the nodes, those who determine consensus, and those who actually use the blockchain to add records may be entirely different groups of people with interests that diverge. Because traditional databases are operated by a single company, changing the technology of a traditional database is usually a straightforward task. This is not necessarily so with blockchains.

Traditional businesses are not typically faced with this kind of need for governance. Accordingly, it may be a new and strange concept to many.

2. Questions to Ask

1. How are changes to the blockchain proposed, vetted, and agreed upon?

2. Who are the stakeholders who get to decide how the blockchain will evolve? What if their interests are not aligned?

3. What is the mechanism for participation in the change process? How are they allowed to participate in the decision-making process?

4. How easy is it for a disgruntled stakeholder to fork the blockchain?

5. How much unanimity is required to modify the blockchain? How do stakeholders “vote” for or against the change?

6. Does anyone or any group have veto power over changes to the blockchain?

7. What happens if all nodes do not agree?

E. Programming

One of the more well-publicized, early failures in blockchain was the DAO. The name DAO was taken from the concept of a “decentralized autonomous organization,” whereby one could create a decentralized business organization that was not necessarily “owned” by anyone. It was created through the operation of a computer program that used the Ethereum blockchain. The Ethereum blockchain has its own cryptocurrency, Ether, which was used for making investments in the DAO.

The DAO was touted as an investment vehicle, whereby holders of the DAO token would decide how to invest the money raised. It attracted over 11,000 investors and raised the equivalent of over US$150 million in about a month. Within a month of raising that money, a vulnerability was discovered in the DAO programming, which allowed a hacker to gain control over about 1/3 of the Ether attributable to the DAO. So, a vulnerability in the computer code allowed the theft of the equivalent of over US$50 million.\footnote{For a description of the DAO and its problems, see \url{https://en.wikipedia.org/wiki/The.DAO_(organization)}, last viewed December 7, 2018.}
Many blockchains implementations use the Ethereum blockchain or other blockchains that allow for the operation of computer code on the blockchain—known as “smart contracts.” As of this writing, these smart contract platforms include Ethereum Classic, NEO, EOS, Cardano, and WAVES. Implementing smart contracts on a blockchain raises additional risks to consider.

It is very difficult to write computer code that does not have vulnerabilities, especially as the code gets longer and more complicated. The quality of a smart contract’s programming can be a critical component to the safety of the implementation. Therefore, great care should go into the development and testing of computer code that is designed to run on a blockchain.

1. Questions

• Tell me about the testing that you went through for the code that will operate on the blockchain.

• How was the smart contract code validated?

• Was any outside service used to validate or test the smart contract?

• If the smart contract has a bug in it, or if the blockchain implementation has vulnerabilities, is there a mechanism for remedying the resulting problems that may occur? If so, describe the mechanism.

• Describe how complex the smart contract code is, relative to other smart contracts on the blockchain that you are using (such as Ethereum).

• What vulnerabilities have been identified in the underlying blockchain that you are using (such as Ethereum)?

III. Conclusion

This article identifies only the most basic of technologies used in blockchain implementations. There is a lot more to blockchains generally and blockchain risks specifically than those we have described.

Blockchain is a rising tide in business, triggering a vast amount of new business opportunities. Despite its complexity, risk identification and evaluation remains a key part of the business world. Just because it’s complex doesn’t mean that risks should be ignored.

Hopefully this article will help you in your thinking about the blockchain implementations you or your clients are facing. Just because blockchain is very technical doesn’t meant that you can’t play a role in making sure that risks are identified and addressed.
Professionalism—AI & The Law

Presented By:

Al Leach  
Alston & Bird  
Atlanta, GA

Will Bracker  
Cox Communications  
Atlanta, GA
THE CHIEF JUSTICE’S COMMISSION ON PROFESSIONALISM  
(Founded 1989) 

A Brief History of the Chief Justice’s Commission on Professionalism 

Karlise Y. Grier, Executive Director

The mission of the Chief Justice’s Commission on Professionalism is to support and encourage lawyers to exercise the highest levels of professional integrity in their relationships with their clients, other lawyers, the courts and the public, and to fulfill their obligations to improve the law and legal system and to ensure access to that system.

After a series of meetings of key figures in Georgia’s legal community in 1988, in February of 1989, the Supreme Court of Georgia created the Chief Justice’s Commission on Professionalism (“Commission”), the first entity of this kind in the world created by a high court to address legal professionalism. In March of 1989, the Rules of the State Bar of Georgia were amended to lay out the purpose, members, powers and duties of the Commission. The brainchild of Justice Thomas Marshall and past Emory University President James Laney, they were joined by Justices Charles Weltner and Harold Clarke and then State Bar President A. James Elliott in forming the Commission. The impetus for this entity then and now is to address uncivil approaches to the practice of law, as many believe legal practice is departing from its traditional stance as a high calling – like medicine and the clergy – to a business.

The Commission carefully crafted a statement of professionalism, A Lawyer’s Creed and the Aspirational Statement on Professionalism, guidelines and standards addressing attorneys’ relationships with colleagues, clients, judges, law schools and the public, and retained its first executive director, Hulett “Bucky” Askew. Professionalism continuing legal education was mandated and programming requirements were developed by then assistant and second executive director Sally Evans Lockwood. During the 1990s, after the Commission conducted a series of convocations with the bench and bar to discern professionalism issues from practitioners’ views, the State Bar instituted new initiatives, such as the Committee on Inclusion in the Profession (f/k/a Women and Minorities in the Profession Committee). Then the Commission sought the concerns of the public in a series of town hall meetings held around Georgia. Two concerns raised in these meetings were: lack of civility and the economic pressures of law practice. As a result, the State Bar of Georgia established the Law Practice Management Program.

Over the years, the Commission has worked with the State Bar to establish other programs that support professionalism ideals, including the Consumer Assistance Program and the Diversity Program. In 1993, under President Paul Kilpatrick, the State Bar’s Committee on Professionalism partnered with the Commission in establishing the first Law School Orientation on Professionalism Program for incoming law students held at every Georgia law school. At one time, this program had been replicated at more than forty U.S. law schools. It engages volunteer practicing attorneys, judges and law professors with law students in small group discussions of hypothetical contemporary professionalism and ethics situations.

In 1997, the Justice Robert Benham Community Service Awards Program was initiated to recognize members of the bench and bar who have combined a professional career with outstanding service to their communities around Georgia. The honorees are recognized for voluntary participation in community organizations, government-sponsored activities, youth programs, religious activities or humanitarian work outside of their professional practice or judicial duties. This annual program is now usually held at the State Bar Headquarters in Atlanta.
In 2006, veteran attorney and former law professor, Avarita L. Hanson became the third executive director. In addition to providing multiple CLE programs for local bars, government and law offices, she served as Chair of the ABA Consortium on Professionalism Initiatives, a group that informs and vets ideas of persons interested in development of professionalism programs. She authored the chapter on *Reputation*, in Paul Haskins, Ed., *ESSENTIAL QUALITIES OF THE PROFESSIONAL LAWYER*, ABA Standing Committee on Professionalism, ABA Center for Professional Responsibility (July 2013) and recently added to the newly-released accompanying *Instructor’s Manual* (April 2017). Ms. Hanson retired in August 2017 after a distinguished career serving the Commission.

Today, the Commission, which meets three times per year, is under the direction and management of its fourth Executive Director, attorney Karlise Yvette Grier. The Commission continues to support and advise persons locally and nationally who are interested in professionalism programming. The Chief Justice of the Supreme Court of Georgia serves as the Commission’s chair, and Chief Justice Harold D. Melton currently serves in this capacity. The Commission has twenty-two members representing practicing lawyers, the state appellate and trial courts, the federal district court, all Georgia law schools and the public. (See Appendix A). In addition to the Executive Director, the Commission staff includes Tere Latala (Assistant Director) and Nneka Harris-Daniel (Administrative Assistant). With its chair, members and staff, the Commission is well equipped to fulfill its mission and to inspire and develop programs to address today’s needs of the legal profession and those concerns on the horizon. (See Appendix B).

The Commission works through committees and working groups (Access to Justice, Finance and Personnel, Continuing Legal Education, Social Media/Awareness, Financial Resources, and Benham Awards Selection) in carrying out some of its duties. It also works with other state and national entities, such as the American Bar Association’s Center for Professional Responsibility and its other groups. To keep Georgia Bar members abreast of professionalism activities and issues, the Commission maintains a website at [www.cjcpga.org](http://www.cjcpga.org). The Commission also provides content for the Professionalism Page in every issue of the *Georgia Bar Journal*. In 2018, the Commission engaged in a strategic planning process. As a result of that process, the Commission decided to focus on four priority areas for the next three to five years: 1) ensuring high quality professionalism CLE programming that complies with CJCP guidelines; 2) promoting the understanding and exercise of professionalism and emphasizing its importance to the legal system; 3) promoting meaningful access to the legal system and services; and 4) ensuring that CJCP resources are used effectively, transparently and consistent with the mission.

After 29 years, the measure of effectiveness of the Commission should ultimately rest in the actions, character and demeanor of every Georgia lawyer. Because there is still work to do, the Commission will continue to lead the movement and dialogue on legal professionalism.
THE MEANING OF PROFESSIONALISM

The three ancient learned professions were the law, medicine, and ministry. The word profession comes from the Latin *professus*, meaning to have affirmed publicly. As one legal scholar has explained, “The term evolved to describe occupations that required new entrants to take an oath professing their dedication to the ideals and practices associated with a learned calling.”

Many attempts have been made to define a profession in general and lawyer professionalism in particular. The most commonly cited is the definition developed by the late Dean Roscoe Pound of Harvard Law School:

> The term refers to a group . . . pursuing a learned art as a common calling in the spirit of public service - no less a public service because it may incidentally be a means of livelihood. Pursuit of the learned art in the spirit of a public service is the primary purpose.

Thinking about professionalism and discussing the values it encompasses can provide guidance in the day-to-day practice of law. Professionalism is a wide umbrella of values encompassing competence, character, civility, commitment to the rule of law, to justice and to the public good. Professionalism calls us to be mindful of the lawyer’s roles as officer of the court, advocate, counselor, negotiator, and problem solver. Professionalism asks us to commit to improvement of the law, the legal system, and access to that system. These are the values that make us a profession enlisted in the service not only of the client but of the public good as well. While none of us achieves perfection in serving these values, it is the consistent aspiration toward them that defines a professional. The Commission encourages thought not only about the lawyer-client relationship central to the practice of law but also about how the legal profession can shape us as people and a society.

BACKGROUND ON THE LEGAL PROFESSIONALISM MOVEMENT IN GEORGIA

In 1986, the American Bar Association ruefully reported that despite the fact that lawyers’ observance of the rules of ethics governing their conduct is sharply on the rise, lawyers’ professionalism, by contrast, may well be in steep decline:

---

[Although] lawyers have tended to take the rules more seriously because of an increased fear of disciplinary prosecutions and malpractice suits, . . . [they] have also tended to look at nothing but the rules; if conduct meets the minimum standard, lawyers tend to ignore exhortations to set their standards at a higher level.3

The ABA’s observation reflects a crucial distinction: while a canon of ethics may cover what is minimally required of lawyers, “professionalism” encompasses what is more broadly expected of them – both by the public and by the best traditions of the legal profession itself.

In response to these challenges, the State Bar of Georgia and the Supreme Court of Georgia embarked upon a long-range project – to raise the professional aspirations of lawyers in the state. Upon taking office in June 1988, then State Bar President A. James Elliott gave Georgia’s professionalism movement momentum when he placed the professionalism project at the top of his agenda. In conjunction with Chief Justice Marshall, President Elliott gathered 120 prominent judges and lawyers from around the state to attend the first Annual Georgia Convocation on Professionalism.

For its part, the Georgia Supreme Court took three important steps to further the professionalism movement in Georgia. First, at the first Convocation, the Supreme Court of Georgia announced and administered to those present a new Georgia attorney’s oath emphasizing the virtue of truthfulness, reviving language dating back to 1729. (See also Appendix C). Second, as a result of the first Convocation, in 1989, the Supreme Court of Georgia took two additional significant steps to confront the concerns and further the aspirations of the profession. First, it created the Chief Justice’s Commission on Professionalism (the “Commission”) and gave it a primary charge of ensuring that the practice of law in this state remains a high calling, enlisted in the service not only of the client, but of the public good as well. This challenging mandate was supplemented by the Court’s second step, that of amending the mandatory continuing legal education (CLE) rule to require all active Georgia lawyers to complete one hour of Professionalism CLE each year [Rule 8-104 (B)(3) of the Rules and Regulations for the Organization and Government of the State Bar of Georgia and Regulation (4) thereunder].

GENERAL PURPOSE OF CLE PROFESSIONALISM CREDIT

Beginning in 1990, the Georgia Supreme Court required all active Georgia lawyers to complete one hour of Professionalism CLE each year [Rule 8-104 (B)(3) of the Rules and Regulations for the Organization and Government of the State Bar of Georgia and Regulation (4) thereunder]. The one hour of Professionalism CLE is distinct from and in addition to the required ethics CLE. The general goal of the Professionalism CLE requirement is to create a

forum in which lawyers, judges and legal educators can explore the meaning and aspirations of professionalism in contemporary legal practice and reflect upon the fundamental premises of lawyer professionalism – competence, character, civility, commitment to the rule of law, to justice, and to the public good. Building a community among the lawyers of this state is a specific goal of this requirement.

DISTINCTION BETWEEN ETHICS AND PROFESSIONALISM

The Supreme Court has distinguished between ethics and professionalism, to the extent of creating separate one-hour CLE requirements for each. The best explanation of the distinction between ethics and professionalism that is offered by former Chief Justice Harold Clarke of the Georgia Supreme Court:

“. . . the idea is that ethics is a minimum standard which is required of all lawyers, while professionalism is a higher standard expected of all lawyers.”

Laws and the Rules of Professional Conduct establish minimal standards of consensus impropriety; they do not define the criteria for ethical behavior. In the traditional sense, persons are not “ethical” simply because they act lawfully or even within the bounds of an official code of ethics. People can be dishonest, unprincipled, untrustworthy, unfair, and uncaring without breaking the law or the code. Truly ethical people measure their conduct not by rules but by basic moral principles such as honesty, integrity and fairness.

The term “Ethics” is commonly understood in the CLE context to mean “the law of lawyering” and the rules by which lawyers must abide in order to remain in good standing before the bar. Legal Ethics CLE also includes malpractice avoidance. “Professionalism” harkens back to the traditional meaning of ethics discussed above. The Commission believes that lawyers should remember in counseling clients and determining their own behavior that the letter of the law is only a minimal threshold describing what is legally possible, while professionalism is meant to address the aspirations of the profession and how we as lawyers should behave. Ethics discussions tend to focus on misconduct -- the negative dimensions of lawyering. Professionalism discussions have an affirmative dimension -- a focus on conduct that preserves and strengthens the dignity, honor, and integrity of the legal system.

As former Chief Justice Benham of the Georgia Supreme Court says, “We should expect more of lawyers than mere compliance with legal and ethical requirements.”

ISSUES AND TOPICS

In March of 1990, the Chief Justice’s Commission adopted A Lawyer’s Creed (See Appendix D) and an Aspirational Statement on Professionalism (See Appendix E). These two documents should serve as the beginning points for professionalism discussions, not because they are to be imposed upon Georgia lawyers or bar associations, but because they serve as
words of encouragement, assistance and guidance. These comprehensive statements should be utilized to frame discussions and remind lawyers about the basic tenets of our profession.

Specific topics that can be used as subject matter to provide context for a Professionalism CLE include:

- Access to Justice
- Administration of Justice
- Advocacy - effective persuasive advocacy techniques for trial, appellate, and other representation contexts
- Alternative Dispute Resolution - negotiation, settlement, mediation, arbitration, early neutral evaluation, other dispute resolution processes alternative to litigation
- Billable Hours
- Civility
- Client Communication Skills
- Client Concerns and Expectations
- Client Relations Skills
- Commercial Pressures
- Communication Skills (oral and written)
- Discovery - effective techniques to overcome misuse and abuse
- Diversity and Inclusion Issues - age, ethnic, gender, racial, sexual orientation, socioeconomic status
- Law Practice Management - issues relating to development and management of a law practice including client relations and technology to promote the efficient, economical and competent delivery of legal services.

Practice Management CLE includes, but is not limited to, those activities which (1) teach lawyers how to organize and manage their law practices so as to promote the efficient, economical and competent delivery of legal services; and (2) teach lawyers how to create and maintain good client relations consistent with existing ethical and professional guidelines so as to eliminate malpractice claims and bar grievances while improving service to the client and the public image of the profession.

- Mentoring
- Proficiency and clarity in oral, written, and electronic communications - with the court, lawyers, clients, government agencies, and the public
- Public Interest
- Quality of Life Issues - balancing priorities, career/personal transition, maintaining emotional and mental health, stress management, substance abuse, suicide prevention, wellness
- Responsibility for improving the administration of justice
- Responsibility to ensure access to the legal system
• Responsibility for performing community, public and pro bono service
• Restoring and sustaining public confidence in the legal system, including courts, lawyers, the systems of justice

Roles of Lawyers
  - The Lawyer as Advocate
  - The Lawyer as Architect of Future Conduct
  - The Lawyer as Consensus Builder
  - The Lawyer as Counselor
  - The Lawyer as Hearing Officer
  - The Lawyer as In-House Counsel
  - The Lawyer as Judge (or prospective judge)
  - The Lawyer as Negotiator
  - The Lawyer as Officer of the Court
  - The Lawyer as Problem Solver
  - The Lawyer as Prosecutor
  - The Lawyer as Public Servant

• Satisfaction in the Legal Profession
• Sexual Harassment
• Small Firms/Solo Practitioners

Karl N. Llewellyn, jurisprudential scholar who taught at Yale, Columbia, and the University of Chicago Law Schools, often cautioned his students:

The lawyer is a man of many conflicts. More than anyone else in our society, he must contend with competing claims on his time and loyalty. You must represent your client to the best of your ability, and yet never lose sight of the fact that you are an officer of the court with a special responsibility for the integrity of the legal system. You will often find, brethren and sistern, that those professional duties do not sit easily with one another. You will discover, too, that they get in the way of your other obligations – to your conscience, your God, your family, your partners, your country, and all the other perfectly good claims on your energies and hearts. You will be pulled and tugged in a dozen directions at once. You must learn to handle those conflicts.4

The real issue facing lawyers as professionals is developing the capacity for critical and reflective judgment and the ability to “handle those conflicts,” described by Karl Llewellyn. A major goal of Professionalism CLE is to encourage introspection and dialogue about these issues.

4 MARY ANN GLENDON, A NATION UNDER LAWYERS 17 (1994)
CHIEF JUSTICE’S COMMISSION ON PROFESSIONALISM

Harold D. Melton, Chief Justice
Supreme Court of Georgia

Karlise Y. Grier
Executive Director

Terie Latala
Assistant Director

Nneka Harris-Daniel
Administrative Assistant

APPENDICES

A – 2018-2019 COMMISSION MEMBERS

B – MISSION STATEMENT

C – OATH OF ADMISSION

D – A LAWYER’S CREED

E – ASPIRATIONAL STATEMENT ON PROFESSIONALISM

F – SELECT PROFESSIONALISM PAGE ARTICLES

Suite 620 • 104 Marietta Street, NW • Atlanta, Georgia 30303
(404) 225-5040 • professionalism@cjcpga.org • www.cjcpga.org
APPENDIX A

CHIEF JUSTICE’S COMMISSION ON PROFESSIONALISM

2018 - 2019

Members
The Honorable Harold D. Melton (Chair), Atlanta
Professor Nathan S. Chapman, Athens
Professor Clark D. Cunningham, Atlanta
The Honorable J. Antonio DelCampo, Atlanta
Mr. Gerald M. Edenfield, Statesboro
The Honorable Susan E. Edlein, Atlanta
Ms. Elizabeth L. Fite, Decatur
Ms. Rebecca Grist, Macon
Associate Dean Sheryl Harrison-Mercer, Atlanta
Mr. Kenneth B. Hodges III, Atlanta
The Honorable Steve C. Jones, Atlanta
The Honorable Meng H. Lim, Tallapoosa
Professor Patrick E. Longan, Macon
Ms. Maria Mackay, Watkinsville
The Honorable Carla W. McMillian, Atlanta
The Honorable Rizza O’Connor, Lyons
Ms. Claudia S. Saari, Decatur
Ms. Adwoa Gharney-Tagoe Seymour, Atlanta
Assistant Dean Rita A. Sheffley, Atlanta
Ms. Nicki Noel Vaughan, Gainesville
Mr. R. Kyle Williams, Decatur
Dr. Monica L. Willis-Parker, Stone Mountain

Advisors
The Honorable Robert Benham, Atlanta
Ms. Jennifer M. Davis, Atlanta
Professor Roy M. Sobelson, Atlanta

LIAISONS
Mr. Robert Arrington, Atlanta
Mr. Jeffrey R. Davis, Atlanta
Ms. Paula J. Frederick, Atlanta
Professor Nicole G. Iannarone, Atlanta
Ms. Tanglea S. King, Atlanta
Ms. Michelle E. West, Atlanta
Ms. DeeDee Worley, Atlanta

Staff
Ms. Karlise Y. Grier, Atlanta
Ms. Terie Latala, Atlanta
Ms. Nneka Harris-Daniel, Atlanta

Italics denotes public member/non-lawyer
APPENDIX B

MISSION STATEMENT

The mission of the Chief Justice’s Commission on Professionalism is to support and encourage lawyers to exercise the highest levels of professional integrity in their relationships with their clients, other lawyers, the courts, and the public and to fulfill their obligations to improve the law and the legal system and to ensure access to that system.

CALLING TO TASKS

The Commission seeks to foster among lawyers an active awareness of its mission by calling lawyers to the following tasks, in the words of former Chief Justice Harold Clarke:

1. To recognize that the reason for the existence of lawyers is to act as problem solvers performing their service on behalf of the client while adhering at all times to the public interest;

2. To utilize their special training and natural talents in positions of leadership for societal betterment;

3. To adhere to the proposition that a social conscience and devotion to the public interest stand as essential elements of lawyer professionalism.
APPENDIX C

HISTORICAL INFORMATION ABOUT THE COMMISSION’S ROLES IN THE DEVELOPMENT OF THE CURRENT GEORGIA ATTORNEY OATH

In 1986, Emory University President James T. Laney delivered a lecture on “Moral Authority in the Professions.” While expressing concern about the decline in moral authority of all the professions, he focused on the legal profession because of the respect and confidence in which it has traditionally been held and because it has been viewed as serving the public in unique and important ways. Dr. Laney expressed the fear that the loss of moral authority has as serious a consequence for society at large as it does for the legal profession.

For its part, the Georgia Supreme Court took an important step to further the professionalism movement in Georgia. At the first convocation on professionalism, the Court announced and administered to those present a new Georgia attorney’s oath emphasizing the virtue of truthfulness, reviving language dating back to 1729. Reflecting the idea that the word “profession” derives from a root meaning “to avow publicly,” this new oath of admission to the State Bar of Georgia indicates that whatever other expectations might be made of lawyers, truth-telling is expected, always and everywhere, of every true professional. Since the convocation, the new oath has been administered to thousands of lawyers in circuits all over the state.

<table>
<thead>
<tr>
<th>Attorney’s Oath</th>
</tr>
</thead>
<tbody>
<tr>
<td>I,_______, swear that I will truly and honestly, justly, and uprightly demean myself, according to the laws, as an attorney, counselor, and solicitor, and that I will support and defend the Constitution of the United States and the Constitution of the State of Georgia. So help me God.</td>
</tr>
</tbody>
</table>

In 2002, at the request of then-State Bar President George E. Mundy, the Committee on Professionalism was asked to revise the Oath of Admission to make the wording more relevant to the current practice of law, while retaining the original language calling for lawyers to “truly and honestly, justly and uprightly” conduct themselves. The revision was approved by the Georgia Supreme Court in 2002.
APPENDIX C

OATH OF ADMISSION
TO THE STATE BAR OF GEORGIA

“I,___________________, swear that I will truly and honestly, justly and uprightly conduct myself as a member of this learned profession and in accordance with the Georgia Rules of Professional Conduct, as an attorney and counselor and that I will support and defend the Constitution of the United States and the Constitution of the State of Georgia. So help me God.”

As revised by the Supreme Court of Georgia, April 20, 2002
APPENDIX D

A LAWYER’S CREED

To my clients, I offer faithfulness, competence, diligence, and good judgment. I will strive to represent you as I would want to be represented and to be worthy of your trust.

To the opposing parties and their counsel, I offer fairness, integrity, and civility. I will seek reconciliation and, if we fail, I will strive to make our dispute a dignified one.

To the courts, and other tribunals, and to those who assist them, I offer respect, candor, and courtesy. I will strive to do honor to the search for justice.

To my colleagues in the practice of law, I offer concern for your welfare. I will strive to make our association a professional friendship.

To the profession, I offer assistance. I will strive to keep our business a profession and our profession a calling in the spirit of public service.

To the public and our systems of justice, I offer service. I will strive to improve the law and our legal system, to make the law and our legal system available to all, and to seek the common good through the representation of my clients.

Entered by Order of Supreme Court of Georgia, October 9, 1992, nunc pro tunc July 3, 1990; Part IX of the Rules and Regulations of the State Bar of Georgia, as amended September 10, 2003 and April 26, 2013
APPENDIX E

ASPIRATIONAL STATEMENT ON PROFESSIONALISM

The Court believes there are unfortunate trends of commercialization and loss of professional community in the current practice of law. These trends are manifested in an undue emphasis on the financial rewards of practice, a lack of courtesy and civility among members of our profession, a lack of respect for the judiciary and for our systems of justice, and a lack of regard for others and for the common good. As a community of professionals, we should strive to make the internal rewards of service, craft, and character, and not the external reward of financial gain, the primary rewards of the practice of law. In our practices we should remember that the primary justification for who we are and what we do is the common good we can achieve through the faithful representation of people who desire to resolve their disputes in a peaceful manner and to prevent future disputes. We should remember, and we should help our clients remember, that the way in which our clients resolve their disputes defines part of the character of our society and we should act accordingly.

As professionals, we need aspirational ideals to help bind us together in a professional community. Accordingly, the Court issues the following Aspirational Statement setting forth general and specific aspirational ideals of our profession. This statement is a beginning list of the ideals of our profession. It is primarily illustrative. Our purpose is not to regulate, and certainly not to provide a basis for discipline, but rather to assist the Bar’s efforts to maintain a professionalism that can stand against the negative trends of commercialization and loss of community. It is the Court’s hope that Georgia’s lawyers, judges, and legal educators will use the following aspirational ideals to reexamine the justifications of the practice of law in our society and to consider the implications of those justifications for their conduct. The Court feels that enhancement of professionalism can be best brought about by the cooperative efforts of the organized bar, the courts, and the law schools with each group working independently, but also jointly in that effort.

Entered by Order of Supreme Court of Georgia, October 9, 1992; nunc pro tunc July 3, 1990; Part IX of the Rules and Regulations of the State Bar of Georgia, as amended September 10, 2003 and April 26, 2013
APPENDIX E

GENERAL ASPIRATIONAL IDEALS

As a lawyer, I will aspire:

(a) To put fidelity to clients and, through clients, to the common good, before selfish interests.

(b) To model for others, and particularly for my clients, the respect due to those we call upon to resolve our disputes and the regard due to all participants in our dispute resolution processes.

(c) To avoid all forms of wrongful discrimination in all of my activities including discrimination on the basis of race, religion, sex, age, handicap, veteran status, or national origin. The social goals of equality and fairness will be personal goals for me.

(d) To preserve and improve the law, the legal system, and other dispute resolution processes as instruments for the common good.

(e) To make the law, the legal system, and other dispute resolution processes available to all.

(f) To practice with a personal commitment to the rules governing our profession and to encourage others to do the same.

(g) To preserve the dignity and the integrity of our profession by my conduct. The dignity and the integrity of our profession is an inheritance that must be maintained by each successive generation of lawyers.

(h) To achieve the excellence of our craft, especially those that permit me to be the moral voice of clients to the public in advocacy while being the moral voice of the public to clients in counseling. Good lawyering should be a moral achievement for both the lawyer and the client.

(i) To practice law not as a business, but as a calling in the spirit of public service.
APPENDIX E

SPECIFIC ASPIRATIONAL IDEALS

As to clients, I will aspire:

(a) To expeditious and economical achievement of all client objectives.

(b) To fully informed client decision-making.
   As a professional, I should:
   (1) Counsel clients about all forms of dispute resolution;
   (2) Counsel clients about the value of cooperation as a means towards the productive resolution of disputes;
   (3) Maintain the sympathetic detachment that permits objective and independent advice to clients;
   (4) Communicate promptly and clearly with clients; and,
   (5) Reach clear agreements with clients concerning the nature of the representation.

(c) To fair and equitable fee agreements.
   As a professional, I should:
   (1) Discuss alternative methods of charging fees with all clients;
   (2) Offer fee arrangements that reflect the true value of the services rendered;
   (3) Reach agreements with clients as early in the relationship as possible;
   (4) Determine the amount of fees by consideration of many factors and not just time spent by the attorney;
   (5) Provide written agreements as to all fee arrangements; and,
   (6) Resolve all fee disputes through the arbitration methods provided by the State Bar of Georgia.

(d) To comply with the obligations of confidentiality and the avoidance of conflicting loyalties in a manner designed to achieve the fidelity to clients that is the purpose of these obligations.

As to opposing parties and their counsel, I will aspire:

(a) To cooperate with opposing counsel in a manner consistent with the competent representation of all parties.
   As a professional, I should:
   (1) Notify opposing counsel in a timely fashion of any cancelled appearance;
(2) Grant reasonable requests for extensions or scheduling changes; and,
(3) Consult with opposing counsel in the scheduling of appearances, meetings, and depositions.

(b) To treat opposing counsel in a manner consistent with his or her professional obligations and consistent with the dignity of the search for justice.

As a professional, I should:
(1) Not serve motions or pleadings in such a manner or at such a time as to preclude opportunity for a competent response;
(2) Be courteous and civil in all communications;
(3) Respond promptly to all requests by opposing counsel;
(4) Avoid rudeness and other acts of disrespect in all meetings including depositions and negotiations;
(5) Prepare documents that accurately reflect the agreement of all parties; and,
(6) Clearly identify all changes made in documents submitted by opposing counsel for review.

As to the courts, other tribunals, and to those who assist them, I will aspire:

(a) To represent my clients in a manner consistent with the proper functioning of a fair, efficient, and humane system of justice.

As a professional, I should:
(1) Avoid non-essential litigation and non-essential pleading in litigation;
(2) Explore the possibilities of settlement of all litigated matters;
(3) Seek non-coerced agreement between the parties on procedural and discovery matters;
(4) Avoid all delays not dictated by a competent presentation of a client’s claims;
(5) Prevent misuses of court time by verifying the availability of key participants for scheduled appearances before the court and by being punctual; and,
(6) Advise clients about the obligations of civility, courtesy, fairness, cooperation, and other proper behavior expected of those who use our systems of justice.
APPENDIX E

(b) To model for others the respect due to our courts.
As a professional I should:
(1) Act with complete honesty;
(2) Know court rules and procedures;
(3) Give appropriate deference to court rulings;
(4) Avoid undue familiarity with members of the judiciary;
(5) Avoid unfounded, unsubstantiated, or unjustified public criticism of members of the judiciary;
(6) Show respect by attire and demeanor;
(7) Assist the judiciary in determining the applicable law; and,
(8) Seek to understand the judiciary’s obligations of informed and impartial decision-making.

As to my colleagues in the practice of law, I will aspire:

(a) To recognize and to develop our interdependence;
(b) To respect the needs of others, especially the need to develop as a whole person; and,
(c) To assist my colleagues become better people in the practice of law and to accept their assistance offered to me.

As to our profession, I will aspire:

(a) To improve the practice of law.
As a professional, I should:
(1) Assist in continuing legal education efforts;
(2) Assist in organized bar activities; and,
(3) Assist law schools in the education of our future lawyers.
(b) To protect the public from incompetent or other wrongful lawyering.
As a professional, I should:
(1) Assist in bar admissions activities;
(2) Report violations of ethical regulations by fellow lawyers; and,
(3) Assist in the enforcement of the legal and ethical standards imposed upon all lawyers.

Entered by Order of Supreme Court of Georgia, October 9, 1992, nunc pro tunc July 3, 1990; Part IX of the Rules and Regulations of the State Bar of Georgia, as amended September 10, 2003 and April 26, 2013
APPENDIX E

As to the public and our systems of justice, I will aspire:

(a) To counsel clients about the moral and social consequences of their conduct.

(b) To consider the effect of my conduct on the image of our systems of justice including the social effect of advertising methods.

As a professional, I should ensure that any advertisement of my services:
(1) is consistent with the dignity of the justice system and a learned profession;
(2) provides a beneficial service to the public by providing accurate information about the availability of legal services;
(3) educates the public about the law and legal system;
(4) provides completely honest and straightforward information about my qualifications, fees, and costs; and,
(5) does not imply that clients’ legal needs can be met only through aggressive tactics.

(c) To provide the pro bono representation that is necessary to make our system of justice available to all.

(d) To support organizations that provide pro bono representation to indigent clients.

(e) To improve our laws and legal system by, for example:

(1) Serving as a public official;
(2) Assisting in the education of the public concerning our laws and legal system;
(3) Commenting publicly upon our laws; and,
(4) Using other appropriate methods of effecting positive change in our laws and legal system.

Entered by Order of Supreme Court of Georgia, October 9, 1992, nunc pro tunc July 3, 1990; Part IX of the Rules and Regulations of the State Bar of Georgia, as amended September 10, 2003 and April 26, 2013
APPENDIX F

SELECT PROFESSIONALISM PAGE ARTICLES
The Importance of Lawyers Abandoning the Shame and Stigma of Mental Illness

One tenet of the Chief Justice’s Commission on Professionalism’s “A Lawyer’s Creed” is “To my colleagues in the practice of law, I offer concern for your welfare.” If you are aware of a colleague that may be experiencing difficulties, ask questions and offer to help them contact the Lawyer Assistance Program for help.

BY MICHELLE BARCLAY

January is the month when Robin Nash, my dear friend and lawyer colleague, godfather to my child, officiate for my brother’s marriage and former director of the Barton Center at Emory University, left the world. Positive reminders of him are all around, including a child law and policy fellowship in his name, but January is a tough month.

Robin’s suicide, 12 years ago, was a shock to me. As time passed and I heard stories about Robin from others who knew him and I learned more about suicide, I can see in hindsight the risk looming for him. Today, I think his death was possibly preventable.

In 2006, Robin wrote this essay about himself for Emory’s website: “Robin Nash, age 53, drew his first breath, attended college and law school and now works at Emory University. He loves to travel to places like Southeast Asia and the Middle East but he always returns home to Emory and his hometown of Decatur. Robin majored in Economics and Mathematics. He began his law practice in 1980 in Decatur surviving mostly on court appointed cases for mentally ill patients in commitment hearings.

His practice expanded to working with institutionalized developmentally delayed clients, special education cases, wills and estate litigation and representing banks in the hugely interesting area of commercial real estate closings.

In 1995, he was appointed as a juvenile court judge in DeKalb County. He resigned from the bench effective December 2005. He sold most of his personal belongings, paid off his remaining debts and moved overseas to think and travel. After thinking and traveling for three months, he returned to the active world of Decatur. He was appointed director of the Barton Clinic effective April 15, 2006.”

When Robin came back from traveling, he told his friends—“I can be more impactful here.”—which was and is true. Robin’s impact continues today through the work of young lawyers serving as Robin Nash Fellows and through the lives of the thousands of mothers, fathers, daughters and sons he touched, helping people traumatized by child abuse, neglect, addiction and crime.

He was impactful in part because he had so much empathy for others. He was...
well regarded and well loved. He was a person you could count on who did extraordinary things for others—helping a student obtain a TPO in the middle of the night to stop a stalker; quietly helping a refugee family get stable and connected to services; and of course, his constant care of his friend Vinny. Vinny was a severely disabled adult Robin befriended and with whom he had a deep connection. Because he was a lawyer, Robin was able to help Vinny obtain full access to available medical services without being institutionalized.

So why did Robin leave? He lost his battle with mental illness. He masked it well and as a private person, did not share his struggles. His friends had some insight into his struggles but it was always complicated. While a judge, Robin was known for saying things like, “I am a manager of misery” or “I manage the competition not to serve the most vulnerable families and children.” But he also said, “Talk like this is just dark humor which is a useful coping mechanism for an emotionally draining job.”

I know today that a low serotonin level in his body was dangerous for his depression and that the medications he took waxed and waned in effectiveness. I also now know that he had not slept well for days before he acted. We’d had a meeting the day before he died where he made a long to do list. Who makes a long to do list when one is contemplating suicide? Plenty of people, I have learned. I saw that to do list on his table when I was in his apartment after his death.

What could have helped? Abandoning the shame and stigma of mental illness is a good start. I have been heartened by the social movement campaign, Time to Change, designed to help people speak up about mental illness. A safety plan shared with a reasonably wide network of people can also help. Antidepressant medications can help. Recent studies about anti-depression drugs “puts to bed the controversy on anti-depressants, clearly showing that these drugs do work in lifting mood and helping most people with depression.” Science is advancing better treatments at a rapid pace. And some experts advise that directly asking whether a person has considered killing themselves can open the door to intervention and saving a life.

Before becoming a lawyer, I worked as a nurse in a variety of settings at both Grady and Emory hospitals. I saw attempted suicides. I witnessed a number of those people who were grateful they were not successful. I saw safety plans work when enough people knew about the risks. Sometimes, medicines were changed, new treatments tried and I saw people get better.

I feel like with my background I could have and should have probed Robin more. But at the time, I thought I was respecting his privacy by not asking too many questions. Today I know that a person can be fine one day and then chemicals in their brain can wildly change within 24 hours, and they’re no longer ok. I learned that not sleeping can be deadly. I have also learned that just talking about it can help a person cope.

A book that has helped me is called Stay: A History of Suicide and the Philosophy Against It,” by Jennifer Michael Hecht. If I had a second chance, I would try to use some of the arguments in that book, such as:

None of us can truly know what we mean to other people, and none of us can know what our future self will experience. History and philosophy ask us to remember these mysteries, to look around at friends, family, humanity, at the surprising life brings—the endless possibilities that living offers—and to persevere.

Of course, first I would have just asked about his mental health with love and listened. I still wish for that chance to try.

Afterword by Chief Justices Commission on Professionalism Executive Director Karliae Yvette Grier: One tenet of the Chief Justices Commission on Professionalism “A Lawyer’s Creed” is “Tony colleagues in the practice are aware of a colleague that may be experiencing a challenging time and take action to help them contact the Lawyer Assistance Program for help.

Counseling for Attorneys

- Depression
- Anxiety/Stress
- Life Transitions
- Career Concerns
- Couples Counseling
- Relationship Conflicts

Elizabeth Mehlman, J.D., Ph.D.
www.AtlantaPsychologist.org
(404) 874-0937
Midtown Atlanta

Michelle and Andy Barday are so grateful to the Emory University community for the grace and care that surrounded everyone, especially the students when Robin died.

Michelle Barclay, J.D., has more than 20 years experience working in Georgia’s judicial branch. She is currently the division director of Communications, Children, Families, and the Courts within the Judicial Council of Georgia’s Administrative Office of the Courts. Before becoming a lawyer, she was a nurse for 10 years, specializing in ICU and trauma care. Her degrees include a Juris Doctor from Emory University School of Law, a Bachelor of Science in Nursing from Emory University and a Bachelor of Interdisciplinary Studies from Georgia State University. She is also co-founder along with her husband Andrew Barclay of the Barton Child Law and Policy Center at Emory University School of Law. She can be reached at 404-657-9219 or michelle.barclay@georgiacourts.gov.

Endnotes

Promoting a Professional Culture of Respect and Safety #MeToo

In keeping with our professionalism aspirations, I challenge you to take a proactive, preventative approach to sexual harassment and to start the discussions ... about things we as lawyers can do to promote a professional culture of respect and safety to prevent #MeToo.

BY KARLISE Y. GRIER

“There is no doubt that Marley was dead. This must be distinctly understood, or nothing wonderful can come of the story I am going to relate.”—Excerpt from: “A Christmas Carol” by Charles Dickens.

To borrow an idea from an iconic writer: There is no doubt that #MeToo testimonials are real. This must be distinctly understood, or nothing wonderful can come of the ideas I am going to share.

I start with this statement because when I co-presented on behalf of the Chief Justice’s Commission on Professionalism at a two-hour seminar on Ethics, Professionalism and Sexual
Harassment at the University of Georgia (UGA) in March 2018, it was clear to me that men and women, young and old, question some of the testimonials of sexual harassment that have recently come to light. For the purposes of starting a discussion about preventing future #MeToo incidents in the Georgia legal profession, I ask you to assume, arguendo, that sexual harassment does occur and to further assume, arguendo, that it occurs in Georgia among lawyers and judges. Our attention and discussion must therefore turn to “How do we prevent it?” We won’t expend needless energy on “Is he telling the truth?” We won’t lament, “Why did she wait so long to come forward?”

First, I want to explain why I believe that sexual harassment in the legal profession is, in part, a professionalism issue. As Georgia lawyers, we have A Lawyer’s Creed and an Aspirational Statement on Professionalism that was approved by the Supreme Court of Georgia in 1990. One tenet of A Lawyer’s Creed states: “To my colleagues in the practice of law, I offer concern for your welfare. I will strive to make our association a professional friendship.”

Frankly, it is only a concern for the welfare of others that in many cases will prevent sexual harassment in the legal profession because of “gaps” in the law and in our ethics rules. For example, under federal law, sexual harassment is a form of sex discrimination that violates Title VII of the Civil Rights Act of 1964. Title VII applies to employers with 15 or more employees. According to a 2016 article on lawyer demographics, three out of four lawyers are working in a law firm that has two to five lawyers working for it. In Georgia, there are no state laws similar to Title VII’s statutory scheme.

There is currently nothing in Georgia’s Rules of Professional Conduct that explicitly prohibits sexual harassment of a lawyer by another lawyer. Moreover, it is my understanding that generally the Office of the General Counsel will not prosecute a lawyer for alleged lawyer-on-lawyer sexual harassment absent a misdemeanor or felony criminal conviction, involving rape, sexual assault, battery, moral turpitude and other similar criminal behavior. Other circumstances in which laws or ethics rules may not apply include sexual harassment of lawyers by clients or sexual harassment that occurs during professional events, such as bar association meetings or continuing education seminars.

Former Georgia Chief Justice Harold Clarke described the distinction between ethics and professionalism as . . . the idea that ethics is a minimum standard which is required of all lawyers while professionalism is a higher standard expected of all lawyers. Therefore, in the absence of laws and ethical rules to guide our behavior, professionalism aspirations call on Georgia lawyers to consider and implement a professional culture of respect and safety that ensures zero tolerance for behavior that gives rise to #MeToo testimonials.


Former Georgia Chief Justice Harold Clarke described the distinction between ethics and professionalism as . . . the idea that ethics is a minimum standard which is required of all lawyers while professionalism is a higher standard expected of all lawyers.
practical advice for legal employers to address or to prevent sexual harassment. Some of the suggestions included: establishing easy and inexpensive ways to detect sexual harassment, such as asking about it in anonymous employee surveys and/or exit interviews; not waiting for formal complaints before responding to known misconduct; and discussing the existence of sexual harassment openly. The federal judiciary's working group on sexual harassment has many reforms that are currently underway, such as conducting a session on sexual harassment during the ethics training for newly appointed judges; reviewing the confidentiality provisions in several employee/law clerk handbooks to clarify that nothing in the provisions prevents the filing of a complaint; and clarifying the data that the judiciary collects about judicial misconduct complaints to add a category for any complaints filed relating to sexual misconduct. For those planning CLE or for any complaints filed relating to sexual misconduct to add a category of a complaint; and clarifying the data in the provisions prevents the filing clerk handbooks to clarify that nothing provisions in several employee/law judges; reviewing the confidentiality the ethics training for newly appointed a session on sexual harassment during are currently underway, such as conducting The federal judiciary's working group on sexual harassment openly. The federal judiciary's working group on sexual harassment openly.10 Some of the suggestions included: establishing easy and inexpensive ways to detect sexual harassment, such as asking about it in anonymous employee surveys and/or exit interviews; not waiting for formal complaints before responding to known misconduct; and discussing the existence of sexual harassment openly.10 The federal judiciary's working group on sexual harassment has many reforms that are currently underway, such as conducting a session on sexual harassment during the ethics training for newly appointed judges; reviewing the confidentiality provisions in several employee/law clerk handbooks to clarify that nothing in the provisions prevents the filing of a complaint; and clarifying the data that the judiciary collects about judicial misconduct complaints to add a category for any complaints filed relating to sexual misconduct. For those planning CLE or for any complaints filed relating to sexual misconduct to add a category of a complaint; and clarifying the data in the provisions prevents the filing clerk handbooks to clarify that nothing provisions in several employee/law judges; reviewing the confidentiality the ethics training for newly appointed a session on sexual harassment during are currently underway, such as conducting The federal judiciary's working group on sexual harassment openly.10

Endnotes
5. The Georgia Code of Judicial Conduct differs from the Georgia Rules of Professional Conduct in that Rule 2.3 (b) of the Code of Judicial Conduct specifically prohibits discrimination by a judge in the performance of his or her judicial duties. See https://
Big Data Monetization

Presented By:

Moderator: Theodore F. “Ted” Claypoole
Womble Bond Dickinson (US) LLP
Atlanta, GA

Panelists:
Forrest Pace
AIG
Atlanta, GA

Jeff Reynolds
Daugherty Business Solutions
Atlanta, GA

JP James
Octane Systems
Atlanta, GA
Big Data Analytics: Business and the Law
By Ted Claypoole
Partner, Womble Bond Dickinson

When you call into your bank, walk into your family’s favorite grocery store, or point your browser into Amazon.com, the company is waiting for you. It knows who you are. It knows what you like. And most of all, it knows the best ways to influence you to spend or invest in the ways that benefit the company.

Digitization and connectivity, low-cost storage and data visualization, management dashboards and quantification – all these changes to business and technology over the past 30 years have led to a boom in analyzing large data bases to gain advantages for business and insights for governments. Whether called “big data” or “information analytics” this trend has led to the collection of enormous databases and constant testing of an action’s impact on the populations and transactions of everyday life. Much of the data used is non-personal, but nearly every retail business and scores of data aggregators keeps detailed files on individuals living in the United States, including preferences and recent transactions of all types.

The internet has detonated explosive growth in the space because every search, browser move, app opening or physical smartphone movement can be measured, captured and tossed into any number of databases for analysis. The holy grail for retailers now is cross-device tracking, where a company can link up one person’s browsing (and real-world travel) habits from that person’s smart phone, laptop, tablet, business computer, smart television and wearable device like a smart watch.

This cross-device tracking is easy for companies that offer consumers a membership registration – like Amazon Prime or your cable company’s footprint on mobile devices – because a consumer signs into with each device to get the most benefit from membership, and the company stitches these devices together with the
personal data filled out on the membership form and data on the credit cards registered to pay for the membership. But companies that do not have membership data are trying various types of device beacons and cookies, and even using subsonic signals between devices, that the user can't hear, but initiates cross device responses that can be recorded by the company.

Further, growth in science's understanding of the human brain and social science's theories of mind, influence and behavior have made gathering mountains of information more valuable to anyone who needs to drive the behavior of certain people one direction or another, whether for political or economic gain. As humans understand more about themselves and about tribal behaviors, the data analytics collected across the internet becomes weaponized for better, for worse, and for the benefit of the drivers, not necessarily the benefit of the data subjects.

As business, governments and other entities build database analytics deeper into their operations, the law has started to take notice. Early privacy laws addressed the sale and transfer of personal data around individuals that could be used for identity theft or even interpolated information that might be embarrassing to a person or dangerous to her financial life. Some rules regulate the companies that aggregate data captured by third parties and make a business of selling personal profiles about specific people. Others are starting to apply limits on life-affecting decisions that are made entirely by automated analytics without significant input or analysis from humans. This paper explores how data analytics are being used now and how the law is changing to better regulate personal impacts of the data revolution.

No current United States laws directly prohibit, proscribe or limit a company's ability to perform data analytics on information the company collected for its own use. However, several statutes and regulations in both the US and other industrialized countries restrict how information may be used or shared, especially in the consumer context.
Privacy Protection: The Consumer’s Best Defense

Some of the first laws to address social harms caused by data analytics were directed toward protecting the privacy of individuals from both the personal information and inferences mined by companies and governments, but also the perceived risks of important decisions being made about people on analytics alone, with no human element. Regulators also noted that some data, once anonymized to protect the privacy of individuals, could subsequently be de-anonymized, leading to harmful implications and extrapolations affecting regular people.

One of the first privacy laws to address the risks of data analytics was the law regulating information about health care information in the United States. The Health Insurance Portability and Accountability Act, or HIPAA became law in 1996. It assists people in porting their health insurance from one company to the next, and streamlined movement of medical records between health care institutions. HIPAA helped recognize and enforce the rights of patients to protect the privacy of their medical records.

In 2002 the HIPAA privacy rule was implemented to protect confidentiality of patients’ healthcare information without hindering the flow of information needed to provide treatment. Applying to healthcare providers and any entity that may have access to healthcare information about a patient, the HIPAA privacy and security rules control who can have access to Protected Health Information (PHI), the conditions under which it can be used, and who it can be disclosed to. So not only doctor’s offices, but health insurers, pharmacies and companies that provide health plans also must comply with the HIPAA privacy laws.

HIPAA privacy laws protect “Individually Identifiable Health Information” which is defined as any information that can reveal a patient’s identity in respect of the patient’s past, present or future physical or mental condition; provision of healthcare treatment and healthcare services to the patient; or payments for the
provision of patient healthcare. The US Department of Health and Human Services, which regulates the US healthcare industry, including interpreting and administering HIPAA, acknowledges that companies can remove the personally identifying characteristics of personal health data, and allows the information's use in a de-identified fashion.

Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify an individual and if the covered entity has no reasonable basis to believe it can be used to identify an individual, although de-identification clearly limits the usefulness of the information. HHS explains deeply detailed rules about the two methods with which health data may be de-identified, primarily so that the same data or information derived from that data cannot be re-identified again.

Re-identification is the process by which anonymized personal data is matched with the data subject it describes, where anonymized data is linked back to a specific individual. Data can be re-identified by combining two datasets with different types of information about an individual. One of the datasets contained anonymized information; the other contained publically accessible data like voter registration data, and which includes names or other clearly identifying information. The two datasets will usually have at least one type of information, like birth date, that is the same in both sets. This cross-available information links the anonymized information to a specific person. By combining information from each of these datasets, and confirming the results with other information, researchers can uniquely identify people in the anonymous data set.

The reidentification concern is especially significant in the medical and biological research field, where the biological data itself could reidentify an individual. Use of biometrics can clearly pinpoint one patient from another, whereas DNA analysis can tell information about specific people, their families and even
their physical attributes. In these cases, a researcher or company may not even need a second database to reidentify a subject that had been anonymized earlier.

Healthcare is not the only place that US law encourages anonymization of data. For example, the Fair Credit Reporting Act regulations define consumer information to expressly exclude "information that does not identify individuals, such as aggregate information or blind data." Similarly, under the federal banking law, the definition of "personally identifiable financial information" excludes "information that does not identify a consumer, such as aggregate information or blind data that does not contain personal identifiers such as account numbers, names, or addresses." So data anonymization allows companies to do more with financial records in the US.

Some US lawmakers have been concerned about the effects of automated decision making on people's lives. New York City Mayor Bill de Blasio announced the creation of the Automated Decision Systems Task Force to analyze how New York City uses algorithms. Mayor de Blasio said, “As data and technology become more central to the work of city government, the algorithms we use to aid decision making must be aligned with our goals and values. The establishment of the Automated Decision Systems Task Force is an important first step towards greater transparency and equity in our use of technology.” The New York City Council had passed a resolution in December of 2017 to stop using algorithms to make important city decisions that affected the lives of residents.

On May 25, 2018, the European Union implemented a new law called the General Data Protection Regulation ("GDPR") to update its privacy protection regime. Among many other things, the GDPR addresses the rights of EU residents in relation to data analytics. Article 22 of the GDPR restricts automated decision making to circumstances where the decision is necessary for the entry into or performance of a contract, authorized by EU law or state law of an EU member state applicable to the controller; or based on the individual’s explicit consent. A
company must publically identify if any of its processing falls under these restrictions, must provide EU residents information about the processing, must introduce simple ways for the residents to request human intervention to challenge a decision, and must carry out regular check to make sure that its systems are working as intended.

The analytics restriction covers solely automated individual decision-making that produces legal or similarly significant effects. These types of effect are not defined in the GDPR, but the decision must have a serious negative impact on an individual to be caught by this provision. A legal effect is something that adversely affects someone’s legal rights. Similarly significant effects could include automatic refusal of an online credit application and hiring practices. Because this type of processing is considered to be high-risk the GDPR requires companies that perform analytics to create a Data Protection Impact Assessment (DPIA) to show that the company has identified and assessed what those risks are and how to address them.

Machine learning is a new stage of analytics, and is the basis of all artificial intelligence, and is defined by algorithms that continually and progressively improve themselves. They use big data to perform this analysis and growth. “Big data is completely opposed to the basis of data protection,” said Lilian Edwards, a law professor at the University of Strathclyde in Glasgow, Scotland. “I think people have been very glib about saying we can make the two reconcilable, because it’s very difficult.” Machine learning algorithms evolve beyond the understanding of their own creators and programmers and data is used in ways that people do not understand. This “black box” analysis and use of data runs against several of the requirements of the GDPR.

The GDPR requires the following:

- Companies collecting personal data must say specifically what it will be used for, and not use it for anything else.
Companies must minimize the amount of data they collect and keep, limiting it to what is strictly necessary for those purposes, and limiting the time they hold the data.

Companies must demonstrate the ability to log and present to auditors details on the use of profiling such as use of personal characteristics or behavior patterns to make generalizations about a person.

Companies must tell people what data they hold on them, and what’s being done with it.

Companies should be able to revise or delete people’s personal data if requested.

If personal data is used to make automated decisions about people, companies must be able to explain the logic behind the decision-making process.

Companies use machine learning to infer things about the data subjects included in their databases, including information that might be considered sensitive personal data under the GDPR, which are given extra protection under this law. Companies would need explicit consent to derive or hold sensitive data, but using the latest analytics, the companies will have the data before they even have the opportunity to ask for such permission.

The Disparate Impact of Black Box Decisions

Analytic black boxes can make decisions that have legal effect on the data subjects, including effects that are otherwise regulated by US financial laws. One of the largest concerns is disparate impact analysis in lending, where people in one racial category or otherwise protected category are disfavored in comparison with people in another racial category. Even if there is no intent to discriminate, the law
protects the more vulnerable class of people by forbidding a “disparate impact” of race-neutral decisions, whether human-based decisions or machine-based decisions. Professionals are already working to squeeze bias out of their data analytics programs. "The program doesn't decide on its own," said Marc Stein, CEO of Underwrite.io "The program is constrained by the same regulations as human underwriters. Racial or gender discrimination doesn't become legal because it's done by a machine. It is incumbent on the developer of the algorithm to insure that the results can't evince illegal bias. When discussing algorithmic lending with major banks, the first question they ask is, 'How does this algorithm prevent disparate impact?'"

Consumer lending is essentially a big data problem, naturally suited for machine learning. The lending decision is tied to the creditworthiness of the individual or business requesting the loan. The more data you have about an individual borrower, and about similar borrowers in the past, the better you can assess creditworthiness. The value of a loan is thus tied to assessments of the value of the collateral, whether car or house, and other broader economic factors such as the likely level of future inflation, and predictions about overall economic growth. Analysis of big data should be able to consider all of these data sources together to create an economically intelligent decision. But if the algorithm decides that people with vowels at the end of their names are the worst credit risk, even if this decision is not based on ethnicity, borrowers of Latin and Japanese descent will suffer more than other ethnic groups, and the impact of the decision violates US lending law. Even worse, if the big data decision is made in a black box, then the lender cannot even explain how the decision was reached to defend its choices.

US lending law clearly protects certain categories of people from wrongly adverse lending decisions. The two key federal fair lending laws are the Equal Credit Opportunity Act (ECOA) and the Fair Housing Act (FHA). ECOA prohibits credit discrimination on the basis of race, color, religion, national origin, sex, marital status, age, receipt of income from any public assistance program, and applies to
both consumer and commercial credit. The FHA applies to credit related to housing and prohibits discrimination on the basis of race or color, national origin, religion, sex, familial status, and handicap. Both of these laws may be used to base a disparate impact lending decision based on data analytics.

In addition, Section 5 of the Federal Trade Commission Act prohibits unfair or deceptive acts or practices while the Dodd–Frank Wall Street Reform and Consumer Protection Act prohibits unfair, deceptive, or abusive acts or practices. Many states also have their own Unfair and Deceptive Acts and Practices laws. Deceptive acts or practices are representations, omissions, or practices that are likely to mislead a consumer acting reasonably under the circumstances and are likely to affect the consumer’s conduct or decision with respect to the loan. Unfair acts or practices are those measures made for unfair or unlawful reasons or with an unfair impact that cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid. These UDAP rules tend to underlie the actions of the Federal Trade Commission or state attorneys general who pursue illegal lending claims against financial institutions. Financial analytics may demonstrate that the lender had a non-discriminatory basis for the decision, but that decision may still be considered unfair or deceptive under the law.

Data Aggregation Laws

Some companies build their entire business models around collecting information describing real people, building profiles of those people based on the data collected, and then selling the profiles and the data subject’s contact information to other companies, governments and political operatives. These companies are called data aggregators and their business has reached the attention of legislators in the United States. The Federal Trade Commission has sued data aggregators in the past for being careless and selling the data of consumers to know identity thieves and others. State attorneys general have also shown interest in how aggregators decide where to sell their collected information.
Data aggregators collect consumers’ financial account information from financial institutions, including transaction, balance, and fee information relating to credit cards, auto loans, mortgages and securities. This data is typically obtained by either screen scraping or application program interfaces without consumer knowledge. Application interfaces let aggregators connect directly to a financial institution’s systems and gather information through software. Screen scraping permits automated systems to log in to a particular financial institution as a consumer using the consumer’s username and password, and the company takes the account information that is made available online. Product aggregators have recently evolved to also aggregate consumer financial data along with transaction information, and use consumers’ detailed personal financial data to make more targeted and tailored offers for financial products and services to the consumer.

Aggregators can also make patient inference that can affect the health data, and therefore insurability and other financial decisions, about consumers. For example, medical data like blood tests are protected as private health information, a company may venture an educated guess about a data subject’s medical condition from the medicine that person purchases at her pharmacy, creating a list of “inferred” diabetics, selling that data to anyone from health insurance companies to retailers wanting to sell certain related items.

Vermont’s legislature just passed bill H.764 enacted into law without the governor’s approval. The law gives Vermont jurisdiction to regulate data brokers, who must register, comply and pay a $100 annual registration fee. Vermont now requires brokers to better inform consumers on the data collect about the consumers and provide clear instructions for opting out when that option is available. The Vermont law establishes new security standards for data aggregators. When data brokers suffer from a data breach, they will be required to notify the Vermont authorities of the incident. If state regulators catch aggregators using data for criminal purposes such as fraud, the state can take action against them. The Vermont law specifically protects the following information:
• Consumer’s name
• Address
• Place of birth
• Mother’s maiden name
• Biometric authentication data (fingerprints, retina or iris images, or unique physical or digital representations)
• Name or address of consumer’s immediate family or someone in household
• Social security number or government-issued identification number
• Any other information, alone or combined with other information, that would allow a reasonable person to identify the consumer with reasonable certainty.

In addition, the Bureau of Consumer Financial Protection brought this issue to the forefront in the United States when it issued a request for information on the ways that consumer financial data aggregators obtain, maintain, use and disclose consumers’ financial data. The CFPB relies on two different sections of the Consumer Financial Protection Act of 2010 (“CFPA”) for the potential regulation of consumer financial data aggregators and their activities. Section 1033(a) of the CFPA gives a consumer the right to make a request to, and receive from, a covered person electronic records in the covered person’s possession related to a consumer financial product or service obtained from that covered person, including transaction, cost, and usage data. The statute exempts certain records from being provided, including: confidential commercial information; information collected to prevent fraud or money laundering; information required to be kept confidential by law; and information that a consumer “cannot retrieve in the ordinary course....” Section 1033(e) of the CFPA states that the CFPB must consult with the federal banking agencies and the Federal Trade Commission (FTC) when prescribing any rule under Section 1033.

The CFPB’s authority over data security issues is also based on the prohibition of unfair, deceptive, or abusive acts or practices under sections 1031 and 1036 of the CFPA. The RFI cites to the CFPB’s recent data-security case against
Dwolla and the FTC's past data security activities as relevant precedent to generally assert that “[a]n entity’s consumer data privacy or security practices can violate UDAAP standards.” The CFPB has filed only one enforcement action involving a company’s own description of its data security practices.
Cyber Panel

Presented By:

*Moderator: Jennifer Ruth Liotta*
Tanager Legal, LLC
Atlanta, GA

*Panelists:*
*Chad Hunt*
Federal Bureau of Investigation
Atlanta, GA

*Johnny Lee*
Grant Thornton LLP
Atlanta, GA
A vast number of companies have fallen victim to scams involving business email compromise (BEC) — also known as CEO fraud. This type of exploitation has grown increasingly sophisticated and frequent over the past few years. According to the FBI, BEC scams affected 17,642 victims and amounted to more than $2.3 billion in losses from October 2013 through February 2016.¹ And the fraudsters are only just hitting their stride. Since January 2015, the FBI reports a 270% spike in both the number of victims and the related loss amounts ($3.1 billion in losses).² While these statistics may be bleak, there are ways to minimize the risk that your organization will fall victim to a BEC scam.

At a high level, the scam looks like this: A legitimate-seeming inbound email from an expected source, such as the CFO or controller, arrives, asking the recipient to transmit funds to a third party. Increasingly, these scammers take measures to spoof the incoming email to appear authentic to the unwary, and they do their homework to assume the identity of the requesting individual — reflecting the relationships, terminology, approval levels, in-depth knowledge of the company and (often) a sense of urgency related to the request. On the surface, these requests seem like nothing out of the ordinary, and a surprising number of companies fall victim — wiring actual funds to a fraudulent vendor with no prospect of recovery. Adding insult to injury, upon discovery of the scam, many companies launch costly investigations, effectively to prove a negative, namely that their IT systems weren’t compromised, resulting in still more costs and distractions from the organization’s charter.

Simply put, the best way to prevent email compromise is to review and strengthen your existing controls, and to employ healthy skepticism in dealings related to the transfers of funds. Often, even basic controls can thwart these BEC scams. For example, in most cases, if the recipient of the spoofed email had phoned the ostensible sender for confirmation that the request was legitimate, the fraud would have been identified and avoided. It is important to note that ancillary controls should leverage communication channels other than the original email. Replying to a fraudulent email may direct you to the fraudster for verification, while a phone call or an email forwarded to a known person may not.

¹ McCabe, Jil. FBI Warns of Dramatic Increase in Business E-Mail Scams. FBI press release.
² Ibid.
A holistic approach
By their very nature, these compromise schemes are designed to circumvent traditional controls, so only a holistic, risk-based approach will be successful in combating this new threat. Moreover, the ROI for the scammers and the automation level of these attacks are both so high that we are not likely to see a diminution in the near future.

As discussed in our white paper Taking AIM at Cyberrisk, Grant Thornton LLP is working with each of our clients to align, integrate and measure its controls environments to ground risk awareness within their organizations to meet this — and other — new threats. These six steps are designed to establish controls that can provide Measurable improvements that are Aligned and Integrated into established business objectives. Furthermore, these steps can go a long way in helping your company avoid being a victim of a costly BEC incident.

1. Revisit your wire transfer protocols.
   • Limit the individuals who are authorized to approve fund transfers.
   • Consider instituting varying the dollar thresholds for each approver, so that different categories of spend trigger different levels of authorization. These schemes often capitalize upon known approval levels, so periodically adjusting these may increase the odds of identifying fraudulent requests.
   • Require two forms of authentication for wire transfer requests, such as an email followed by a phone call from or to a known company number. For instance, while an authorized payment administrator might log in and queue up a payment, consider having a second person approve before payment is sent.
   • Segregate the approval responsibilities from the requesting responsibilities. Fraudsters research reporting relationships on social media and networking sites, and they work hard to simulate requests that resemble the normal workflow of your business.

2. Train employees on similar scams and fraud schemes.
   Raising awareness is key. Make sure employees know that this type of fraud happens. Explain that these scams are plentiful, and enlist their help in safeguarding the assets of the organization. It is important in these awareness campaigns to emphasize the rather basic steps that can prevent frauds of this kind. The more vigilant your people are, the less exposed your organization is.

   Consider integrating such training into established training regimens at the organization. This awareness training doesn’t need to be a one-off experience. Indeed there is something to be said for layering a BEC training module into existing training (such as the annual HR training).
   • Train finance and treasury employees, in particular, to be suspicious of requests for secrecy and for pressure to act immediately on requests. Phrases like “this is related to a confidential transaction,” “please do not discuss with anyone else” or “this payment is related to pending litigation and counsel would like us to keep it confidential” should raise alarms.
   • Encourage all employees to say something if they see something suspicious, possibly via a hotline or anonymous reporting if the company has such a system.

Grant Thornton LLP. Taking AIM at Cyberrisk. 2016.
3. **Revise your data security procedures.**
Consider requiring employees, as well as consultants and vendors who are entrusted with confidential data about your payroll and reporting relationships, to sign confidentiality agreements. This will help ensure that employees and vendors alike appreciate that your protocols are confidential. Employees should never give out information such as who your key third-party vendors are, and vendors should never share information about the internal machinations of your organization.

- Revisit the list of employees who have elevated access to key systems, and make sure you have strict controls on users with privileged access. Are the roles commensurate with the level of systems access? If not, adjust the levels of access accordingly.

- Ensure that role changes within the company are reviewed vis-à-vis system permissions. A role change should not result in systems access that combines authorities inappropriately. For instance, if an employee used to have the ability to set up vendors in the system, and that individual’s new role puts him in charge of disbursements, that’s a dangerous combination and an inappropriate segregation of duties. Companies would be well-served to periodically revisit all system privileges for appropriateness, since often what is practiced procedurally is not always enforced systematically.

- Identify and secure any repositories that contain sensitive data, such as key file shares, secure sites, and crucial aspects of the general ledger or banking applications. The focus here should shift to an appreciation of the organization’s assets — whether financial, proprietary or simply embarrassing if they were revealed outside the organization. Of course, any systems or repositories that might result in misstated financials, transmitting money to the wrong party or information that could hurt the company should be included in such reviews.

4. **Improve security on web-based email and applications.**
The better job you do at locking down your system from a security perspective, the easier it will be to spot forgeries.

- Enable two-step or two-factor verifications for access to your network generally.

- Introduce additional controls for access to (and monitoring of) critical systems, such as bank systems, accounts payable check runs and any financial record that is sensitive to your company.

- Revisit the controls for these systems as appropriate.

5. **Test and improve your enterprise-wide technology.**
Be sure that your operating systems and browsers are secure and your incident response plan is up-to-date, and audit your systems to make sure controls are working as intended to avoid BEC fraud, as well as all others types of fraud.

- Update and patch systems used for anti-phishing and malware, and ensure that your operating systems and browsers are patched and secure.

- Identify similar domain names to those legitimately owned by your organization. Consider purchasing these, if only to take them out of circulation.

- Create or leverage a system to flag emails with email addresses similar to (but different from) known organizations, e.g., .co versus .com.

- Conduct audits to test controls that include BEC fraud scenarios. For example, you can hire a third party to try and entice employees to take an action, and then log those who fall for the scam. Tests such as this can demonstrate the strength of awareness for BEC within your organization.

- Revisit your organization’s incident response plan, including protocols for categorization of incidents, response steps, escalation procedures, etc. In particular, consider introducing BEC scams as one of the scenarios in the periodic testing of your incident response plan.
6. Remediate identified issues.

As you consider the assessment of areas for concern, you may want to consider involving counsel in any gap assessment and/or remediation efforts. Many organizations find it possible to both assert and maintain the attorney-client privilege for these efforts. This can be crucial, as assessments of these kinds can reveal control deficiencies in key areas, some of which have existed for a lengthy period of time. While not a silver bullet, discussions with your in-house or outside counsel can help identify ways in which such assessments may be protected from discovery in a future litigation.

Regardless of who directs the efforts to revisit and assess your control environment, it’s important to do so proactively — before the bad thing happens. The steps outlined above are basic, but powerful. They permit an organization to align its control improvements to the actual, bona fide risks it faces; to integrate the controls, processes and protocols necessary to meet those risks; and to measure whether the designed controls are operating effectively to address the risks identified. Taking these six steps will advance your organization’s preparedness to detect — and avoid — BEC fraud.

Contact
Johnny Lee
Principal
Forensic Advisory Services
National Practice Leader
Forensic Technology Services
T +1 404 704 0144
E jlee@us.gt.com

Editor
Phil Quimby
T +1 202 861 4107
E phil.quimby@us.gt.com

Minimize the risk of business email compromise in 6 steps
Recent cybersecurity incidents a wake-up call:

Take action with these proactive steps

Over 1,000 reported data breaches in 2017 thus far, according to an Identity Theft Resource Center report—a jump of 23% over 2016 levels and an increase of 29% in just the first half of the year.

Cybersecurity still isn’t getting the respect it deserves. Despite an increasing number of data breaches, including the recent Equifax breach which exposed sensitive information such as names, birth date, social security numbers, driving license information and credit card numbers of millions of consumers, many organizations have yet to embrace privacy and security as core values. Now is not the time to point fingers but rather consider it a wake-up call to take proactive action.

Even though the Equifax incident is the largest known hack this year, there have been over 1,000 reported data breaches in 2017 thus far, according to an Identity Theft Resource Center report—a jump of 23% over 2016 levels and an increase of 29% in just the first half of the year. The 12 million records exposed in the 791 breaches that took place during the first half of the year are just the tip of the iceberg.

With the average cost of a data breach at a record high of $7.35M and an average of 55 days to contain a breach, according to the 2017 Cost of a Data Breach Report, it’s never been more important for organizations to prioritize security over convenience and implement a proactive program to protect their data, especially the sensitive personal data of their customers and clients.

An average of 55 days to contain a breach, according to the 2017 Cost of a Data Breach Report.
Recent cybersecurity incidents a wake-up call: Take action with these proactive steps

Grant Thornton’s 2017 CFO Survey revealed 72% of financial institutions ranked cyber as a key area of risk for their organizations, as well as an urgent area of investment.

What caused the incident?

Information about the event itself is still in the process of being investigated, however, Equifax has disclosed that the incident was caused by an application security vulnerability that had been previously disclosed in Apache Struts2. Leveraging this vulnerability, attackers were able to get a trove of personal data from 143 million U.S. consumers. The amount of personal information leaked has put virtually every organization and concerned individuals on notice to be on a heightened level of alert and awareness to fraudulent activity.

This event continues to shine a light on the importance of focusing on the protection of assets most critical to the organization. By taking an “asset-centric” approach to cyberrisk management, organizations will be better positioned to protect their most critical information and assets from nefarious exposure.

Building a resilient cyberrisk program

Organizations continually have to make decisions as to how to allocate resources and focus to protect their assets, and this holds true for managing and mitigating cyberrisk as well. Recent studies have found that 60% of all breaches involved web applications, such as Apache Struts, while organizations take an average of over 12 weeks to apply security patches. The timeliness and completeness involved with conducting basic cyber hygiene functions such as patch management can vary greatly between organizations, however issues such as governance between patch and vulnerability management functions, lack of business involvement around vulnerability risk acceptance, and legacy technology environments with cumbersome patching processes can be drivers for this risk exposure.

An “asset-centric” cyberrisk management approach can provide clarity and focus in the area of basic cyber hygiene to limit the probability of similar occurrences within their organizations.

2 Recent cybersecurity incidents a wake-up call: Take action with these proactive steps
For organizations to take a more “asset-centric approach” to cyberrisk management, we recommend the following:

Understand your most critical data that needs to be protected
- Organizations focused on cyberrisk need to adopt a full-stack view of assets, consisting of full mapping of business processes, the potential users and related technologies. You need to weigh your cyberrisk by conducting risk assessment against the assets that are important to your operations, customers, and workforce members.

Map business processes, stakeholders and data systems. Organizations focused on cyberrisk need to adopt a full-stack view of assets, consisting of full mapping of business processes, the potential users and related technologies. Where risk is elevated, controls need to be higher.

Establish an agile vulnerability management program
- Vulnerability management programs enable organizations to identify potential security vulnerabilities and determine proper remediation strategies based on asset criticality and potential business exposure. Vulnerability assessments should occur on a more agile basis based on changing threat landscape and take remediation actions promptly.

Maintaining consistent secure configuration baselines and an accurate asset inventory will help. Vulnerability management should not be an operation solely driven by Information Security. It should be embedded in day-to-day IT operations and application development.

Apply security patches in a timely manner
- Ensuring that vendor security patches are applied in a timely manner can help safeguard against malicious attacks using known vulnerabilities. Equifax has disclosed that a vulnerability in Apache Struts2 (CVE-2017-9805) led to the security breach. Focusing on having well-vetted processes for patching systems that house critical information can serve as a bedrock to a sound and foundational cybersecurity program.

Have in place a fully-tested response strategy
- You need to be prepared to adequately identify a potential breach, then quickly coordinate resources and invoke the necessary processes to contain and mitigate effects of the breach. A great incident response program includes the following components:
  - **Clearly defined roles and responsibilities within your team.** Have all stakeholders been identified and trained on their responsibilities in the event of a cyber incident or breach?
  - **Technology.** What information security detection, alerting and mitigating technology solutions are in use?
  - **Reporting.** Has the organization identified all of its obligations related to reporting an incident? Legal? Regulatory? Contractual? To shareholders?

Align, integrate and measure
- It is vital to bring together operational and financial leaders with risk leaders, and align and integrate their goals, objectives, compliance demands and stakeholder expectations. This will require operational processes to be meshed with cyber controls — with a special focus on where the business is most sensitive. And all this must be overlaid with a system of measurement and metrics, so that leaders always can assess the threat outlook, have options to dial up controls and further enact a digital strategy.
The key to managing threats isn’t necessarily greater investment or even manpower. Instead, it takes the imagination of a criminal — seeing your own enterprise as they would see it. Wherever you are most sensitive is the most likely target of future cyber threats. What is most valuable to you is also most valuable to someone who wants to hurt you.

The following figure demonstrates the AIM approach:

**Align**

1. Business strategy and cyber strategy

**Integrate**

2. Business process and cyber controls

**Measure**

3. Business outcomes leveraging cyber analytics

**Contacts**

**Vishal Chawla**
National Managing Principal, Risk Advisory Services
T +1 703 847 7680
E vishal.chawla@us.gt.com

**John Pearce**
Principal
T +1 703 637 4071
E john.pearce@us.gt.com

“Grant Thornton” refers to Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd (GTIL), and/or refers to the brand under which the GTIL member firms provide audit, tax and advisory services to their clients, as the context requires. GTIL and each of its member firms are separate legal entities and are not a worldwide partnership. GTIL does not provide services to clients. Services are delivered by the member firms in their respective countries. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another’s acts or omissions. In the United States, visit grantthornton.com for details.

© 2017 Grant Thornton LLP | All rights reserved | U.S. member firm of Grant Thornton International Ltd.
Resilience—the best strategy for cyber threats

It is now axiomatic that data breaches have become a function of “when, not if”. At long last, organizations are increasingly cognizant of this fact. In Grant Thornton’s 2017 Corporate General Counsel Survey, 72% of respondents cite cyber threats as their most significant source of risk. Cyber risk is significant, and it’s changing.

Today’s risks are significantly different than they were even a few years ago. Cybercrimes have evolved from blunt, brute-force tactics to highly automated, tailored, and targeted attacks. Cybercriminals employ sophisticated skills and operate within a thriving and evolving criminal marketplace. This sophistication breeds commoditization, meaning that bad actors no longer need to possess deep technical capabilities to wreak havoc; they merely need to know where to shop for the skills they need.

Accordingly, an organization’s information security controls alone are no longer sufficient to counter these threats. In the face of this evolving threat, organizations need to move from a cyber strategy focused purely on defensive technology towards a holistic approach that focuses on the concept of resilience. To be sure, organizations must continue to maintain effective preventative measures, but they must also build their ability to identify, to contain, and to recover from data incidents by employing a multi-disciplinary approach that incorporates skills from several core competencies.

Four steps to resiliency
Consider the following steps, all of which combine to form a resilient approach to cybersecurity.

1. Build a collaborative, cross-functional team
   Yes, strong technical controls remain vital, but your cybersecurity team needs to either develop internally or to partner with external parties to address a variety of disciplines. It should coordinate closely with operational areas to fully understand data needs, uses, and exposures. Vendor management resources will need to focus on third-party risk profiles and to develop controls suitable to the risk profile of each third party (without over-engineering controls in a way that could unduly hamper operations). Your general counsel should play a key role in helping to ensure that appropriate contractual protections are in place, to provide guidance concerning when and how to involve law enforcement and to invoke and manage the attorney-client privilege.

Crisis management and communications resources also play a key role to ensure consistent and accurate communications are relayed to affected stakeholders and customers in the event of a breach, thus helping to mitigate reputational damage.

grantthornton.com/advisory
2. Get the right insurance, but understand its limitations

Insurance products are evolving to offer protection against a breach, but organizations need to understand the difference between insurable and uninsurable risks. Many organizations only discover the gaps, exclusions, and limitations in their coverage after a breach has occurred. Organizations should conduct regular, detailed reviews of the evolving array of insurance products available to tailor a solution. Organizations must also understand that some risks, such as reputational damage, are difficult to insure against.

3. Control third-party risk

Most organizations today rely on a web of external and internal resources to meet evolving customer needs. This often means granting vendors and other third parties access to your infrastructure, transferring sensitive data, and maintaining your "cyber footprint" beyond the traditional boundaries of your organization. Organizations must conduct due diligence on its key third parties to ensure that effective cybersecurity practices are maintained and that contractual protections against third-party failures are available.

4. Practice, practice, practice

Once you’ve assembled the right incident response team (including external forensic and legal experts, as needed), this team needs to be run through its paces "before the bad thing happens". Put differently, the effectiveness of a good team can only be measured through regular drills, which will identify gaps and better ensure that everyone is prepared to act quickly and appropriately in the event of a breach.

Focusing on resilience, not just defense, is the best way to prepare for an environment where a breach of some nature is almost inevitable. Grant Thornton’s white paper, *Taking AIM at Cyber Risk*, offers further insights on how a holistic, resilient approach best positions companies to address today’s evolving cyber threats.

**About Grant Thornton**

Grant Thornton LLP’s Advisory Services professionals are progressive thinkers who create, protect and transform value today so our clients have the opportunity to thrive tomorrow. While business goals and strategies evolve, our services can support you wherever you are — whether you’re looking at a transaction to propel you forward, focusing on developing and implementing the right controls to mitigate risk, or advancing your company’s finance and technology infrastructure to match your aspirations.
Cybersecurity incident response:
Planning is just the beginning
Contents
3 Executive summary
4 Introduction
5 Cybersecurity incident response
7 Exercises and training
8 Board involvement
9 Cyberinsurance
10 Third-party risk
11 Communications
12 Conclusion
13 Interviewees
Author and contributors

14 About Financial Executives Research Foundation Inc.
   About Grant Thornton LLP
15 Our supporters

Author
Thomas (Tom) Thompson
Manager, Research
Financial Executives Research Foundation

Contributors
Johnny Lee
Managing Director, Forensic and Valuation Services
Grant Thornton LLP

Todd Fitzgerald
Global Director, Information Security
Grant Thornton International Ltd
Executive summary

By now, most senior-level executives have heard that either you have had a data breach or you just don’t know that you’ve had a data breach. Cyberattacks are now as much a part of doing business as taxes and financial statements, and they are getting expensive. According to the 2015 *U.S. Cost of a Data Breach Study* by the Ponemon Institute, last year there was an 11% increase in the total cost of a data breach, to a $217 average per lost or stolen record. To be sure, those numbers are based on estimated costs of actual data loss incidents, not hypotheticals.

In an effort to support senior financial executives in their cybersecurity incident planning and response, Grant Thornton LLP and Financial Executives Research Foundation (FERF) have identified several essential areas for their consideration. This report’s findings are based on in-depth interviews, conducted between August and September 2015, with 10 subject matter experts of various specializations, including legal, PR and communications, insurance, and IT security. The interviewees provided their perspectives on cyberrisk management strategies and best practices in cyberbreach response.

Key findings include:

- Simply having a cybersecurity incident response (IR) plan is not enough. It must be reviewed and updated regularly as part of a comprehensive cybersecurity incident response program.
- Regular training and exercises are important in keeping the IR plan effective. Employees can be a critical line of defense.
- Board involvement is crucial. Senior management and the board need to have open dialogue about expectations regarding risk tolerances, budget considerations, IR planning and breach response.
- General liability insurance and director’s insurance most likely will not cover a cybersecurity incident. A full review of insurance should be an integral part of cyberrisk management.

---

Introduction

Today’s organizations face a sobering reality. The question is no longer whether we will be breached but when we will be breached. Cybersecurity is a C-suite and board-level issue requiring a comprehensive risk management strategy, intelligent investment and integration across the organization.

While the costs associated with a data breach continue to rise, there are established best practices that can mitigate some of those costs. The 2015 U.S. Cost of a Data Breach Study² found that having an IR plan and team in place, extensive use of encryption, business continuity management (BCM) involvement, chief information security officer (CISO) leadership, employee training, board-level involvement, and insurance protection are viewed as reducing the cost of a data breach. An IR team can decrease the average cost of a data breach from $217 to $193.2 (decrease = $23.8) per lost or stolen record. However, third-party error, a rush to notify, lost or stolen devices, and the engagement of external consultants to support the IR team response to a breach increased data breach cost.

Clearly, having an IR plan and team in place, extensive use of encryption, BCM involvement, CISO leadership, employee training, board-level involvement, and insurance protection would all be considered best practices. These elements should be considered the foundation of a robust cybersecurity incident program. FERF, in cooperation with Grant Thornton LLP, spoke with several subject matter experts from a variety of fields to glean insights and recommendations for instituting an effective cybersecurity incident response program.

When determined adversaries such as hacktivists, state-sponsored actors and organized criminal syndicates set their minds on finding a way inside, every organization with valuable digitized information is at risk of having its information assets breached and its critical assets compromised. Indeed, most organizations today would do well to expand their efforts to mitigate the consequences of inevitable breaches, which likely affect infrastructure systems and compromise key data such as personally identifiable information and confidential business information. A properly drafted IR plan guides the proactive planning and management necessary to effectively react to such breaches.

It all starts with a plan
The primary objective of an IR plan is to prepare for and manage a cybersecurity incident in a way that limits damage, increases the confidence of external stakeholders, and reduces recovery time and costs. Unfortunately, IR plans are one of the most neglected aspects of information security. Without a plan, organizations do not respond to a cybersecurity incident — they react to it, and reactions are usually based on misinformation and misunderstanding or, worse yet, fear.

To this point, Melissa Krasnow, partner and U.S. Certified Information Privacy Professional (CIPP/US) with Dorsey & Whitney LLP, noted: “While a number of companies have them [IR plans], you might be surprised by the companies that do not have them even though there is guidance about them, regulators are encouraging companies to have them, and they are a best practice. Once a company or a competitor or a business partner experiences a breach, incident or cyberattack, they develop an awareness that often galvanizes preparation, including an IR plan.”

Fellow attorney Liisa Thomas, chair of the principal and data security practice at Winston & Strawn LLP, said: “Most companies have a disaster recovery plan. If a 9/11 type of event happens, they know what to do. Typically, they will dust off that plan and make sure it works for them at least once a year, if not more.”

As it relates specifically to cyberincidents, Thomas continued: “A potential data breach should be treated in much the same way. An IR plan should give high-level information about how the company will handle the incident. Not all breaches are the same. Some might be cyberevents; some might be internal thefts. I’ve seen plans that are 30, 40 or maybe 100 pages long. Often they’re very focused on specific steps that the IT department would take to contain the incident. These plans may have their place, depending on the organization. But they might not instruct those outside of the IT department — senior leadership — on what to do at a high level. I advise clients to have a shorter, high-level document. The high-level document helps not only during an incident, but also before it, raising awareness with the senior leadership about the types of decisions they’re going to be asked to make. A plan like that can be used by the decision-makers to practice against, just like they would a disaster recovery plan.”

---

Cybersecurity incident response: Planning is just the beginning

Johnny Lee, Grant Thornton managing director of Forensic, Investigative and Dispute Services, adds, “While the IR plan can resemble a high-level policy, it is important to note that each constituent department (IT, legal, communications, risk management, etc.) might have far more detailed protocols invoked during an incident response.”

Jerry Wynne, CISO and senior director of enterprise security with Noridian Mutual Insurance, said his company does have a cybersecurity IR plan: “We are in the process of updating it again based on several breaches that have occurred within the industry in the last year. It will include some additional areas that are outside of the traditional cybersecurity IR time.”

Those updates were the result of lessons learned within their industry peer group. This follows best practices, as IR plans should be revisited regularly to ensure that they don’t get stale. Wynne continued, “We have a stronger legal presence on the team, and we’ve made sure that our privacy area and compliance areas are more heavily involved than they have been in the past.”

Information security expert and former CISO Bill Barouski believes there are two aspects organizations should consider in reviewing their cybersecurity incident response plans: “I think every program, every plan should be reviewed at least annually. Then, probably every 18 to 24 months, have a third party review the plans. Any high-performing organization would want an outside view into their effectiveness.”

IR team

When asked who should head the response team or what departments should be included in the team, John Kennedy, corporate partner in the IT and outsourcing, privacy, and information security group at Wiggin and Dana LLP, said: “It varies by organization, but I believe a best practice is to create an IR governance committee, which should include representatives from executive management, so that decisions can be made quickly. In terms of the preparedness side and the planning and the communications chain, it will include legal, IT, risk management, human resources, public relations and, in some cases, facilities management. There may be, in addition, a compliance officer as well as a risk officer. In the end, the incident response team should represent a cross-section of key stakeholder interests that will be affected by different kinds of incidents.”

Ashley McCown, president at Solomon McCown, had a few suggestions regarding which business operations should be a part of the IR team: “The CFO certainly is included; there are obviously significant financial implications in a breach, so he or she needs to be at the table. The general counsel, and as companies are getting very organized around potential cyberattacks and identifying a law firm or lawyer with expertise in cybercrimes and breaches, that person can be brought into the effort. IT clearly should be involved; HR, sometimes, if employee data and personally identifiable information are leaked. Definitely the communications department, which could include internal and external communications.”

She continued: “Additionally, you want to have backups and redundancies because people go on vacation. Even with cellphones and Wi-Fi everywhere, people can be out of touch, and being able to mobilize your team quickly is essential. Incidents don’t often happen at the most opportune times.”
Exercises and training

Putting a plan like this together, keeping it up-to-date and exercising it periodically is a lot of work — a major reason that it doesn’t always get done. But when something bad happens (and it will), having the plan available and the experience that only comes from practice will save a lot of time and potentially avoid embarrassment at best, and litigation at worst.\(^5\)

Having a cybersecurity incident response plan is an important step, but it’s only the beginning. The plan is not of much use if it only exists on paper or on a server somewhere — it must be reviewed regularly and periodically exercised. All of the interviewees stressed the importance of tabletop exercises and employee training. Additionally, as they relate to tabletop exercises, these updates should include industry-, regulatory- and technology-specific scenarios. An executive director of information security with a large insurance company noted: “We’ve had numerous exercises in 2015. Traditionally, we’ve conducted exercises focused on business continuity and disaster recovery. However, we’ve stepped it up this year to do more crisis management tabletop exercises to address cybersecurity threats. We engage the threat response team, which is our cross-functional IT team, to participate in cybersecurity tabletop exercises based on real-life scenarios. We exercised our plans to determine how prepared we are to respond and to determine if our response plans are well-documented.”

She continued: “We’ve also done a tabletop with our midlevel executives, our vice presidents and other key stakeholders across the organization, to make sure plans are in place, including communication plans. Social media is going to be a big part of our response plan to make sure we handle social media issues timely and appropriately. Soon we’re going to conduct an exercise with our senior-level executives so they are prepared to handle crisis management events. We are really putting a lot of effort and emphasis on tabletop exercises and preparedness as key to managing a major event.”

John Kennedy, corporate partner at Wiggin and Dana, noted: “Organizations that are seriously focused on this issue are doing training directed at all employees who may be in a position to expose the company to risk by virtue of the activity that they’re permitted within the company’s network. We have done training sessions with hedge funds specifically for the issue of social engineering and phishing. The training was not just limited to the senior officers either; it was a room full of traders and analysts. Phishing attacks are becoming increasingly sophisticated; you hear stories where someone very high up in the organization was impersonated and a middle-management employee was duped to transfer funds or execute an order that was bogus.”

Todd Fitzgerald, Grant Thornton International global director of Information Security, adds: “Training methods have to change from 45-minute slide decks to online cyberassessments, phishing simulations and interactive training to grab the end users’ attention and deliver relevant 15-minute training. Only after users have been fake-phished will they really pay attention to the training where information flow and demands on our time are at all-time highs.”

While there are those that will view employees as the weakest link in their organization’s cyberincident preparedness, Bill Barouski, information security expert and former CISO, thinks the opposite. “Someone that is very well-trained and cyberaware is going to be far more effective than technology,” he said. “People can become your strongest link.”

For attorney Jason Bernstein, partner and co-chair of the data security and privacy group at Barnes & Thornburg LLP, training also means reinforcement: “If you do it once a month, people start getting kind of blind eyes, like a parent talking to a 16-year-old. With the IT directors and CIOs that I talk to, it’s constant education. It does not matter how high- or low-level you are at this; these phishing attacks have gotten so good, and there are so many nuances in them that it’s real easy to just click on them.”

---

Board involvement

With recent high-profile legal cases involving board members making headlines, boards need to be more than just aware of cybersecurity incident response, they need to be involved in the IR planning. As Melissa Krasnow, partner and CIPP/US with Dorsey & Whitney LLP, pointed out, “The intersection of cybersecurity and corporate governance is an area that’s developing and where awareness continues to increase.”

She continued: “IT is in the middle of all this, and increasingly is being called upon by the board of directors and executives. Some companies are being transparent about their cybersecurity, for example stating, ‘Here’s where we’re lacking in our security, and here’s what we need to do to address it,’ and providing steps that should be considered. Company ethics and culture may transcend legal requirements about how a company handles things. It’s interesting to see this dynamic play out.”

Unfortunately, the reality is that boards are often focused on other competing priorities. The former CISO of a large educational system noted that there was limited support at the board level: “If they did get involved, it did not trickle down to me. To my knowledge, senior management did not have much expectation from the board relating to cybersecurity. The board was focused on other topics.”

However, other boards are very involved in cybersecurity. The executive director of information security with a large insurance company said the board in her organization takes this issue very seriously: “It’s considered in every board meeting now. My boss is the chief information security officer, and he reports to the CIO. Every quarter, they have to give an update regarding not only IT in general, but also cybersecurity threats. The board is very interested and they do care, and I think it’s helping to drive our investments in security, which is a good thing.”

From the senior management perspective, she continued, “[t]he expectation of the board is to drive awareness. The board sets the tone so senior management and the end users know that it’s important that security and the controls work properly.”
Given that cybersecurity is all about risk assessment and management, no cybersecurity IR program would be complete without a review of an organization’s existing insurance coverage. Do not just assume the company’s general liability or directors insurance coverage will suffice. That said, there are certainly some companies that are ahead of the curve. Jerry Wynne, CISO and senior director of enterprise security at Noridian Mutual Insurance, said his company has been carrying cyberliability insurance for several years: “We went down the road of cyberinsurance after recognizing the potential liability. The discussion focused on the financial impact a breach would be to the company and to everyone involved. In the end we decided that we really had to have cyberinsurance, so we’ve been maintaining that for about five years.”

Nolan Wilson, Southeast region leader of professional risk solutions at AON, notes: “Probably more do not purchase [cyberinsurance] than do, even though it’s such a big topic today. I think from a general liability perspective, it’s more and more common to see a specific exclusion for access or disclosure of confidential and personal information. It’s critical to not just assume that you have insurance that will cover a specific incident, and to make sure that you’re looking at the policy and any exclusions that it might have.”

John Kennedy, corporate partner at Wiggin and Dana LLP, noted more policy review: “Companies are paying much more attention to it. At least some of them are waking up to the fact that commercial general liability (CGL) policies and other kinds of standard policies do not address cyber risk. We do a fair amount of work in the insurance sector, so we’ve actually worked with insurance companies on how to draft cyberinsurance policies, but also how to draft cyber risk exclusions from their CGL policies.”

Kennedy continued: “Companies just don’t seem to pay the same degree of attention to the risk of loss to their information assets as they do to their tangible assets, and therefore may not understand that data loss is not covered. Or if you outsourced something and that third-party provider lost your data, your policies may not cover that. Insurance provisions have gotten very detailed and demanding. Customers are telling their vendors or their suppliers that they’ve got to carry all these types of cyberliability coverage, criminal cyberliability coverage, etc., in addition to the other types of insurance.”

Todd Fitzgerald, Grant Thornton International global director of Information Security, also notes: “Cyberinsurance is an important tool to mitigate risk; however, this cannot be a substitute for having reasonable controls and an adequate IR program. Many policies have exclusions for not having minimum controls, such as an exclusion for losses due to unencrypted laptops, or not having a plan in place. Some policies will also require the use of their service providers in the event of an incident. These policies should be reviewed carefully to determine acceptable coverage for the organization.”
Third-party risk

Just because an organization’s systems do not suffer a breach does not mean its information cannot be compromised. Third-party or vendor risk is another key area of consideration for a company’s cybersecurity IR program. Are they protecting data with the same fervor you are? To find out, it’s critical to conduct an assessment of your partners’ cybersecurity measures and assess your vendors’ management processes. You’ll need to determine how these organizations will protect your data, either through contractual agreements, assessments or audits.

Depending on the size of your organization, your vendor management group may be able to handle this, or it might require a combined effort, with your accounting group and IT security staff working together to look at vendors. For more insight, see the article “Unprepared Organizations Pay More for Cyberattacks,” originally published in Grant Thornton’s CorporateGovernor newsletter on Feb. 4, 2015.

The former CISO of a large educational system said he instituted vendor security and a vendor assessment questionnaire: “Anytime a new vendor would come on board, we would have them complete the questionnaire and we would make a risk recommendation whether or not to proceed. Now the organization could always accept the risk, but IT would at least make some recommendation based on our vendor security review.”

Bill Barouski, information security expert and former CISO, noted: “I think this has started to get more attention in the last 18 months. Any large, extended enterprise will have a very wide array of third-party vendors and partners. They’re saying, ‘We need to take a holistic view of cybersecurity across the entire enterprise, including contractors, vendors, partners, etc.’ so I see a lot of energy around this topic, especially in the financial services industry.”

Ashley McGown, president of Solomon McCown, commented: “In business in general, we are hearing more about companies requiring verification from third-party vendors to show what systems and processes they have in place to protect data. I think that’s becoming much more commonplace.”

An executive director of information security with a large insurance company said her company has spent a lot of time looking at third parties because incidents can occur outside your systems but have implications for your company: “Many times it had to do with a third party either having some kind of entry point into your system, or just the fact that we’re sharing our data with third parties. So we have a strong, robust third-party vendor management program. We look at it from a privacy, security and legal perspective. But we know it’s really working with our procurement department, as well as our business partners, to have a strategy of what type of information lends itself to be hosted externally with third parties and the criticality of the business. So we’re putting a lot of criteria and strategy around our third-party vendor management to make sure we’re providing the right oversight.”

She continued: “If vendors have access to critical and/or confidential information, we require what’s called a minimum security requirements document that’s a part of the contract, like an addendum, and one of our requirements is data security at rest, in addition to many other things. It seems like the industry has shifted, and a lot of companies and third-party vendors — at least the ones that deal in health care information — are taking it seriously and adhering to that requirement.”
Communications

PR and communications must be an integral part of any cybersecurity incident response plan. This is the area of expertise of Ashley McCown, president of Solomon McCown, and she summed this up perfectly: “Social media is a game changer in our world in terms of how quickly information and/or rumors can spread. Now hackers will often be the ones that go onto a blog or other social channels to put it out there that they’ve hacked an organization or company. So then the clock starts ticking. Someone’s going to tell the story, and you want that someone to be you and your company and not other people.”

Bill Barouski, information security expert and former CISO, noted: “What I’ve observed, increasingly so, is the sooner you’re able to provide clear and unambiguous information, the sooner you reduce the attention, uncertainty and the number of news stories. By nature, if the public doesn’t believe you’re being straightforward or cooperating, the scrutiny and intensity increase. But I think you’ve seen in the last two years how firms are much quicker to announce what they do know even without full understanding of what’s happened.”

While putting out a public communication statement following a breach is important, Jason Bernstein, partner and co-chair of the data security and privacy group at Barnes & Thornburg LLP, did provide some words of caution: “A lot of times when we’re talking about a small company, they don’t have a PR firm, certainly not a PR firm that knows how to deal with data breach communications. Part of what we do in our role is to help manage this whole process, and one of the things that a PR firm and certainly the client tends to do in terms of communication is say, ‘We are guilty, we’re sorry, mea culpa.’ We try and advise them on what they should be saying or not to say just yet.”

He continued: “One key to managing communications is to communicate early and clearly what you do know, and that you will provide more details as they become available. In a major breach incident, it’s not a good idea to release information that is not confirmed. Delaying an initial announcement makes the public suspicious of your motivations. But restating the facts later is likely to be more damaging. So managing that communications process is a balancing act. And, in the big picture, the way the company handles communications will be remembered long after the breach is fixed and individuals have been taken care of, and this is the key to minimizing damage to the company’s brand reputation and regaining trust.”
Cybersecurity incident response: Planning is just the beginning

Hardly a day goes by without cyberattacks and data breaches grabbing media headlines. No company, organization or even government is immune. That’s the bad news. The good news is that companies can use these events to bolster their own cybersecurity incident response. Once again we consider those factors that can reduce the cost of a data breach. Some of the most valuable investments companies can make seem to be an IR plan, extensive use of encryption, the involvement of business continuity management, the appointment of a CISO with enterprise-wide responsibility, employee training, board-level involvement and insurance protection.7

Prevention through implementing reasonable controls is still very important; however, these controls are point-in-time and, even if implemented correctly 100% of the time, there are new threats and exploits that are emerging. There will always be a gap between the implemented controls and the resources available to a determined attacker. Thus, planning for this situation by implementing an IR program is critical to reducing the risk and cost to the enterprise.

The risks of cyberattacks span functions and business units, companies and customers. Given the stakes and the challenging circumstances related to becoming cyberresilient, making the decisions necessary can only be achieved with active engagement from the CEO and other members of the senior management team.8 Cybersecurity is not a check-the-box-and-you’re-done issue. It requires a commitment of time and resources. It’s too late to start planning for a breach once a breach has taken place. Start planning now; best practices begin with a cybersecurity incident response plan as part of a comprehensive IR program.

Conclusion

Key areas of consideration in cybersecurity incident response planning include:

- Who is a part of the cybersecurity incident response team? Who will lead that team?
- How often will the cybersecurity incident response plan be reviewed?
- Does the company perform tabletop exercises and testing of employee cyberreadiness?
- What training is/will be provided to all employees on cybersecurity?
- What are the board of directors’ expectations regarding cybersecurity and cyberreadiness planning?
- Is your organization adequately insured to cover data breaches?
- Has your company identified its third-party risks?
- Who will be the company spokesperson to communicate in the event of a breach?

Ten in-depth research interviews provided insights into how companies are reacting to cybersecurity. The following subject matter experts participated in these interviews:

- Bill Barouski, information security expert and former CISO
- Jason Bernstein, partner, data security and privacy group, Barnes & Thornburg LLP
- John Kennedy; corporate partner, IT and outsourcing, privacy, and information security group; Wiggin and Dana LLP
- Melissa J. Krasnow, corporate partner and CIPP/US, Dorsey & Whitney LLP; Governance Fellow, National Association of Corporate Directors
- Ashley McCown, president, Solomon McCown
- Liisa Thomas, chair, privacy and data security practice, Winston & Strawn LLP; Governance Fellow, National Association of Corporate Directors
- Nolan Wilson, Southeast region leader, professional risk solutions, AON
- Jerry Wynne, CISO and senior director of enterprise security, Noridian Mutual Insurance
- Anonymous, executive director of information security with a large insurance company
- Anonymous, former CISO of a large educational system

**Thomas (Tom) Thompson**

Thomas (Tom) Thompson is manager of research at FERF, the nonprofit research affiliate of Financial Executives International (FEI). Thompson specializes in qualitative and quantitative research methodologies, and has authored more than 60 executive reports and white papers. He earned a BA in economics from Rutgers University and a BA in psychology from Montclair State University. Prior to joining FERF, Thompson held positions in business operations and client relations at NCG Energy Solutions, AXA Equitable and Morgan Stanley Dean Witter.

He can be reached at +1 973 765 1007 or tthompson@financialexecutives.org.

**Johnny Lee**

Johnny Lee is a managing director in Grant Thornton’s Forensic and Valuation Services practice, a practice leader of the Forensic Technology Services group, and a member of the cybersecurity leadership team. Lee is a former attorney, as well as a management and litigation consultant specializing in data analytics, computer forensics and electronic discovery in support of investigations and litigation.

He can be reached at +1 404 704 0144 or j.lee@us.gt.com.

**Todd Fitzgerald**

Todd Fitzgerald is a global director of Information Security for Grant Thornton International Ltd, providing strategic information security leadership for Grant Thornton member firms supporting 40,000 employees in more than 130 countries. Fitzgerald is also an information security author specializing in information security leadership and governance issues.

He can be reached at +1 630 873 2720 or todd.fitzgerald@gti.gt.com.
About Financial Executives Research Foundation Inc.

Financial Executives Research Foundation (FERF) is the non-profit 501(c)(3) research affiliate of Financial Executives International (FEI). FERF researchers identify key financial issues and develop impartial, timely research reports for FEI members and non-members alike, in a variety of publication formats. FERF relies primarily on voluntary tax-deductible contributions from corporations and individuals. FERF publications can be ordered by logging onto www.ferf.org/reports.

The views set forth in this publication are those of the authors and do not necessarily represent those of the FERF Board as a whole, individual trustees, employees or the members of the Research Committee. FERF shall be held harmless against any claims, demands, suits, damages, injuries, costs, or expenses of any kind or nature whatsoever except such liabilities as may result solely from misconduct or improper performance by FERF or any of its representatives.

© 2015 by Financial Executives Research Foundation, Inc. All rights reserved. No part of this publication may be reproduced in any form or by any means without written permission from the publisher.

International Standard Book Number 978-1-61509-194-2

Authorization to photocopy items for internal or personal use, or for the internal or personal use of specific clients, is granted by FERF provided that an appropriate fee is paid to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923. Fee inquiries can be directed to Copyright Clearance Center at +1 978 750 8400. For further information, please visit the Copyright Clearance Center online at www.copyright.com.

About Grant Thornton LLP

Founded in Chicago in 1924, Grant Thornton LLP (Grant Thornton) is the U.S. member firm of Grant Thornton International Ltd, one of the world’s leading organizations of independent audit, tax and advisory firms. In the United States, Grant Thornton has revenue in excess of $1.3 billion and operates 57 offices with more than 500 partners and 6,000 employees. Grant Thornton works with a broad range of dynamic publicly and privately held companies, government agencies, financial institutions, and civic and religious organizations.

“Grant Thornton” refers to Grant Thornton LLP, the U.S. member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. Services are delivered by the member firms. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another’s acts or omissions. Please see grantthornton.com for further details.
Financial Executives Research Foundation gratefully acknowledges these companies for their support and generosity:

**Platinum Major Gift | $50,000+**
Exxon Mobil Corporation
Microsoft Corporation

**Gold President’s Circle | $10,000–$14,999**
Cisco Systems Inc.
Dow Chemical Company
General Electric Co.
Wells Fargo & Company

**Silver President’s Circle | $5,000–$9,999**
Accenture LLP
Apple Inc.
The Boeing Company
Comcast Corporation
Corning Incorporated
Cummins Inc.
Dell Inc.
DuPont
Eli Lilly and Company
GM Foundation
Halliburton
IBM Corporation
Johnson & Johnson
Lockheed Martin Corp.
McDonald’s Corporation
Medtronic Inc.
MetLife
PepsiCo, Inc.
Pfizer Inc.
Procter & Gamble Co.
Tenneco
Tyco International
Wal-Mart Stores Inc.
CCPA And Beyond—Where Is Privacy Headed

Presented By:

Jonathan A. “Jon” Neiditz
Kilpatrick Townsend & Stockton LLP
Atlanta, GA
Knowledge Assets and the Futures of Privacy and Cybersecurity Regulation

Jon Neiditz
October, 2018
The Second Annual Study on the Cybersecurity Risk to Knowledge Assets, produced by the Ponemon Institute and Kilpatrick Townsend, was done to see whether and in what ways organizations are beginning to focus on safeguarding “knowledge assets” (also often known as “crown jewels”) in a period of targeted attacks on those assets.

“Knowledge assets” are defined as confidential information critical to the development, performance and marketing of a company’s core business, other than personal information that would trigger notice requirements under law. For example, they include:

- trade secrets and corporate confidential information such as product design, development or pricing;
- sensitive non-public information about the organization, its plans or relationships; and
- competitively valuable or other important information of or about customers, including profiles.

This presentation is about how the study and current developments in privacy, data protection and cybersecurity in Europe and the US may help point us toward better approaches to the protection of data.
The CCPA Overcomes EU’s Disfavoring of Automated Processing

• The EU data protection has for decades – understandably given history – disfavored “automated decision-taking,” and the GDPR now disfavors profiling, creating obstacles for the digital economy.

• Instead, the CCPA treats automated and manual processing equally, and profiles as just another type of personal data.

• In that respect, CCPA creates more of a level playing field between AI and humans, perhaps paving the way for an American GDPR.

• (In cybersecurity, the needs for AI are ever-present.)
The GDPR and CCPA Create the Best Chance for a National Privacy Law

• Complete alignment between tech companies at Senate Commerce on 9/26
  – Uniform Federal preemptive law
  – FTC as regulator

• Senators generally very confused between privacy and cybersecurity

• Privacy advocates will seek “strong” regulation, but nobody is wedded to the details of the CCPA
LabMD and the Quiet Death of the FTC’s Unfairness Cybersecurity Jurisdiction

- The 11th Circuit determines that the “unfairness” consent orders are unconstitutionally vague.
- The deadline for a cert petition passed quietly.
- Where to go from here?
- To get more specific through rules on information security, as the FTC is contemplating, would be a mistake except in setting minimum standards for “low-hanging fruit”
  - the threats change too fast for the FTC to keep up, even if they hire a lot more technologists, and
  - the needs for public-private cybersecurity initiatives transcend FTC-style regulation of whether corporations practice “reasonable” security.
The Net-Net

• Privacy (Data Protection) is a Compliance Framework; Cybersecurity is an Always-Escalating Battle
• The FTC should oversee a national privacy/data protection compliance framework
• Cybersecurity and NIST (US)
• Cybersecurity and NIS (ENISA)
• Cybersecurity Regulation Beyond GDPR
• Cybersecurity’s Geneva Convention
Framework as Battle Plan

NIST Cybersecurity Framework

**IDENTIFY**
- Asset management
- Business environment
- Governance
- Risk assessment
- Risk management strategy

**PROTECT**
- Awareness control
- Awareness and training
- Data security
- Info protection and procedures
- Maintenance
- Protective technology

**DETECT**
- Anomalies and events
- Security continuous monitoring
- Detection process

**RESPOND**
- Response planning
- Communications
- Analysis
- Mitigation
- Improvements

**RECOVER**
- Recover planning
- Communications
- Improvements
No Company is Alone

[Diagram showing various sectors and their interconnections, emphasizing the concept of no company being alone in the digital landscape.]
Back to the Study, and the Battle

<table>
<thead>
<tr>
<th>Sample response</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling frame</td>
<td>17,991</td>
<td>17,540</td>
</tr>
<tr>
<td>Total returns</td>
<td>709</td>
<td>691</td>
</tr>
<tr>
<td>Rejected or screened surveys</td>
<td>75</td>
<td>88</td>
</tr>
<tr>
<td>Final sample</td>
<td>634</td>
<td>603</td>
</tr>
<tr>
<td>Response rate</td>
<td>3.5%</td>
<td>3.4%</td>
</tr>
</tbody>
</table>
Current position within the organization

- Senior Executive: 16%
- Vice President: 35%
- Director: 21%
- Manager: 14%
- Supervisor: 9%
- Technician: 3%
- Staff: 2%
The primary person reported to within the organization:

- Chief Information Officer (CIO) 51%
- Chief Information Security Officer (CISO) 22%
- Chief Risk Officer (CRO) 7%
- Compliance Officer 4%
- General Counsel 3%
- Chief Security Officer (CSO) 1%
- Chief Financial Officer (CFO) 9%
- CEO/Executive Committee 4%
- Human Resources VP 22%
Primary industry classification

- Financial services
- Public sector
- Industrial & manufacturing
- Health & pharmaceutical
- Retail
- Services
- Technology & software
- Consumer products
- Energy & utilities
- Communications
- Hospitality & leisure
- Education & research
- Transportation
- Other
Worldwide headcount of the organization

- Less than 500: 7%
- 500 to 1,000: 12%
- 1,001 to 5,000: 9%
- 5,001 to 25,000: 18%
- 25,001 to 50,000: 27%
- 50,001 to 75,000: 19%
- More than 75,000: 8%
What are your crown jewels?
New study: Increased threats and awareness

*Very likely and Likely responses combined*

- Likely and Very likely responses for data breach detection: FY2016: 74%, FY2017: 82%
- Likely and Very likely responses for knowledge assets theft: FY2016: 60%, FY2017: 65%
Evidence of the growing awareness of threats to knowledge assets

- Boards of directors requiring assurances
- Integration into IT security strategy
- Focus on employee carelessness and third party access
- Clear trends in technologies to protect knowledge assets
Some more – but still few – consider their organizations good at this

1 = not effective to 10 = highly effective, 7 + responses reported

FY2016: 28%
FY2017: 35%
For the 65% who don’t think they’ve got this:
What is holding your company back?

More than one response allowed

- Lack of in-house expertise: FY2016 67% FY2017 73%
- Lack of clear leadership: FY2016 59% FY2017 55%
- Lack of collaboration with other functions: FY2016 56% FY2017 53%
- Insufficient staffing: FY2016 38% FY2017 47%
- Insufficient budget (money): FY2016 43% FY2017 42%
- No understanding how to protect against attacks: FY2016 30% FY2017 34%
- Not considered a priority: FY2016 15% FY2017 13%
- Other: FY2016 2% FY2017 1%

Note: More than one response allowed.
For the 35% who think their company is effective: Why?

More than one response allowed

- Restricts access to only those who have a need to know: 64% FY2016, 69% FY2017
- Creates employee awareness about information risk: 56% FY2016, 63% FY2017
- Accomplishes mission within budgetary constraints: 40% FY2016, 63% FY2017
- Prevents attacks that seek to exfiltrate information: 37% FY2016, 35% FY2017
- Innovates in the use of enabling security technologies: 23% FY2016, 29% FY2017
- Detects and contains data breaches quickly: 19% FY2016, 21% FY2017
- Other: 3% FY2016, 4% FY2017

More than one response allowed
The “high performers,” the 14% who rate their firms 9 or 10, are instructive:

- Much greater attention by senior management and the board
- External, third-party audits and regular, customized, actionable training
- More convinced that their knowledge assets are very valuable to a nation state attacker
- Much greater reliance on these 3 techs/processes: access governance, privileged user management and DLP
Perceptions about senior management and boards of directors

Strongly agree and Agree responses combined

- Board of directors requires assurances that knowledge assets are managed and safeguarded appropriately: 52% Overall, 44% Hi Performer
- Senior management understands the risk caused by insecure knowledge assets: 48% Overall, 35% Hi Performer
- Senior management is more concerned about a data breach involving credit card information or Social Security numbers (SSNs) than the leakage of knowledge assets: 42% Overall, 50% Hi Performer
Differences in security practices

Strongly agree and Agree responses combined

- **Employee access is restricted to knowledge assets based on a need to know basis**: 70% Hi Performer vs. 61% Overall
- **Our company is effective in protecting trade secrets**: 61% Hi Performer vs. 50% Overall
- **The theft of knowledge assets is increasing in our company**: 45% Hi Performer vs. 58% Overall
- **All information asset types are considered equal in terms of risk**: 10% Hi Performer vs. 19% Overall
More training/awareness, audits for the handling of insiders (vs. monitoring, evals, incentives)

- Regular training and awareness programs: 83%
- Monitoring of employees: 71%
- Audits and assessments of areas most vulnerable to employee negligence: 55%
- Part of performance evaluations: 38%
- Incentives to stop negligent behavior: 5%
- Other: 3%

# Hi Performer vs. Overall
High performers strongly favor independent 3rd-party audits
Root Causes: Rise of Nation State Attackers

52% of High Performers think their Knowledge Assets are “very valuable” to nation states, vs. 43% of all participants. All participants are increasingly seeing nation-state attacks as “very likely.”

- Very likely: 17% (2016) vs. 25% (2017)
- Somewhat likely: 33% (2016) vs. 36% (2017)
- Not likely: 42% (2016) vs. 35% (2017)
- No chance: 8% (2016) vs. 4% (2017)
Root Causes: Who is responsible?

Careless insider most likely

75% of both High Performers & all respondents rate “employee negligence” “most significant” in 2017

<table>
<thead>
<tr>
<th>Category</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Careless insider</td>
<td>1.67</td>
<td>1.52</td>
</tr>
<tr>
<td>Malicious or criminal insider</td>
<td>2.45</td>
<td>2.33</td>
</tr>
<tr>
<td>External attacker</td>
<td>2.89</td>
<td>3.01</td>
</tr>
<tr>
<td>Combined insider and external attacker</td>
<td>3.49</td>
<td>3.50</td>
</tr>
</tbody>
</table>
Root Causes: Attacker motives

Economic espionage most likely, particularly when one considers such espionage by nation states.

- Economic espionage: 2016 - 1.78, 2017 - 1.88
- Hackivism: 2016 - 2.73, 2017 - 2.64
- Sabotage: 2016 - 3.62, 2017 - 3.54
The knowledge-asset-type security gap

Three responses allowed

- Most valuable asset
- Asset appropriately secured
- Most difficult to secure

<table>
<thead>
<tr>
<th>Asset Type</th>
<th>Most Valuable</th>
<th>Appropriately Secured</th>
<th>Difficult to Secure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private communications</td>
<td>45%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Product/Market Information</td>
<td>27%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presentations</td>
<td>24%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Source code</td>
<td>32%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trade secrets</td>
<td>33%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business correspondence</td>
<td>15%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Confidential information</td>
<td>26%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operational information</td>
<td>32%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial information</td>
<td>19%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Research results</td>
<td>13%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Consumer data</td>
<td>10%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Analytics</td>
<td>16%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileged information</td>
<td>8%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The knowledge-asset-type security gap

Three responses allowed

- Private communications
- Product / Market Information
- Presentations
- Source code
- Trade secrets
- Business correspondence
- Company confidential information
- Operational information
- Financial information
- Research results
- Consumer data
- Analysis
- Privileged information

- Most valuable asset
- Asset appropriately secured
- Most difficult to secure
The knowledge-asset-type security gap

Three responses allowed

- Most valuable asset
- Asset appropriately secured
- Most difficult to secure

Private communications
Product / Market Information
Presentations
Source code
Trade secrets
Business correspondence
Company / confidential information
Operational information
Financial information
Research results
Consumer data
Analysis
Privileged information

<table>
<thead>
<tr>
<th>Asset Type</th>
<th>Most Valuable</th>
<th>Asset Appropriately Secured</th>
<th>Most Difficult to Secure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private communications</td>
<td>45%</td>
<td>27%</td>
<td>15%</td>
</tr>
<tr>
<td>Product / Market Information</td>
<td>65%</td>
<td>10%</td>
<td>15%</td>
</tr>
<tr>
<td>Presentations</td>
<td>45%</td>
<td>36%</td>
<td>26%</td>
</tr>
<tr>
<td>Source code</td>
<td>50%</td>
<td>33%</td>
<td>32%</td>
</tr>
<tr>
<td>Trade secrets</td>
<td>51%</td>
<td>51%</td>
<td>32%</td>
</tr>
<tr>
<td>Business correspondence</td>
<td>46%</td>
<td>46%</td>
<td>15%</td>
</tr>
<tr>
<td>Company / confidential information</td>
<td>26%</td>
<td>26%</td>
<td>19%</td>
</tr>
<tr>
<td>Operational information</td>
<td>41%</td>
<td>41%</td>
<td>32%</td>
</tr>
<tr>
<td>Financial information</td>
<td>45%</td>
<td>45%</td>
<td>19%</td>
</tr>
<tr>
<td>Research results</td>
<td>35%</td>
<td>35%</td>
<td>19%</td>
</tr>
<tr>
<td>Consumer data</td>
<td>32%</td>
<td>32%</td>
<td>19%</td>
</tr>
<tr>
<td>Analysis</td>
<td>45%</td>
<td>35%</td>
<td>13%</td>
</tr>
<tr>
<td>Privileged information</td>
<td>52%</td>
<td>20%</td>
<td>8%</td>
</tr>
</tbody>
</table>
Note that the high performers are making strides here as well, even for private communications.
Trends in overall security technologies for protecting knowledge assets

Eight responses allowed

- Identity management & authentication
- Security information and event management (SIEM)
- Endpoint management systems
- Tokenization technology
- Web application firewalls (WAF)
- Mobile device management (MDM)
- Anti-virus & anti-malware
- Penetration testing
- Big data analytics

FY2016 vs FY2017
What technologies are used to secure access to knowledge assets?

Three responses allowed

- Identity & Access Management (IAM): 67%
- Access Monitoring & Tracking: 59%
- Access Governance: 53%
- Governance, Risk & Compliance (GRC): 53%
- Privileged User Management: 47%
- User Behavior Analytics (UBA): 45%
- Data Loss Prevention (DLP): 44%
- Digital Rights Management: 29%
- Other: 5%
High performers rely more on 4 technologies

<table>
<thead>
<tr>
<th>Category</th>
<th>Hi Performer</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity &amp; Access Management</td>
<td>73%</td>
<td>67%</td>
</tr>
<tr>
<td>Privileged User Management</td>
<td>64%</td>
<td>47%</td>
</tr>
<tr>
<td>Access Governance</td>
<td>62%</td>
<td>53%</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>56%</td>
<td>44%</td>
</tr>
</tbody>
</table>
The mean time to identify (MTTI) a data breach involving knowledge assets caused by a careless insider or malicious outsider (in DAYS)

Mean time to identify (MTTI) a data breach involving a knowledge asset caused by a malicious outsider

Mean time to identify (MTTI) a data breach involving a knowledge asset caused by a careless insider
The mean time to contain (MTTC) a data breach involving knowledge assets caused by a careless insider or malicious outsider (in DAYS)

- Mean time to contain (MTTC) a data breach involving a knowledge asset caused by a malicious outsider: 152.7 days
- Mean time to contain (MTTC) a data breach involving a knowledge asset caused by a careless insider: 76.3 days

Bar chart showing the comparison between high performers and overall averages.
Some Parting Questions – L’Envoi

• When is the joint regulation of privacy and cybersecurity
  – More helpful than not?
  – More harmful than not?

• What would a good cybersecurity agency be and do?

• What traits of a good CISO are not generally traits of a
good CPO, and vice versa?
Questions About the Study

Ponemon Institute
Toll Free: 800.887.3118
Michigan HQ: 2308 US 31 N.
Traverse City, MI 49686 USA
research@ponemon.org

Jon Neiditz
jneiditz@kilpatricktownsend.com
https://www.linkedin.com/in/informationmanagementlaw
404.815.6004

Download the Study:
Caveats

- This study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier Ponemon Institute research. However, there are inherent limitations to benchmark research that need to be carefully considered before drawing conclusions from findings.
- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are familiar with their companies' approach to managing knowledge assets and involved in the process and are located in the United States. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.
The Second Annual Study on the Cybersecurity Risk to Knowledge Assets

Co-authored by Kilpatrick Townsend and Ponemon Institute
Independently conducted by Ponemon Institute LLC
Publication Date: April 2018
The Second Annual Study on the Cybersecurity Risk to Knowledge Assets
Kilpatrick Townsend and Ponemon Institute, April 2018

Part 1. Introduction

The Second Annual Study on the Cybersecurity Risk to Knowledge Assets\(^1\), produced in collaboration between Kilpatrick Townsend and Ponemon Institute, was done to see whether and in what ways organizations are beginning to focus on how they are safeguarding confidential information critical to the development, performance and marketing of their core businesses in a period of targeted attacks on these assets.

Ponemon Institute surveyed 634 IT security practitioners who are familiar and involved with their organization’s approach to managing knowledge assets. All organizations represented in this study have a program or set of activities for managing knowledge assets. The first study, *Cybersecurity Risk to Knowledge Assets*, was released in July 2016.

**Awareness of the risk to knowledge assets increases.** As shown in Figure 1, more respondents acknowledge that their companies very likely failed to detect a breach involving knowledge assets (an increase from 74 percent of respondents in 2016 to 82 percent of respondents in this year’s research). Moreover, in this year’s research, 65 percent of respondents are aware that one or more pieces of the company’s knowledge assets are now in the hands of a competitor, an increase from 60 percent of respondents in the 2016 study.

**Figure 1. The likelihood high value assets have been breached and possibly in the possession of a competitor**

\[\text{Very likely and Likely responses combined}\]

<table>
<thead>
<tr>
<th>FY2016</th>
<th>FY2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>74%</td>
<td>82%</td>
</tr>
<tr>
<td>60%</td>
<td>65%</td>
</tr>
</tbody>
</table>

**The cost to recover from an attack against knowledge assets increases.** The average total cost incurred by organizations represented in this research due to the loss, misuse or theft of knowledge assets over the past 12 months increased 26 percent from $5.4 million to $6.8 million.

---

\(^1\) These knowledge assets do not include personal information that triggers notice requirements when a data breach occurs. Knowledge assets may include trade secrets and corporate confidential information such as profiles of high-value customers, product design, development and pricing, pre-release financial reports, strategic plans, confidential information about existing relationships or contemplated transactions, source code, or research and development secrets, any of which may reside within the company or with its partners or vendors.
Eighty-four percent of respondents state that the maximum loss their organizations could experience as a result of a material breach of knowledge assets is greater than $100 million as compared to 67 percent of respondents in 2016.

Actions taken that support the growing awareness of the risk to knowledge assets

Following are findings that illustrate how the growing awareness of the risk to knowledge assets is improving cybersecurity practices in many of the companies represented in this study.

- Companies are making the protection of knowledge assets an integral part of their IT security strategy (68 percent of respondents vs. 62 percent of respondents in 2016).
- Boards of directors are requiring assurances that knowledge assets are managed and safeguarded appropriately (58 percent of respondents vs. 50 percent of respondents in 2016).
- Companies are addressing the risk of employee carelessness in the handling of knowledge assets. Specifically, training and awareness programs are focused on decreasing employee errors in the handling of sensitive and confidential information (73 percent of respondents) and confirming employees' understanding and ability to apply what they learn to their work (68 percent of respondents).
- Companies are adopting specific technologies designed to protect knowledge assets. The ones for which use is increasing most rapidly include big data analytics, identity management and authentication and SIEM.
- There is a greater focus on assessing which knowledge assets are more difficult to secure and will require stricter safeguards for their protection. These are presentations, product/market information and private communications.
- There is greater recognition that third party access to a company’s knowledge assets is a significant risk. As a result, more companies are requiring proof that the third party meets generally accepted security requirements (an increase from 31 percent of respondents in 2016 to 41 percent in this year’s study) and proof that the third party adheres to compliance mandates (an increase from 25 percent of respondents in 2016 to 34 percent in this year’s study).
- Companies are aware that nation-state attackers are targeting their company’s knowledge assets (an increase from 50 percent to 61 percent in this year’s study) and 79 percent of respondents believe their companies’ trade secrets or knowledge assets are very valuable or valuable to a nation-state attacker.

Best practices and insights of organizations most effective in safeguarding knowledge assets

As part of the research, we did a special analysis of those respondents (89 respondents out of the total sample of 634 respondents) who rated their organizations’ effectiveness in protecting their knowledge assets as very high (9+ on a scale of 1 = not effective to 10 = highly effective). In this study, effectiveness means mitigating the loss or theft of knowledge assets by insiders and external attackers.

Following are characteristics of high performing organizations:

- Senior management and boards of directors in high performing organizations are more concerned about the leakage of their organizations’ knowledge assets and require assurances that knowledge assets are managed and safeguarded appropriately.
High performing organizations are more likely to restrict employee access to knowledge assets based on need to know.

High performing organizations are more likely to conduct audits to ensure adherence to their practices and policies that safeguard knowledge assets. They are significantly more likely to have independent audits by third parties.

High performing organizations are more likely to conduct regular training and awareness programs and audits and assessments of areas most vulnerable to employee negligence.

High performing organizations say a key characteristic of their training programs is the ability to result in a decrease of employee errors in the handling of sensitive and confidential information. Their training programs are more likely to be able to determine employees’ understanding and ensure employees are able to apply what they learn to their work. The programs are also customized based on the role and handling of sensitive and confidential information.

High-value knowledge assets are more secure in high performing organizations. Six knowledge assets that high performing organizations are more effective in safeguarding are source code, financial information, trade secrets, company-confidential information, private communications and analytics.

High performing organizations are more likely to use certain technologies and processes specifically used to protect knowledge assets. More respondents in high performing organizations report they are using identity & access management, privileged user management, access governance and data loss prevention.

High performing organizations are more likely than other organizations to detect and contain breaches of knowledge assets. More high performing organizations are restricting access to only those who have a need to know and a role in the prevention of breaches.

More high performing organizations have achieved a mature level of digital transformation and have either deployed many digital transformation activities across the enterprise or have core digital transformation activities deployed. They are also more likely to say it is important to balance the security of their high value assets while enabling the free flow of information and an open business model.

High performing organizations are faster at identifying a data breach involving knowledge assets caused by a malicious outsider or careless insider. High performing organizations on average reduce the (MTTI) to identify a data breach involving a knowledge asset caused by a malicious outsider by more than 90 days and the MTTI to identify a breach by a careless insider by 58 days.

High performing organizations are faster at containing a data breach involving knowledge assets caused by a malicious outsider or careless insider. High performing organizations on average reduce the (MTTC) to identify a data breach involving a knowledge asset caused by a malicious outsider by more than 34 days and the MTTC to identify a breach by a careless insider by 32.54 days.
Part 2. Key findings

This section provides a more detailed analysis of the findings. The complete audited findings are presented in the Appendix of this report. The report is organized according to the following themes.

- Awareness grows about the vulnerability of knowledge assets to security exploits
- The insider threat to knowledge assets
- Trends in the risk to knowledge assets
- Governance practices for knowledge assets
- The cost of an insider or malicious outsider attack on knowledge assets
- The practices of organizations highly effective in safeguarding knowledge assets

**Awareness grows about the vulnerability of knowledge assets to security exploits**

**Insiders pose the greatest risk to knowledge assets.** Respondents were asked to rank the most likely root causes involving the loss or theft of knowledge assets from 1 = most likely to 4 = least likely. As shown in Figure 2, the most likely causes are careless insiders and malicious or criminal insiders. These root causes have increased in likelihood since 2016.

**Figure 2. What are the most likely root causes of data breaches involving your company's knowledge assets?**

<table>
<thead>
<tr>
<th>Root Cause</th>
<th>FY2016</th>
<th>FY2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Careless insider</td>
<td>1.67</td>
<td>1.52</td>
</tr>
<tr>
<td>Malicious or criminal insider</td>
<td>2.45</td>
<td>2.33</td>
</tr>
<tr>
<td>External attacker</td>
<td>2.89</td>
<td>3.01</td>
</tr>
<tr>
<td>Combined insider and external attackers</td>
<td>3.49</td>
<td>3.50</td>
</tr>
</tbody>
</table>
Economic espionage and hacktivism are the main motivations of attackers. Respondents were asked to rank the motivations of attackers from 1 = most likely to 4 = least likely. According to Figure 3, the most likely motivations are economic espionage and hacktivism. The third most likely motive is cyber warfare or nation-state attacks.

**Figure 3. Why are attackers motivated to steal knowledge assets?**
1 = most likely to 4 = least likely

<table>
<thead>
<tr>
<th></th>
<th>FY2016</th>
<th>FY2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economic espionage</td>
<td>1.78</td>
<td>1.88</td>
</tr>
<tr>
<td>Hacktivism</td>
<td>2.73</td>
<td>2.64</td>
</tr>
<tr>
<td>Cyber warfare</td>
<td>3.26</td>
<td>3.39</td>
</tr>
<tr>
<td>Sabotage</td>
<td>3.62</td>
<td>3.54</td>
</tr>
</tbody>
</table>

Awareness about the possibility of a nation-state attack against knowledge assets increases. As shown in Figure 4, the likelihood of a nation state attacker targeting a company’s knowledge assets is increasing from 50 percent of respondents (17 percent + 33 percent) to 61 percent of respondents (25 percent + 36 percent).

**Figure 4. Do you believe nation state attackers target your company’s knowledge assets?**

<table>
<thead>
<tr>
<th></th>
<th>FY2016</th>
<th>FY2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, very likely</td>
<td>17%</td>
<td>25%</td>
</tr>
<tr>
<td>Yes, somewhat likely</td>
<td>33%</td>
<td>36%</td>
</tr>
<tr>
<td>No, not likely</td>
<td>42%</td>
<td>35%</td>
</tr>
<tr>
<td>No chance</td>
<td>8%</td>
<td>4%</td>
</tr>
</tbody>
</table>
If respondents are aware of the possibility their companies’ knowledge assets have been targeted, only half say it is because of root cause or forensic analysis, according to Figure 5. However, 47 percent of respondents say it was gut feel. Forty-two percent of respondents say it was the signature of the attack and 31 percent of respondents say it was an alert from peers and/or law enforcement.

Figure 5. If likely, how do you know if nation state attackers have targeted your company’s knowledge assets?

More than one response allowed

<table>
<thead>
<tr>
<th>Reason</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root cause (forensic) analysis</td>
<td>50%</td>
</tr>
<tr>
<td>Gut feel</td>
<td>47%</td>
</tr>
<tr>
<td>Signature of the attack</td>
<td>42%</td>
</tr>
<tr>
<td>Alert from peers and/or law enforcement</td>
<td>31%</td>
</tr>
<tr>
<td>Geo-location of the attacker</td>
<td>27%</td>
</tr>
<tr>
<td>Contact from the attacker</td>
<td>19%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
</tr>
</tbody>
</table>

0% 10% 20% 30% 40% 50% 60%
There is a gap in the ability to secure the most valuable knowledge assets. Figure 6 presents 13 types of knowledge assets and responses to the following questions: What knowledge assets are most valuable to a nation state attacker or competitor, what knowledge assets are most difficult to secure and what knowledge assets are appropriately secured?

As shown, private communications (i.e. emails, texting, social media) are considered most valuable to nation state attackers or competitors (45 percent of respondents). However, only 16 percent of respondents say these knowledge assets are appropriately secured. Seventy-two percent of respondents say these assets are difficult to secure.

Knowledge assets that are typically well-secured are attorney-client privileged information and knowledge assets recognized as trade secrets (52 percent and 51 percent of respondents, respectively). Also difficult to secure are product/market information and presentations (65 percent and 52 percent of respondents, respectively).

Figure 6. The knowledge asset security gap
Three responses allowed
The insider threat to knowledge assets

More companies are taking steps to address the risk of employee carelessness in the handling of knowledge assets. Because the careless insider seems to pose the greatest threat to knowledge assets, 67 percent of respondents say their organization takes steps to address the risk of employee carelessness in the handling of knowledge assets, an increase from 61 percent in the 2016 research.

Of the 67 percent of respondents who say their organization takes steps, 71 percent of respondents say they conduct regular training and awareness programs and 69 percent of respondents say they are monitoring employees, as shown in Figure 7.

Figure 7. What steps does your organization take to reduce the careless insider risk?
More than one response allowed
The goal of training programs is to reduce employees’ errors in the handling of sensitive and confidential information. Figure 8 shows what respondents believe should be the most important goals for a training program. The number one component is a reduction in employee errors (73 percent of respondents) followed by the ability to determine if employees not only understand how to reduce the risk of carelessness but apply it to their work (68 percent of respondents). The cost-effectiveness of the program ranked third at 65 percent.

Figure 8. The most important components of a training and awareness program
Three responses allowed

- Training results in a decrease of employee errors in the handling of sensitive and confidential information (73%)
- Ability to determine employees’ understanding and ability to apply what they learn to their work (68%)
- Training is cost effective (65%)
- Training is customized based on the role and handling of sensitive and confidential information (51%)
- Proof of training results in a reduction in corporate liability (43%)
- Ability to measure employees’ retention of the course content (24%)
- Other (2%)
In most companies, ordinary users are not restricted from access to knowledge assets. Only 14 percent of respondents say their organizations only permit privileged users to access knowledge assets, as shown in Figure 9. In the context of this study, privileged users in this research are individuals who are assigned broad access rights to IT networks, enterprise systems, applications and knowledge assets based on their roles and responsibilities within the organization. Fifty-two percent of respondents say both privileged and ordinary users have access to knowledge assets.

Figure 9. In the normal course of business, who has access to your company’s knowledge assets?

The top three technologies and processes used to ensure secure access are identity and access management (IAM) (67 percent of respondents), access monitoring and tracking (59 percent of respondents) and access governance (53 percent of respondents), as shown in Figure 10.

Figure 10. What technologies are used to ensure secure access to knowledge assets?

Three responses allowed

- Identity & Access Management (IAM)
- Access Monitoring & Tracking
- Access Governance
- Governance, Risk & Compliance (GRC)
- Privileged User Management
- User Behavior Analytics (UBA)
- Data Loss Prevention (DLP)
- Digital Rights Management
- Other
Trends in the risks to knowledge assets

Third party access to knowledge assets without appropriate security is a risk. Sixty-nine percent of respondents are concerned that third party access to knowledge assets is a serious risk to their organizations.

Sixty-one percent of respondents say third parties have access to their company’s knowledge. Figure 13 reveals the steps organizations take to ensure the knowledge assets shared with third parties are protected. Most rely upon contracts with indemnification by the third party (48 percent of respondents). There are, however, interesting trends since 2016. More companies are requiring proof that the third party meets generally accepted security requirements (41 percent of respondents vs. 31 percent of respondents in 2016) and proof that the third party adheres to compliance mandates (25 percent of respondents vs. 34 percent of respondents in 2016).

Figure 11. How companies ensure third parties protect knowledge assets
More than one response allowed
Businesses are embracing the digital economy, but it puts knowledge assets at risk. The digital economy has been described as the worldwide network of economic activities, commercial transactions and professional interactions that are enabled by information and communications technologies.²

According to Figure 12, 68 percent of respondents say their business goals will increasingly depend upon the digital economy to be competitive and 60 percent of respondents say a platform-based business model and collaboration with digital partners is critical to success.

However, 65 percent of respondents recognize that the digital economy will significantly increase the risk to high value assets such as intellectual property and trade secrets. The challenge for companies is being able to balance the security of high value assets while still enabling the free flow of information and an open business model.

Figure 12. Perceptions about the risk to knowledge assets in the digital economy
Strongly agree and Agree responses combined

<table>
<thead>
<tr>
<th>Perception</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is important to balance the security of our high value assets while enabling the free flow of information and an open business model</td>
<td>75%</td>
</tr>
<tr>
<td>Business goals will increasingly depend upon the digital economy to be competitive</td>
<td>68%</td>
</tr>
<tr>
<td>The digital economy significantly increases risk to high value assets such as our intellectual property, trade secrets and so forth</td>
<td>65%</td>
</tr>
<tr>
<td>A platform-based business model and collaboration with digital partners is critical to success</td>
<td>60%</td>
</tr>
</tbody>
</table>

² The Digital Economy by Margaret Rouse, Search CIO.com, TechTarget, September 6, 2017
More companies are using identity management & authentication and SIEM to protect knowledge assets. Figure 13 presents trends in the technologies companies are deploying to protect knowledge assets. While the use of endpoint management systems, tokenization, mobile device management and anti-virus & anti-malware technologies have declined, Identity management and authentication, security information and event management (SIEM) and web application firewalls (WAF) have increased in use.

Figure 13. Trends in the use of enabling security technologies for protecting knowledge assets

Eight responses allowed
Companies' effectiveness in protecting knowledge assets remains low. Respondents were asked to rank their effectiveness in protecting knowledge assets on a scale of 1 = not effective to 10 = effective. As shown in Figure 14, those respondents ranking their organizations as highly effective in protecting knowledge assets (7+ respondents) increased from 28 percent in 2016 to 35 percent in this year's research.

**Figure 14. Effectiveness in protecting knowledge assets**

1 = not effective to 10 = highly effective, 7+ responses reported
Reasons for not having an effective approach to the protection of knowledge assets are due to lack of in-house expertise and staffing. Those 65 percent of respondents who rate their organizations as not effective (a rating of 6 or lower) believe it is due to lack of in-house expertise (73 percent of respondents), lack of clear leadership (55 percent of respondents) and lack of collaboration with other functions (55 percent of respondents).

The most significant trends in barriers to effectiveness are the lack of in-house expertise (an increase from 67 percent of respondents in 2016 to 73 percent in this year’s research) and insufficient staffing (an increase from 38 percent of respondents in 2016 to 47 percent of respondents in this year’s research), as shown in Figure 15.

Figure 15. What prevents your company from being very effective?
More than one response allowed

- Lack of in-house expertise: 67% to 73%
- Lack of clear leadership: 59% to 55%
- Lack of collaboration with other functions: 56% to 53%
- Insufficient staffing: 38% to 47%
- Insufficient budget (money): 43% to 42%
- No understanding how to protect against attacks: 30% to 34%
- Not considered a priority: 15% to 13%
- Other: 2% to 1%

# FY2016  # FY2017
Those 35 percent of respondents who rate their organizations as effective (7+ respondents) say it is because it restricts access to only those who have a need to know (69 percent of respondents) and creates employee awareness about information risk (63 percent of respondents), as shown in Figure 16.

**Figure 16. Why is your company effective?**
More than one response allowed

<table>
<thead>
<tr>
<th>Reason</th>
<th>FY2016</th>
<th>FY2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricts access to only those who have a need to know</td>
<td>64%</td>
<td>69%</td>
</tr>
<tr>
<td>Creates employee awareness about information risk</td>
<td>56%</td>
<td>63%</td>
</tr>
<tr>
<td>Accomplishes mission within budgetary constraints</td>
<td>40%</td>
<td>35%</td>
</tr>
<tr>
<td>Prevents attacks that seek to exfiltrate information</td>
<td>37%</td>
<td>35%</td>
</tr>
<tr>
<td>Innovates in the use of enabling security technologies</td>
<td>23%</td>
<td>29%</td>
</tr>
<tr>
<td>Detects and contains data breaches quickly</td>
<td>19%</td>
<td>21%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Governance practices for knowledge assets

**More boards of directors are informed about data breaches involving knowledge assets.** According to Figure 17, the awareness of boards of directors about the loss or theft of knowledge assets increased from 23 percent of respondents to 31 percent of respondents.

**Figure 17. Is your company’s board of directors made aware of breaches involving the loss or theft of knowledge assets?**

<table>
<thead>
<tr>
<th>Yes, all breaches</th>
<th>Yes, only material breaches</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>23%</td>
<td>50%</td>
<td>27%</td>
</tr>
<tr>
<td>31%</td>
<td>51%</td>
<td>18%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FY2016</th>
<th>FY2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>10%</td>
</tr>
<tr>
<td>20%</td>
<td>30%</td>
</tr>
<tr>
<td>40%</td>
<td>50%</td>
</tr>
<tr>
<td>60%</td>
<td>70%</td>
</tr>
</tbody>
</table>
More boards of directors require assurances that knowledge assets are managed and safeguards appropriately. Since 2016, the requirement for assurance that knowledge assets are protected has increased from 37 percent of respondents to 44 percent of respondents, as shown in Figure 18.

Figure 18. Perceptions about governance for knowledge assets
Strongly agree and Agree responses combined
The cost of an insider or malicious outsider attack on knowledge assets

In the aftermath of an attack against knowledge assets, most costs are related to the restoration of reputation and brand. The average total cost incurred by organizations represented in this research due to the loss, misuse or theft of knowledge assets over the past 12 months increased 26 percent from $5.4 million to $6.8 million. As shown in Figure 19, 40 percent of this cost is spent on mitigating the consequences of reputation loss and brand damage.

Figure 19. The allocation of total costs for attacks against knowledge assets

- Revenue loss and customer turnover (churn): 44%
- Remediation & technical support activities: 17%
- Reputation loss and brand damage: 11%
- Users’ downtime and lost productivity: 12%
- Fines, penalties and lawsuits *: 9%
- Damage or theft of IT assets and infrastructure: 8%
- Disruptions to normal business operations *: 5%

* Not a response in FY2016

FY2016 FY2017
The time to identify and contain a data breach involving knowledge assets is greater for malicious outsiders than careless insiders. In this year’s study, we asked respondents to estimate the mean time to identify (MTTI) and mean time to contain (MTTC) a data breach involving knowledge assets caused by a careless insider or a malicious outsider. According to the research, on average, it takes 203 days to identify a data breach caused by a careless insider but it takes 323 days to identify a data breach caused by a malicious outsider. Because it takes longer to respond to a malicious outsider, the costs and negative consequences can be greater than for the careless insider.

Figure 20. The mean time to identify (MTTI) a data breach involving knowledge assets caused by a careless insider or malicious outsider

Extrapolated average reported

```
<table>
<thead>
<tr>
<th></th>
<th>Extrapolated average reported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean time to identify</td>
<td></td>
</tr>
<tr>
<td>caused by a malicious</td>
<td>323.3</td>
</tr>
<tr>
<td>outsider</td>
<td></td>
</tr>
<tr>
<td>Mean time to identify</td>
<td>202.6</td>
</tr>
<tr>
<td>caused by a careless</td>
<td></td>
</tr>
<tr>
<td>insider</td>
<td></td>
</tr>
</tbody>
</table>
```

Similarly, it takes less time to contain a data breach caused by a careless insider (76 days vs. 153 days to contain a data breach.

Figure 21. The mean time to contain (MTTC) a data breach involving knowledge assets caused by a careless insider or malicious outsider

```
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean time to contain</td>
<td></td>
</tr>
<tr>
<td>caused by a malicious</td>
<td>152.7</td>
</tr>
<tr>
<td>outsider</td>
<td></td>
</tr>
<tr>
<td>Mean time to contain</td>
<td>76.3</td>
</tr>
<tr>
<td>caused by a careless</td>
<td></td>
</tr>
<tr>
<td>insider</td>
<td></td>
</tr>
</tbody>
</table>
```
The practices of organizations highly effective in safeguarding knowledge assets

As part of the research, we did a special analysis of those respondents (89 respondents out of the total sample of 634 respondents) who rated their organizations’ effectiveness in protecting their knowledge assets as very high (9+ on a scale of 1 = not effective to 10 = highly effective). In this study, effectiveness means mitigating the loss or theft of knowledge assets by insiders and external attackers.

**Senior management and boards of directors are more engaged in the protection of knowledge assets.** As shown in Figure 22, senior management and boards of directors in high performing organizations are more likely to be concerned than the overall sample about the leakage of knowledge assets. They also understand the risk caused by insecure knowledge assets. In addition, boards of directors require assurances that knowledge assets are managed and safeguarded appropriately.

**Figure 22. Perceptions about senior management and boards of directors**

<table>
<thead>
<tr>
<th>Perception</th>
<th>Hi Performer</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Board of directors requires assurances that knowledge assets are managed and safeguarded appropriately</td>
<td>52%</td>
<td>44%</td>
</tr>
<tr>
<td>Senior management understands the risk caused by insecure knowledge assets</td>
<td>48%</td>
<td>35%</td>
</tr>
<tr>
<td>Senior management is more concerned about a data breach involving credit card information or Social Security numbers (SSNs) than the leakage of knowledge assets</td>
<td>42%</td>
<td>50%</td>
</tr>
</tbody>
</table>
High performing organizations believe they are more effective in protecting trade secrets. Seventy percent of respondents in high performing organizations vs. 61 percent of respondents in the overall sample say their organizations restrict employee access to knowledge assets based on a need to know basis. As a consequence, high performing organizations believe they are more effective in protecting trade secrets and the theft of their knowledge assets is not increasing.

**Figure 23. Differences in security practices**
Strongly agree and Agree responses combined

High performing organizations are more likely to conduct audits of practices and policies. Sixty-five percent of respondents in high performing organizations vs. 54 percent of respondents in the overall sample say their organizations conduct audits to ensure adherence to its practices and policies that safeguard knowledge assets. As shown in Figure 24, high performing organizations are more likely to have independent audits by third parties.

**Figure 24. How are audits conducted to ensure adherence to practices and policies that safeguard knowledge assets?**
High performing organizations are more likely to address the risk of employee carelessness in the handling of knowledge assets. Seventy-five percent of respondents in high performing organizations vs. 67 percent of respondents in the overall sample are proactive in trying to reduce the risk of employee carelessness. According to Figure 25, high performing organizations are more likely to conduct regular training and awareness programs and audits and assessments of areas most vulnerable to employee negligence.

Figure 25. What steps does your organization take to minimize employee carelessness in the handling of knowledge assets?
More than one response permitted

- Regular training and awareness programs: 83% (Hi Performer), 71% (Overall)
- Monitoring of employees: 71% (Hi Performer), 69% (Overall)
- Audits and assessments of areas most vulnerable to employee negligence: 55% (Hi Performer), 47% (Overall)
- Part of performance evaluations: 38% (Hi Performer), 39% (Overall)
- Incentives to stop negligent behavior: 5% (Hi Performer), 7% (Overall)
- Other: 3% (Hi Performer), 0% (Overall)
Training in high performing organizations is not “one size fits all”. As shown in Figure 26, 88 percent of high performing organizations say a key characteristic of their training programs is the ability to decrease of employee errors in the handling of sensitive and confidential information vs. 73 percent of respondents in the overall sample.

Seventy-nine percent of respondents in high performing organizations say their training programs are more likely to be able to determine employees’ understanding and improve the ability to apply what they learn to their work. The programs are also customized based on the role and handling of sensitive and confidential information (63 percent vs. 51 percent of respondents). High performing organizations are also more likely to want to ensure the training results in a decrease of employee errors in the handling of sensitive and confidential information.

**Figure 26. Characteristics of high performing training and awareness programs**

More than one response permitted

- Training results in a decrease of employee errors in the handling of sensitive and confidential information: 88% (Hi Performer), 73% (Overall)
- Ability to determine employees’ understanding and ability to apply what they learn to their work: 79% (Hi Performer), 68% (Overall)
- Training is customized based on the role and handling of sensitive and confidential information: 63% (Hi Performer), 51% (Overall)
- Training is cost effective: 62% (Hi Performer), 65% (Overall)
- Proof of training results in a reduction in corporate liability: 39% (Hi Performer), 43% (Overall)
- Ability to measure employees’ retention of the course content: 26% (Hi Performer), 24% (Overall)
- Other: 2%
High value knowledge assets are more secure in high performing organizations. Figure 27 presents six knowledge assets that high performing organizations are more effective in safeguarding: source code, financial information, trade secrets, company-confidential information, private communications and analytics.

**Figure 27. High performing organizations are more effective in securing certain knowledge assets**
More than one response permitted

![Bar chart showing the comparison between Hi Performer and Overall for different knowledge assets](image)

**Figure 28. Technologies or processes used by high performing organizations**
More than one response permitted

![Bar chart showing the comparison between Hi Performer and Overall for different processes](image)
High performing organizations are more likely than other organizations to detect and contain data breaches. According to Figure 29, 35 percent of respondents in high performing organizations are more likely than the overall sample to detect and contain a data breach (35 percent vs. 21 percent of respondents). More high performing organizations are restricting access to only those who have a need to know and prevent attacks that seek to exfiltrate information (44 percent vs. 35 percent of respondents).

**Figure 29. Why are high performing organizations more effective?**

More than one response permitted

<table>
<thead>
<tr>
<th>Reason</th>
<th>Hi Performer</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricts access to only those who have a need to know</td>
<td>78%</td>
<td>69%</td>
</tr>
<tr>
<td>Creates employee awareness about information risk</td>
<td>69%</td>
<td>63%</td>
</tr>
<tr>
<td>Prevents attacks that seek to exfiltrate information</td>
<td>44%</td>
<td></td>
</tr>
<tr>
<td>Accomplishes mission within budgetary constraints</td>
<td>35%</td>
<td>41%</td>
</tr>
<tr>
<td>Innovates in the use of enabling security technologies</td>
<td>37%</td>
<td>29%</td>
</tr>
<tr>
<td>Detects and contains data breaches quickly</td>
<td>21%</td>
<td>35%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
<td>4%</td>
</tr>
</tbody>
</table>
High performing organizations are more effective than other companies keeping knowledge assets out of the hands of competitors. According to Figure 30, 54 percent of respondents in high performing organizations vs. 65 percent of respondents in the overall sample to say it is very likely or somewhat likely that one or more of their knowledge assets has been stolen by a competitor. While all organizations in this research believe it is likely that they failed to detect a data breach involving the loss or theft of knowledge assets, high performing organizations are less likely to say they failed to detect such an incident.

Figure 30. The likelihood that a data breach was not detected and a competitor has your organization’s knowledge assets
Very likely and Somewhat likely responses combined

| likelihood that your company failed to detect a data breach involving the loss or theft of knowledge assets | 76% |
| Likelihood that one or more pieces of your company’s knowledge assets are now in the hands of a competitor | 54% |

0% 10% 20% 30% 40% 50% 60% 70% 80% 90%

= Hi Performer = Overall
More high performing organizations have achieved a mature level of digital transformation. Sixty-four percent of respondents in high performing organizations say they have either deployed many digital transformation activities deployed across the enterprise or have core digital transformation activities deployed, maintained and/or refined across the enterprise. In contrast, only 45 percent of respondents in the overall sample have achieved such maturity.

According to Figure 30, high performing organizations are more likely to say their business goals will increasingly depend upon the digital economy to be competitive. They are also more likely to say it is important to balance the security of their high value assets while enabling the free flow of information and an open business model.

Figure 31. Perceptions about knowledge assets in the digital economy
Strongly agree and Agree responses combined

<table>
<thead>
<tr>
<th>Perception</th>
<th>Hi Performer</th>
<th>Overall</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is important to balance the security of our high value assets while enabling the free flow of information and an open business model</td>
<td>73%</td>
<td>68%</td>
</tr>
<tr>
<td>Business goals will increasingly depend upon the digital economy to be competitive</td>
<td>81%</td>
<td>75%</td>
</tr>
</tbody>
</table>
High performing organizations are faster at identifying a data breach involving knowledge assets caused by a malicious outsider or careless insider. According to Figure 32, high performing organizations on average reduce the (MTTI) to identify a data breach involving a knowledge asset caused by a malicious outsider by more than 90 days (323.3 – 233) and the MTTI to identify a breach by a careless insider by 58 days (202.6 – 144.6).

Figure 32. The mean time to identify (MTTI) a data breach involving knowledge assets caused by a careless insider or malicious outsider
Extrapolated values reported
High performing organizations are faster at containing a data breach involving knowledge assets caused by a malicious outsider or careless insider. According to Figure 33, high performing organizations on average reduce the (MTTC) to identify a data breach involving a knowledge asset caused by a malicious outsider by more than 34 days (152.7 - 118) and the MTTC to identify a breach by a careless insider by 32.54 days (76.3 – 43.76).

Figure 33. The mean time to contain (MTTC) a data breach involving knowledge assets caused by a careless insider or malicious outsider
Extrapolated values reported
Part 3. Methods

A sampling frame of 17,991 individuals familiar with and involved in their company’s approach to managing knowledge assets were selected as participants in the research. Table 1 shows 709 total returns. Screening and reliability checks required the removal of 75 surveys. Our final sample consisted of 634 surveys or a 3.5 percent response rate.

<table>
<thead>
<tr>
<th>Table 1. Sample response</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sampling frame</td>
<td>17,991</td>
<td>17,540</td>
</tr>
<tr>
<td>Total returns</td>
<td>709</td>
<td>691</td>
</tr>
<tr>
<td>Rejected or screened surveys</td>
<td>75</td>
<td>88</td>
</tr>
<tr>
<td>Final sample</td>
<td>634</td>
<td>603</td>
</tr>
<tr>
<td>Response rate</td>
<td>3.5%</td>
<td>3.4%</td>
</tr>
</tbody>
</table>

Pie Chart 1 reports the respondents’ organizational levels within the participating organizations. By design, more than half of the respondents (56 percent) are at or above the supervisory levels.

Pie Chart 2 shows that 51 percent of respondents report to the CIO, 22 percent report to the CISO and 9 percent indicated they report to the CRO.
Pie Chart 3 reports the industry segments of respondents’ organizations. This chart identifies financial services (18 percent) as the largest segment, followed by public sector (12 percent), industrial and manufacturing (11 percent), health and pharmaceutical (10 percent) and retail sector (10 percent).

Pie Chart 3. Primary industry classification of respondents’ organizations

As shown in Pie Chart 4, 73 percent of respondents are from organizations with a global headcount of more than 1,000 employees.

Pie Chart 4. Worldwide headcount of the organization
In addition to the United States, 71 percent of respondents indicated their organization has employees located in Canada, 70 percent responded their organization has employees in Europe, 63 percent have employees in Asia-Pacific, 57 percent have employees in Latin America and 46 percent have employees in the Middle East and Africa, as shown in Table 2.

<table>
<thead>
<tr>
<th>Table 2. Global location of employees</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
</tr>
<tr>
<td>Canada</td>
</tr>
<tr>
<td>Europe</td>
</tr>
<tr>
<td>Asia-Pacific</td>
</tr>
<tr>
<td>Latin America (including Mexico)</td>
</tr>
<tr>
<td>Middle East &amp; Africa</td>
</tr>
</tbody>
</table>

Part 4. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- **Non-response bias**: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- **Sampling-frame bias**: The accuracy is based on contact information and the degree to which the list is representative of individuals who are familiar with their companies’ approach to managing knowledge assets and involved in the process and are located in the United States. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result in a different pattern of findings.

- **Self-reported results**: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.
### Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured between December 6, 2017 and December 20, 2017.

<table>
<thead>
<tr>
<th>Survey response</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total sampling frame</td>
<td>17,991</td>
<td>17,540</td>
</tr>
<tr>
<td>Total returns</td>
<td>709</td>
<td>691</td>
</tr>
<tr>
<td>Rejected or screened surveys</td>
<td>75</td>
<td>88</td>
</tr>
<tr>
<td>Final sample</td>
<td>634</td>
<td>603</td>
</tr>
<tr>
<td>Response rate</td>
<td>3.5%</td>
<td>3.4%</td>
</tr>
</tbody>
</table>

### Screening questions

<table>
<thead>
<tr>
<th>S1. How familiar are you with your organization’s approach to managing knowledge assets?</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very familiar</td>
<td>25%</td>
<td>23%</td>
</tr>
<tr>
<td>Familiar</td>
<td>46%</td>
<td>45%</td>
</tr>
<tr>
<td>Somewhat familiar</td>
<td>29%</td>
<td>32%</td>
</tr>
<tr>
<td>No knowledge (Stop)</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>S2. Does your company have a program or set of activities for managing knowledge assets?</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>No (Stop)</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>S3. Do you have any involvement in managing knowledge assets?</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, full involvement</td>
<td>26%</td>
<td>23%</td>
</tr>
<tr>
<td>Yes, partial involvement</td>
<td>49%</td>
<td>51%</td>
</tr>
<tr>
<td>Yes, minimal involvement</td>
<td>25%</td>
<td>26%</td>
</tr>
<tr>
<td>No involvement (Stop)</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>
### Part 2. Attributions: Please rate each of the following statements using the five-point agreement scale provided below each item. % Strongly Agree and Agree response combined.

<table>
<thead>
<tr>
<th>Statement</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1. Senior management makes the protection of knowledge assets a priority.</td>
<td>35%</td>
<td>31%</td>
</tr>
<tr>
<td>Q2. Third party access to our company’s knowledge assets poses a serious risk.</td>
<td>69%</td>
<td>67%</td>
</tr>
<tr>
<td>Q3. All information asset types are considered equal in terms of risk to our company.</td>
<td>19%</td>
<td>22%</td>
</tr>
<tr>
<td>Q4. The protection of knowledge assets is an integral part of our company’s IT security strategy.</td>
<td>68%</td>
<td>62%</td>
</tr>
<tr>
<td>Q5. Our company’s senior management understands the risk caused by insecure knowledge assets.</td>
<td>35%</td>
<td>32%</td>
</tr>
<tr>
<td>Q6. Our company’s senior management is more concerned about a data breach involving credit card information or Social Security numbers (SSNs) than the leakage of knowledge assets.</td>
<td>50%</td>
<td>53%</td>
</tr>
<tr>
<td>Q7. The most significant threat to the security of knowledge assets is employee negligence.</td>
<td>75%</td>
<td>71%</td>
</tr>
<tr>
<td>Q8. Our company restricts employee access to knowledge assets based on a need to know basis.</td>
<td>61%</td>
<td>59%</td>
</tr>
<tr>
<td>Q9. Our company’s board of directors requires assurances that knowledge assets are managed and safeguarded appropriately.</td>
<td>44%</td>
<td>37%</td>
</tr>
<tr>
<td>Q10. The theft of knowledge assets is increasing in our company.</td>
<td>58%</td>
<td>50%</td>
</tr>
<tr>
<td>Q11. The protection of knowledge assets is difficult to achieve in our company.</td>
<td>68%</td>
<td>69%</td>
</tr>
<tr>
<td>Q12. Our company is effective in protecting trade secrets.</td>
<td>50%</td>
<td></td>
</tr>
</tbody>
</table>

### Part 3. Governance & IT security practices

<table>
<thead>
<tr>
<th>Question</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q13. Who is involved in determining your company’s approach for protecting knowledge assets? Please select your top 3 choices.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>General Counsel</td>
<td>42%</td>
<td>39%</td>
</tr>
<tr>
<td>Chief Executive Officer</td>
<td>4%</td>
<td>5%</td>
</tr>
<tr>
<td>Chief Operating Officer</td>
<td>12%</td>
<td>14%</td>
</tr>
<tr>
<td>Chief Compliance Officer</td>
<td>39%</td>
<td>45%</td>
</tr>
<tr>
<td>Chief Financial Officer (CFO)</td>
<td>35%</td>
<td>33%</td>
</tr>
<tr>
<td>Chief Technology Officer (CTO)</td>
<td>13%</td>
<td>14%</td>
</tr>
<tr>
<td>Chief Information Officer (CIO)</td>
<td>53%</td>
<td>56%</td>
</tr>
<tr>
<td>Chief Information Security Officer (CISO)</td>
<td>32%</td>
<td>28%</td>
</tr>
<tr>
<td>Chief Security Officer (CSO)</td>
<td>3%</td>
<td>4%</td>
</tr>
<tr>
<td>Chief Privacy Officer (CPO)</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>Head of Human Resources</td>
<td>19%</td>
<td>21%</td>
</tr>
<tr>
<td>Head of R&amp;D</td>
<td>6%</td>
<td>7%</td>
</tr>
<tr>
<td>Chief Risk Officer (CRO)</td>
<td>30%</td>
<td>26%</td>
</tr>
<tr>
<td>No one person/department</td>
<td>9%</td>
<td>6%</td>
</tr>
<tr>
<td>Total</td>
<td>300%</td>
<td>300%</td>
</tr>
</tbody>
</table>
Q14. Who is most responsible for protecting your company’s knowledge assets?

<table>
<thead>
<tr>
<th>Role</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Counsel</td>
<td>5%</td>
<td>6%</td>
</tr>
<tr>
<td>Chief Executive Officer</td>
<td>8%</td>
<td>10%</td>
</tr>
<tr>
<td>Chief Operating Officer</td>
<td>7%</td>
<td>7%</td>
</tr>
<tr>
<td>Chief Compliance Officer</td>
<td>12%</td>
<td>13%</td>
</tr>
<tr>
<td>Chief Financial Officer (CFO)</td>
<td>5%</td>
<td>6%</td>
</tr>
<tr>
<td>Chief Technology Officer (CTO)</td>
<td>2%</td>
<td>0%</td>
</tr>
<tr>
<td>Chief Information Officer (CIO)</td>
<td>20%</td>
<td>23%</td>
</tr>
<tr>
<td>Chief Information Security Officer (CISO)</td>
<td>15%</td>
<td>12%</td>
</tr>
<tr>
<td>Chief Security Officer (CSO)</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Chief Privacy Officer (CPO)</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Head of human resources</td>
<td>4%</td>
<td>3%</td>
</tr>
<tr>
<td>Head of R&amp;D</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>Chief Risk Officer (CRO)</td>
<td>6%</td>
<td>5%</td>
</tr>
<tr>
<td>No one person/department</td>
<td>16%</td>
<td>15%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q15a. Does your company conduct audits to ensure adherence to its practices and policies that safeguard knowledge assets?

<table>
<thead>
<tr>
<th>Response</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>54%</td>
<td>54%</td>
</tr>
<tr>
<td>No</td>
<td>41%</td>
<td>46%</td>
</tr>
<tr>
<td>Unsure</td>
<td>5%</td>
<td>3%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q15b. If yes, how are these audits conducted? Please select all that apply.

<table>
<thead>
<tr>
<th>Method</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Independent audit by third parties</td>
<td>26%</td>
<td>26%</td>
</tr>
<tr>
<td>Internal audit by in-house experts</td>
<td>40%</td>
<td>40%</td>
</tr>
<tr>
<td>Combination of independent and internal audit</td>
<td>32%</td>
<td>32%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q16a. Does your organization take steps to address the risk of employee carelessness in the handling of knowledge assets?

<table>
<thead>
<tr>
<th>Response</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>67%</td>
<td>61%</td>
</tr>
<tr>
<td>No</td>
<td>26%</td>
<td>30%</td>
</tr>
<tr>
<td>Unsure</td>
<td>7%</td>
<td>9%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q16b. If yes, what steps does it take? Please select all that apply.

<table>
<thead>
<tr>
<th>Step</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regular training and awareness programs</td>
<td>71%</td>
<td>70%</td>
</tr>
<tr>
<td>Monitoring of employees</td>
<td>69%</td>
<td>65%</td>
</tr>
<tr>
<td>Audits and assessments of areas most vulnerable to employee negligence</td>
<td>47%</td>
<td>43%</td>
</tr>
<tr>
<td>Incentives to stop negligent behavior</td>
<td>7%</td>
<td>8%</td>
</tr>
<tr>
<td>Part of performance evaluations</td>
<td>39%</td>
<td>36%</td>
</tr>
<tr>
<td>Other</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>Total</td>
<td>236%</td>
<td>224%</td>
</tr>
</tbody>
</table>
Q17. If your organization has a training and awareness program, what should its most important components be? Please select your top 3 responses. FY2017

<table>
<thead>
<tr>
<th>Component</th>
<th>FY2017 Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to determine employees' understanding and ability to apply what they learn to their work</td>
<td>68%</td>
</tr>
<tr>
<td>Ability to measure employees' retention of the course content</td>
<td>24%</td>
</tr>
<tr>
<td>Training is cost effective</td>
<td>65%</td>
</tr>
<tr>
<td>Training is customized based on the role and handling of sensitive and confidential information</td>
<td>51%</td>
</tr>
<tr>
<td>Training results in a decrease of employee errors in the handling of sensitive and confidential information</td>
<td>73%</td>
</tr>
<tr>
<td>Proof of training results in a reduction in corporate liability</td>
<td>43%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>2%</td>
</tr>
<tr>
<td>Total</td>
<td>326%</td>
</tr>
</tbody>
</table>

Q18. What are the most important enabling security technologies for protecting knowledge assets? Please select 8 top choices. FY2017 FY2016

<table>
<thead>
<tr>
<th>Technology</th>
<th>FY2017 Percentage</th>
<th>FY2016 Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access governance</td>
<td>42%</td>
<td>43%</td>
</tr>
<tr>
<td>Anti-virus &amp; anti-malware</td>
<td>30%</td>
<td>36%</td>
</tr>
<tr>
<td>Big data analytics</td>
<td>21%</td>
<td>15%</td>
</tr>
<tr>
<td>Blockchain</td>
<td>6%</td>
<td></td>
</tr>
<tr>
<td>Code vulnerability scanning and debugging systems</td>
<td>15%</td>
<td>14%</td>
</tr>
<tr>
<td>Data loss prevention (DLP)</td>
<td>45%</td>
<td>48%</td>
</tr>
<tr>
<td>Encryption for data at rest</td>
<td>53%</td>
<td>54%</td>
</tr>
<tr>
<td>Encryption for data in motion</td>
<td>45%</td>
<td>49%</td>
</tr>
<tr>
<td>Endpoint management systems</td>
<td>39%</td>
<td>46%</td>
</tr>
<tr>
<td>Governance, risk and compliance systems (eGRC)</td>
<td>19%</td>
<td>21%</td>
</tr>
<tr>
<td>Hardware security modules (HSM)</td>
<td>40%</td>
<td>39%</td>
</tr>
<tr>
<td>Identity management &amp; authentication</td>
<td>62%</td>
<td>52%</td>
</tr>
<tr>
<td>Intrusion detection systems (IDS)</td>
<td>25%</td>
<td>21%</td>
</tr>
<tr>
<td>Intrusion prevention systems (IPS)</td>
<td>22%</td>
<td>22%</td>
</tr>
<tr>
<td>Mobile device management (MDM)</td>
<td>30%</td>
<td>38%</td>
</tr>
<tr>
<td>Network and traffic intelligence systems</td>
<td>34%</td>
<td>35%</td>
</tr>
<tr>
<td>Next generation firewalls</td>
<td>22%</td>
<td>19%</td>
</tr>
<tr>
<td>Penetration testing</td>
<td>27%</td>
<td>22%</td>
</tr>
<tr>
<td>Secure USB flash device or mobile media</td>
<td>15%</td>
<td>19%</td>
</tr>
<tr>
<td>Security information and event management (SIEM)</td>
<td>52%</td>
<td>47%</td>
</tr>
<tr>
<td>Test data anonymization solution</td>
<td>13%</td>
<td>17%</td>
</tr>
<tr>
<td>Tokenization technology</td>
<td>36%</td>
<td>42%</td>
</tr>
<tr>
<td>Traditional firewalls</td>
<td>42%</td>
<td>40%</td>
</tr>
<tr>
<td>Virtual private networks (VPN)</td>
<td>35%</td>
<td>33%</td>
</tr>
<tr>
<td>Web application firewalls (WAF)</td>
<td>30%</td>
<td>23%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>0%</td>
<td>5%</td>
</tr>
<tr>
<td>Total</td>
<td>800%</td>
<td>800%</td>
</tr>
</tbody>
</table>
Q19. Following are 13 categories of knowledge assets. Please select the three knowledge assets categories that in your experience are most difficult to secure.*

<table>
<thead>
<tr>
<th>Knowledge Asset Category</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source code</td>
<td>50%</td>
<td>51%</td>
</tr>
<tr>
<td>Business correspondence</td>
<td>46%</td>
<td>52%</td>
</tr>
<tr>
<td>Financial information</td>
<td>34%</td>
<td>37%</td>
</tr>
<tr>
<td>Operational information</td>
<td>36%</td>
<td>40%</td>
</tr>
<tr>
<td>Research results</td>
<td>18%</td>
<td>25%</td>
</tr>
<tr>
<td>Attorney-client privileged information</td>
<td>11%</td>
<td>10%</td>
</tr>
<tr>
<td>Presentations</td>
<td>52%</td>
<td>45%</td>
</tr>
<tr>
<td>Product/market information</td>
<td>65%</td>
<td>60%</td>
</tr>
<tr>
<td>Trade secrets</td>
<td>48%</td>
<td>44%</td>
</tr>
<tr>
<td>Company-confidential information</td>
<td>41%</td>
<td>40%</td>
</tr>
<tr>
<td>Private communications (i.e., emails, texting, social media)</td>
<td>72%</td>
<td>67%</td>
</tr>
<tr>
<td>Consumer data</td>
<td>15%</td>
<td>18%</td>
</tr>
<tr>
<td>Analytics</td>
<td>12%</td>
<td>11%</td>
</tr>
<tr>
<td>Total</td>
<td>500%</td>
<td>500%</td>
</tr>
</tbody>
</table>

*FY2016 Allowed 5 responses

Q20. How confident are you that the above 13 knowledge asset categories are appropriately secured within your company? Please rate each information asset category using the following five-point confidence scale: % High confidence response.

<table>
<thead>
<tr>
<th>Knowledge Asset Category</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source code</td>
<td>36%</td>
<td>39%</td>
</tr>
<tr>
<td>Business correspondence</td>
<td>15%</td>
<td>18%</td>
</tr>
<tr>
<td>Financial information</td>
<td>45%</td>
<td>49%</td>
</tr>
<tr>
<td>Operational information</td>
<td>19%</td>
<td>21%</td>
</tr>
<tr>
<td>Research results</td>
<td>35%</td>
<td>41%</td>
</tr>
<tr>
<td>Attorney-client privileged information</td>
<td>52%</td>
<td>50%</td>
</tr>
<tr>
<td>Presentations</td>
<td>16%</td>
<td>19%</td>
</tr>
<tr>
<td>Product/market information</td>
<td>15%</td>
<td>19%</td>
</tr>
<tr>
<td>Trade secrets</td>
<td>51%</td>
<td>45%</td>
</tr>
<tr>
<td>Company-confidential information</td>
<td>23%</td>
<td>24%</td>
</tr>
<tr>
<td>Private communications (i.e., emails, texting, social media)</td>
<td>16%</td>
<td>16%</td>
</tr>
<tr>
<td>Consumer data</td>
<td>32%</td>
<td>28%</td>
</tr>
<tr>
<td>Analytics</td>
<td>20%</td>
<td>24%</td>
</tr>
<tr>
<td>Total</td>
<td>375%</td>
<td>393%</td>
</tr>
</tbody>
</table>

Q21. In the normal course of business, who has access to your company’s knowledge assets?

<table>
<thead>
<tr>
<th>Access Level</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only privileged users</td>
<td>14%</td>
<td>17%</td>
</tr>
<tr>
<td>Privileged users plus a small number or ordinary users</td>
<td>34%</td>
<td>33%</td>
</tr>
<tr>
<td>Both privileged and ordinary users</td>
<td>52%</td>
<td>50%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>
Q22. What technologies or processes are used to ensure secure access to your company’s knowledge assets?  

<table>
<thead>
<tr>
<th>Tech/Process</th>
<th>FY2017</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>User Behavior Analytics (UBA)</td>
<td>45%</td>
<td></td>
</tr>
<tr>
<td>Governance, Risk &amp; Compliance (GRC)</td>
<td>53%</td>
<td></td>
</tr>
<tr>
<td>Digital Rights Management</td>
<td>29%</td>
<td></td>
</tr>
<tr>
<td>Access Governance</td>
<td>53%</td>
<td></td>
</tr>
<tr>
<td>Privileged User Management</td>
<td>47%</td>
<td></td>
</tr>
<tr>
<td>Data Loss Prevention (DLP)</td>
<td>44%</td>
<td></td>
</tr>
<tr>
<td>Identity &amp; Access Management (IAM)</td>
<td>67%</td>
<td></td>
</tr>
<tr>
<td>Access Monitoring &amp; Tracking</td>
<td>59%</td>
<td></td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>5%</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>402%</td>
<td></td>
</tr>
</tbody>
</table>

Q23a. Do third parties have access to your company’s knowledge assets?  

<table>
<thead>
<tr>
<th>Access Status</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>61%</td>
<td>57%</td>
</tr>
<tr>
<td>No</td>
<td>27%</td>
<td>29%</td>
</tr>
<tr>
<td>Unsure</td>
<td>12%</td>
<td>14%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q23b. If yes, how does your company ensure knowledge assets shared with third parties are appropriately protected?  

<table>
<thead>
<tr>
<th>Protection Method</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption or tokenization of data at rest</td>
<td>44%</td>
<td>40%</td>
</tr>
<tr>
<td>Encryption of data in motion</td>
<td>45%</td>
<td>44%</td>
</tr>
<tr>
<td>Contract with indemnification by the third party</td>
<td>48%</td>
<td>50%</td>
</tr>
<tr>
<td>Proof that the third party meets generally accepted security requirements</td>
<td>41%</td>
<td>31%</td>
</tr>
<tr>
<td>Proof that the third party adheres to compliance mandates</td>
<td>34%</td>
<td>25%</td>
</tr>
<tr>
<td>Careful vetting of the third party</td>
<td>36%</td>
<td>33%</td>
</tr>
<tr>
<td>Site visit and assessment of the third party</td>
<td>20%</td>
<td>22%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>268%</td>
<td>284%</td>
</tr>
</tbody>
</table>

Part 4. The threat to knowledge assets  

Q24. Using the following 10-point scale, please rate your company’s effectiveness in protecting its knowledge assets. In the context of this study, effectiveness means mitigating the loss or theft of knowledge assets by insiders and external attackers. 1 = not effective to 10 = very effective.  

<table>
<thead>
<tr>
<th>Rating</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 or 2</td>
<td>8%</td>
<td>11%</td>
</tr>
<tr>
<td>3 or 4</td>
<td>24%</td>
<td>25%</td>
</tr>
<tr>
<td>5 or 6</td>
<td>33%</td>
<td>36%</td>
</tr>
<tr>
<td>7 or 8</td>
<td>21%</td>
<td>18%</td>
</tr>
<tr>
<td>9 or 10</td>
<td>14%</td>
<td>10%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td><strong>Extrapolated value</strong></td>
<td>5.68</td>
<td>5.32</td>
</tr>
</tbody>
</table>
### Q25. For those who rate 6 and below: What prevents your company from being very effective? (FY2017 vs. FY2016)

<table>
<thead>
<tr>
<th>Factor</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insufficient budget (money)</td>
<td>42%</td>
<td>43%</td>
</tr>
<tr>
<td>Insufficient staffing</td>
<td>47%</td>
<td>38%</td>
</tr>
<tr>
<td>Lack of in-house expertise</td>
<td>73%</td>
<td>67%</td>
</tr>
<tr>
<td>Lack of clear leadership</td>
<td>55%</td>
<td>59%</td>
</tr>
<tr>
<td>No understanding how to protect against attacks</td>
<td>34%</td>
<td>30%</td>
</tr>
<tr>
<td>Lack of collaboration with other functions</td>
<td>53%</td>
<td>56%</td>
</tr>
<tr>
<td>Not considered a priority</td>
<td>13%</td>
<td>15%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>1%</td>
<td>2%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>318%</td>
<td>310%</td>
</tr>
</tbody>
</table>

### Q26. For those who rate 7 and above: Why is your company effective? (FY2017 vs. FY2016)

<table>
<thead>
<tr>
<th>Reason</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricts access to only those who have a need to know</td>
<td>69%</td>
<td>64%</td>
</tr>
<tr>
<td>Prevents attacks that seek to exfiltrate information</td>
<td>35%</td>
<td>37%</td>
</tr>
<tr>
<td>Creates employee awareness about information risk</td>
<td>63%</td>
<td>56%</td>
</tr>
<tr>
<td>Accomplishes mission within budgetary constraints</td>
<td>35%</td>
<td>40%</td>
</tr>
<tr>
<td>Innovates in the use of enabling security technologies</td>
<td>29%</td>
<td>23%</td>
</tr>
<tr>
<td>Detects and contains data breaches quickly</td>
<td>21%</td>
<td>19%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>4%</td>
<td>3%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>256%</td>
<td>242%</td>
</tr>
</tbody>
</table>

### Q27. In your opinion, is your company’s board of directors made aware of breaches involving the loss or theft of knowledge assets? (FY2017 vs. FY2016)

<table>
<thead>
<tr>
<th>Awareness Level</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, all breaches</td>
<td>31%</td>
<td>23%</td>
</tr>
<tr>
<td>Yes, only material breaches</td>
<td>51%</td>
<td>50%</td>
</tr>
<tr>
<td>No</td>
<td>18%</td>
<td>27%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

### Q28. In your opinion, what is the likelihood that one or more pieces of your company’s knowledge assets are now in the hands of a competitor? (FY2017 vs. FY2016)

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very likely</td>
<td>30%</td>
<td>24%</td>
</tr>
<tr>
<td>Somewhat likely</td>
<td>35%</td>
<td>36%</td>
</tr>
<tr>
<td>Not likely</td>
<td>27%</td>
<td>30%</td>
</tr>
<tr>
<td>No chance</td>
<td>8%</td>
<td>10%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

### Q29. In your opinion, what is the likelihood that your company **failed to detect** a data breach involving the loss or theft of knowledge assets? (FY2017 vs. FY2016)

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very likely</td>
<td>39%</td>
<td>34%</td>
</tr>
<tr>
<td>Somewhat likely</td>
<td>43%</td>
<td>40%</td>
</tr>
<tr>
<td>Not likely</td>
<td>16%</td>
<td>21%</td>
</tr>
<tr>
<td>No chance</td>
<td>2%</td>
<td>5%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>
Q30. What are the most likely root causes of data breaches involving your company’s knowledge assets? Please rank the following list from 1 = most likely to 4 = least likely.

<table>
<thead>
<tr>
<th>Cause</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Careless insider</td>
<td>1.52</td>
<td>1.67</td>
</tr>
<tr>
<td>Malicious or criminal insider</td>
<td>2.33</td>
<td>2.45</td>
</tr>
<tr>
<td>External attacker</td>
<td>3.01</td>
<td>2.89</td>
</tr>
<tr>
<td>Combined insider and external attackers</td>
<td>3.50</td>
<td>3.49</td>
</tr>
<tr>
<td>Average</td>
<td>2.59</td>
<td>2.63</td>
</tr>
</tbody>
</table>

Q31. What are the main motivations of attackers that seek to steal your company’s knowledge assets? Please rank the following list from 1 = most likely to 4 = least likely.

<table>
<thead>
<tr>
<th>Motivation</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Economic espionage</td>
<td>1.88</td>
<td>1.78</td>
</tr>
<tr>
<td>Sabotage</td>
<td>3.54</td>
<td>3.62</td>
</tr>
<tr>
<td>Hacktivism</td>
<td>2.64</td>
<td>2.73</td>
</tr>
<tr>
<td>Cyber warfare (nation-state attacks)</td>
<td>3.39</td>
<td>3.26</td>
</tr>
<tr>
<td>Average</td>
<td>2.86</td>
<td>2.85</td>
</tr>
</tbody>
</table>

Q32. What best describes the maturity level of your organization’s digital transformation today?

<table>
<thead>
<tr>
<th>Stage</th>
<th>FY2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has not been launched (Skip to Q34a)</td>
<td>5%</td>
</tr>
<tr>
<td>Early stage – many digital transformation activities have not as yet been planned or deployed</td>
<td>19%</td>
</tr>
<tr>
<td>Middle stage – digital transformation activities are planned and defined but only partially deployed</td>
<td>31%</td>
</tr>
<tr>
<td>Late-middle stage – many digital transformation activities are deployed across the enterprise</td>
<td>25%</td>
</tr>
<tr>
<td>Mature stage – Core digital transformation activities are deployed, maintained and/or refined across the enterprise</td>
<td>20%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Please express your opinion about each one of the following statements using the five-point agreement scale provided below each item. % Strongly Agree and Agree response combined.

<table>
<thead>
<tr>
<th>Statement</th>
<th>FY2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q33a. My organization’s business goals will increasingly depend upon the digital economy to be competitive.</td>
<td>68%</td>
</tr>
<tr>
<td>Q33b. In my organization, it is important to balance the security of our high value assets while enabling the free flow of information and an open business model.</td>
<td>75%</td>
</tr>
<tr>
<td>Q33c. In my organization, the digital economy significantly increases risk to high value assets such as our intellectual property, trade secrets and so forth.</td>
<td>65%</td>
</tr>
<tr>
<td>Q33d. In my organization, a platform-based business model and collaboration with digital partners is critical to success.</td>
<td>60%</td>
</tr>
</tbody>
</table>

Q34a. Do you believe nation state attackers target your company’s knowledge assets?

<table>
<thead>
<tr>
<th>Response</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes, very likely</td>
<td>25%</td>
<td>17%</td>
</tr>
<tr>
<td>Yes, somewhat likely</td>
<td>36%</td>
<td>33%</td>
</tr>
<tr>
<td>No, not likely</td>
<td>35%</td>
<td>42%</td>
</tr>
<tr>
<td>No chance</td>
<td>4%</td>
<td>8%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>
Q34b. If likely, how do you know if nation state attackers have targeted your company's knowledge assets? Please select all that apply.

<table>
<thead>
<tr>
<th>Factor</th>
<th>FY2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root cause (forensic) analysis</td>
<td>50%</td>
</tr>
<tr>
<td>Signature of the attack</td>
<td>42%</td>
</tr>
<tr>
<td>Geo-location of the attacker</td>
<td>27%</td>
</tr>
<tr>
<td>Contact from the attacker</td>
<td>19%</td>
</tr>
<tr>
<td>Alert from peers and/or law enforcement</td>
<td>31%</td>
</tr>
<tr>
<td>Gut feel</td>
<td>47%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td>3%</td>
</tr>
<tr>
<td>Total</td>
<td>219%</td>
</tr>
</tbody>
</table>

Q35. How valuable do you believe your trade secrets or knowledge assets are to a nation state attacker?

<table>
<thead>
<tr>
<th>Valuation</th>
<th>FY2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very valuable</td>
<td>45%</td>
</tr>
<tr>
<td>Valuable</td>
<td>34%</td>
</tr>
<tr>
<td>Not valuable</td>
<td>21%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
</tr>
</tbody>
</table>

Q36. Please select the three knowledge assets categories that in your experience would be most valuable to a nation state attacker or competitor?

<table>
<thead>
<tr>
<th>Category</th>
<th>FY2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source code</td>
<td>32%</td>
</tr>
<tr>
<td>Business correspondence</td>
<td>15%</td>
</tr>
<tr>
<td>Financial information</td>
<td>19%</td>
</tr>
<tr>
<td>Operational information</td>
<td>32%</td>
</tr>
<tr>
<td>Research results</td>
<td>13%</td>
</tr>
<tr>
<td>Attorney-client privileged information</td>
<td>8%</td>
</tr>
<tr>
<td>Presentations</td>
<td>24%</td>
</tr>
<tr>
<td>Product/market information</td>
<td>27%</td>
</tr>
<tr>
<td>Trade secrets</td>
<td>33%</td>
</tr>
<tr>
<td>Company-confidential information</td>
<td>26%</td>
</tr>
<tr>
<td>Private communications (i.e., emails, texting, social media)</td>
<td>45%</td>
</tr>
<tr>
<td>Consumer data</td>
<td>10%</td>
</tr>
<tr>
<td>Analytics</td>
<td>16%</td>
</tr>
<tr>
<td>Total</td>
<td>300%</td>
</tr>
</tbody>
</table>
### Part 5. Budget and cost

**Q37.** Approximately, how much was the total cost incurred by your organization due to the loss, misuse or theft of knowledge assets over the past 12 months? Approximately, how much was the total cost due to attacks against knowledge assets over the past 12 months?  

<table>
<thead>
<tr>
<th>Category</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero</td>
<td>0%</td>
<td>5%</td>
</tr>
<tr>
<td>Less than $50,000</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>50,001 to $100,000</td>
<td>3%</td>
<td>7%</td>
</tr>
<tr>
<td>100,001 to $250,000</td>
<td>5%</td>
<td>7%</td>
</tr>
<tr>
<td>250,001 to $500,000</td>
<td>11%</td>
<td>15%</td>
</tr>
<tr>
<td>500,001 to $1,000,000</td>
<td>18%</td>
<td>15%</td>
</tr>
<tr>
<td>1,000,001 to $5,000,000</td>
<td>26%</td>
<td>20%</td>
</tr>
<tr>
<td>5,000,001 to $10,000,000</td>
<td>16%</td>
<td>14%</td>
</tr>
<tr>
<td>10,000,001 to $25,000,000</td>
<td>13%</td>
<td>12%</td>
</tr>
<tr>
<td>More than $25,000,000</td>
<td>8%</td>
<td>5%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

**Extrapolated value**  

- FY2017: $6,842,250  
- FY2016: $5,435,650

**Q38.** To understand the relationship of each of the seven (7) categories to the total cost of attacks against knowledge assets, please allocate points to each category for a total of 100 points.  

<table>
<thead>
<tr>
<th>Category</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remediation &amp; technical support activities</td>
<td>11</td>
<td>14</td>
</tr>
<tr>
<td>Users' downtime and lost productivity</td>
<td>10</td>
<td>12</td>
</tr>
<tr>
<td>Disruptions to normal business operations</td>
<td>17</td>
<td>21</td>
</tr>
<tr>
<td>Damage or theft of IT assets and infrastructure</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>Revenue loss and customer turnover (churn)</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Reputation loss and brand damage</td>
<td>40</td>
<td>44</td>
</tr>
<tr>
<td>Fines, penalties and lawsuits</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Total points</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>

*Five categories in FY2016

**Q39.** What is the likelihood of a data breach involving knowledge assets over the next 12 months?  

<table>
<thead>
<tr>
<th>Category</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 1%</td>
<td>0%</td>
<td>4%</td>
</tr>
<tr>
<td>1% to 5%</td>
<td>6%</td>
<td>0%</td>
</tr>
<tr>
<td>6% to 10%</td>
<td>6%</td>
<td>14%</td>
</tr>
<tr>
<td>11% to 15%</td>
<td>9%</td>
<td>17%</td>
</tr>
<tr>
<td>16% to 20%</td>
<td>18%</td>
<td>18%</td>
</tr>
<tr>
<td>21% to 25%</td>
<td>24%</td>
<td>25%</td>
</tr>
<tr>
<td>26% to 50%</td>
<td>30%</td>
<td>22%</td>
</tr>
<tr>
<td>More than 50%</td>
<td>7%</td>
<td>0%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

**Extrapolated value**  

- FY2017: 25.7%  
- FY2016: 20.6%
Q40. What is the mean time to identify (MTTI) a data breach involving a knowledge asset caused by a careless insider? FY2017

<table>
<thead>
<tr>
<th>Time Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 1 day</td>
<td>0%</td>
</tr>
<tr>
<td>1 to 10 days</td>
<td>5%</td>
</tr>
<tr>
<td>11 to 50 days</td>
<td>7%</td>
</tr>
<tr>
<td>51 to 100 days</td>
<td>14%</td>
</tr>
<tr>
<td>101 to 150 days</td>
<td>21%</td>
</tr>
<tr>
<td>151 to 200 days</td>
<td>18%</td>
</tr>
<tr>
<td>201 to 300 days</td>
<td>18%</td>
</tr>
<tr>
<td>301 to 600 days</td>
<td>12%</td>
</tr>
<tr>
<td>More than 600 days</td>
<td>5%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

Extrapolated value (days) 202.6

Q41. What is the mean time to contain (MTTC) a data breach involving a knowledge asset caused by a careless insider? FY2017

<table>
<thead>
<tr>
<th>Time Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 1 day</td>
<td>5%</td>
</tr>
<tr>
<td>1 to 10 days</td>
<td>13%</td>
</tr>
<tr>
<td>11 to 50 days</td>
<td>38%</td>
</tr>
<tr>
<td>51 to 100 days</td>
<td>23%</td>
</tr>
<tr>
<td>101 to 150 days</td>
<td>9%</td>
</tr>
<tr>
<td>151 to 200 days</td>
<td>6%</td>
</tr>
<tr>
<td>201 to 300 days</td>
<td>3%</td>
</tr>
<tr>
<td>301 to 600 days</td>
<td>1%</td>
</tr>
<tr>
<td>More than 600 days</td>
<td>2%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

Extrapolated value (days) 76.3

Q42. What is the mean time to identify (MTTI) a data breach involving a knowledge asset caused by a malicious outsider? FY2017

<table>
<thead>
<tr>
<th>Time Range</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 1 day</td>
<td>0%</td>
</tr>
<tr>
<td>1 to 10 days</td>
<td>1%</td>
</tr>
<tr>
<td>11 to 50 days</td>
<td>6%</td>
</tr>
<tr>
<td>51 to 100 days</td>
<td>5%</td>
</tr>
<tr>
<td>101 to 150 days</td>
<td>12%</td>
</tr>
<tr>
<td>151 to 200 days</td>
<td>15%</td>
</tr>
<tr>
<td>201 to 300 days</td>
<td>19%</td>
</tr>
<tr>
<td>301 to 600 days</td>
<td>23%</td>
</tr>
<tr>
<td>More than 600 days</td>
<td>19%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

Extrapolated value (days) 323.3
Q43. What is the mean time to contain (MTTC) a data breach involving a knowledge asset caused by a malicious outsider? FY2017

<table>
<thead>
<tr>
<th>Duration</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 1 day</td>
<td>1%</td>
</tr>
<tr>
<td>1 to 10 days</td>
<td>2%</td>
</tr>
<tr>
<td>11 to 50 days</td>
<td>12%</td>
</tr>
<tr>
<td>51 to 100 days</td>
<td>30%</td>
</tr>
<tr>
<td>101 to 150 days</td>
<td>18%</td>
</tr>
<tr>
<td>151 to 200 days</td>
<td>17%</td>
</tr>
<tr>
<td>201 to 300 days</td>
<td>10%</td>
</tr>
<tr>
<td>301 to 600 days</td>
<td>8%</td>
</tr>
<tr>
<td>More than 600 days</td>
<td>2%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
<tr>
<td><strong>Extrapolated value (days)</strong></td>
<td><strong>152.7</strong></td>
</tr>
</tbody>
</table>

Q44. Approximately, what percentage of the total cost is due to careless insiders? FY2017

<table>
<thead>
<tr>
<th>Percentage</th>
<th>FY2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero</td>
<td>0%</td>
</tr>
<tr>
<td>Less than 10%</td>
<td>11%</td>
</tr>
<tr>
<td>10% to 25%</td>
<td>23%</td>
</tr>
<tr>
<td>26% to 50%</td>
<td>19%</td>
</tr>
<tr>
<td>51% to 75%</td>
<td>32%</td>
</tr>
<tr>
<td>76% to 100%</td>
<td>15%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
<tr>
<td><strong>Extrapolated value (days)</strong></td>
<td><strong>45%</strong></td>
</tr>
</tbody>
</table>

Q45. Approximately, what percentage of the total cost is due to malicious outsiders? FY2017

<table>
<thead>
<tr>
<th>Percentage</th>
<th>FY2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zero</td>
<td>0%</td>
</tr>
<tr>
<td>Less than 10%</td>
<td>9%</td>
</tr>
<tr>
<td>10% to 25%</td>
<td>15%</td>
</tr>
<tr>
<td>26% to 50%</td>
<td>18%</td>
</tr>
<tr>
<td>51% to 75%</td>
<td>30%</td>
</tr>
<tr>
<td>76% to 100%</td>
<td>28%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
<tr>
<td><strong>Extrapolated value (days)</strong></td>
<td><strong>53%</strong></td>
</tr>
</tbody>
</table>

Q46. What is the maximum loss that your organization could experience as a result of a material data breach of knowledge assets? FY2017 FY2016

<table>
<thead>
<tr>
<th>Loss Range</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than $500,000</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td>$500,000 to $1,000,000</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td>$1,000,001 to $5,000,000</td>
<td>2%</td>
<td>3%</td>
</tr>
<tr>
<td>$5,000,001 to $10,000,000</td>
<td>1%</td>
<td>5%</td>
</tr>
<tr>
<td>$10,000,001 to $25,000,000</td>
<td>2%</td>
<td>7%</td>
</tr>
<tr>
<td>$25,000,001 to $50,000,000</td>
<td>4%</td>
<td>7%</td>
</tr>
<tr>
<td>$50,000,000 to $100,000,000</td>
<td>7%</td>
<td>10%</td>
</tr>
<tr>
<td>$100,000,001 to $250,000,000</td>
<td>25%</td>
<td>18%</td>
</tr>
<tr>
<td>$250,000,001 to $500,000,000</td>
<td>36%</td>
<td>30%</td>
</tr>
<tr>
<td>More than $500,000,000</td>
<td>23%</td>
<td>19%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
</tr>
<tr>
<td><strong>Extrapolated value</strong></td>
<td><strong>$323,985,000</strong></td>
<td><strong>$269,822,500</strong></td>
</tr>
</tbody>
</table>
### Part 6. Organizational Characteristics & Demographics

#### D1. What organizational level best describes your current position?

<table>
<thead>
<tr>
<th>Position</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior Executive</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>Vice President</td>
<td>2%</td>
<td>3%</td>
</tr>
<tr>
<td>Director</td>
<td>16%</td>
<td>17%</td>
</tr>
<tr>
<td>Manager</td>
<td>21%</td>
<td>20%</td>
</tr>
<tr>
<td>Supervisor</td>
<td>14%</td>
<td>15%</td>
</tr>
<tr>
<td>Technician</td>
<td>35%</td>
<td>33%</td>
</tr>
<tr>
<td>Staff</td>
<td>9%</td>
<td>8%</td>
</tr>
<tr>
<td>Contractor</td>
<td>0%</td>
<td>2%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

#### D2. Check the Primary Person you or your leader reports to within the organization.

<table>
<thead>
<tr>
<th>Position</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO/Executive Committee</td>
<td>1%</td>
<td>2%</td>
</tr>
<tr>
<td>Chief Financial Officer (CFO)</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>General Counsel</td>
<td>4%</td>
<td>5%</td>
</tr>
<tr>
<td>Chief Information Officer (CIO)</td>
<td>51%</td>
<td>53%</td>
</tr>
<tr>
<td>Chief Information Security Officer (CISO)</td>
<td>22%</td>
<td>18%</td>
</tr>
<tr>
<td>Compliance Officer</td>
<td>7%</td>
<td>10%</td>
</tr>
<tr>
<td>Human Resources VP</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Chief Security Officer (CSO)</td>
<td>3%</td>
<td>2%</td>
</tr>
<tr>
<td>Chief Risk Officer (CRO)</td>
<td>9%</td>
<td>8%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

#### D3. What industry best describes your organization’s primary industry classification?

<table>
<thead>
<tr>
<th>Industry</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agriculture &amp; food services</td>
<td>0%</td>
<td>1%</td>
</tr>
<tr>
<td>Communications</td>
<td>3%</td>
<td>3%</td>
</tr>
<tr>
<td>Consumer products</td>
<td>6%</td>
<td>5%</td>
</tr>
<tr>
<td>Defense &amp; aerospace</td>
<td>1%</td>
<td>0%</td>
</tr>
<tr>
<td>Education &amp; research</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>Energy &amp; utilities</td>
<td>5%</td>
<td>6%</td>
</tr>
<tr>
<td>Financial services</td>
<td>18%</td>
<td>19%</td>
</tr>
<tr>
<td>Health &amp; pharmaceutical</td>
<td>10%</td>
<td>11%</td>
</tr>
<tr>
<td>Hospitality &amp; leisure</td>
<td>3%</td>
<td>4%</td>
</tr>
<tr>
<td>Industrial &amp; manufacturing</td>
<td>11%</td>
<td>10%</td>
</tr>
<tr>
<td>Media &amp; entertainment</td>
<td>1%</td>
<td>2%</td>
</tr>
<tr>
<td>Public sector</td>
<td>12%</td>
<td>12%</td>
</tr>
<tr>
<td>Retail</td>
<td>10%</td>
<td>9%</td>
</tr>
<tr>
<td>Services</td>
<td>9%</td>
<td>9%</td>
</tr>
<tr>
<td>Technology &amp; software</td>
<td>7%</td>
<td>5%</td>
</tr>
<tr>
<td>Transportation</td>
<td>2%</td>
<td>2%</td>
</tr>
<tr>
<td>Other</td>
<td>0%</td>
<td>0%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
<td><strong>100%</strong></td>
</tr>
<tr>
<td>D4. Where are your employees located? Check all that apply.</td>
<td>FY2017</td>
<td>FY2016</td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td>--------</td>
<td>--------</td>
</tr>
<tr>
<td>United States</td>
<td>100%</td>
<td>100%</td>
</tr>
<tr>
<td>Canada</td>
<td>71%</td>
<td>70%</td>
</tr>
<tr>
<td>Europe</td>
<td>70%</td>
<td>68%</td>
</tr>
<tr>
<td>Middle East &amp; Africa</td>
<td>46%</td>
<td>44%</td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td>63%</td>
<td>61%</td>
</tr>
<tr>
<td>Latin America (including Mexico)</td>
<td>57%</td>
<td>58%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>D5. What is the worldwide headcount of your organization?</th>
<th>FY2017</th>
<th>FY2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 500</td>
<td>9%</td>
<td>10%</td>
</tr>
<tr>
<td>500 to 1,000</td>
<td>18%</td>
<td>21%</td>
</tr>
<tr>
<td>1,001 to 5,000</td>
<td>27%</td>
<td>29%</td>
</tr>
<tr>
<td>5,001 to 25,000</td>
<td>19%</td>
<td>20%</td>
</tr>
<tr>
<td>25,001 to 50,000</td>
<td>8%</td>
<td>0%</td>
</tr>
<tr>
<td>50,001 to 75,000</td>
<td>12%</td>
<td>12%</td>
</tr>
<tr>
<td>More than 75,000</td>
<td>7%</td>
<td>8%</td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>100%</td>
</tr>
</tbody>
</table>

Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

Ponemon Institute  
Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high-quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.
Adtech

Presented By:

Jodi Daniels
Red Clover Advisors
Atlanta, GA
Ad Tech Evolution

- 1993: 1st banner ad
- 1995: World’s 1st ad network (160 sites syndicated)
- 2000: Google AdWords launched
- Early 2000s: Early popup blocking began
- 2008: Use of ad networks begins
- 2012: Ad exchanges
- 2018: Complex landscape
- Future
Ad Targeting

Target exactly the audience you want

Location  
Country  
State  
City or Town  
Age  
Gender  
Interests  
Activities  
Music  
Books  
TV shows  
Education  
High school  
College  
Magazines  
Work  
Politics  
Relationships

Source: Forbes.com. Photo Credit: AP Craig Ruttle
Digital Advertising Continues to Increase

Digital Advertising Growth Rate Expectations
(% of respondents expecting an increase of at least 10%, by category*)

- Social: 71% in 2017, 78% in 2018
- Mobile marketing: 76% in 2017, 80% in 2018
- Custom content / native advertising: 67% in 2017, 71% in 2018
- Video: 62% in 2017, 69% in 2018
- Programmatic: 59% in 2017, 59% in 2018
- Search advertising: 33% in 2017, 67% in 2018
- Online display: 27% in 2017, 33% in 2018

*Figures exclude those who “don’t know”

Published on MarketingCharts.com in December 2017. Data Source: AdMeme Partners.
Marketing technology to make it happen
Consumers care about *how* data is used

<table>
<thead>
<tr>
<th>Feature</th>
<th>First choice</th>
<th>Second choice</th>
<th>Third choice</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ability to dynamically segment audiences</td>
<td>22%</td>
<td>26%</td>
<td>19%</td>
</tr>
<tr>
<td>Omnichannel media execution to deliver cohesive messages</td>
<td>19%</td>
<td>20%</td>
<td>20%</td>
</tr>
<tr>
<td>AI technology that dynamically powers creative</td>
<td>14%</td>
<td>17%</td>
<td>18%</td>
</tr>
<tr>
<td>Less intrusive ad formats such as native</td>
<td>16%</td>
<td>14%</td>
<td>16%</td>
</tr>
<tr>
<td>Giving consumers choice over how data is used</td>
<td>18%</td>
<td>14%</td>
<td>12%</td>
</tr>
<tr>
<td>A standard, shared identity space that reduces web latency</td>
<td>9%</td>
<td>9%</td>
<td>15%</td>
</tr>
</tbody>
</table>

Published on MarketingCharts.com in September 2018 | Data Source: MediaMath / Econsultancy

*Based on responses from 250 executives involved in digital advertising, most of whom are based in the UK and US*
Pixel Overload
Why care about pixel governance

- Data leakage
- Security risks
- Latency
- Inaccurate cookie notices
Pixel Governance Process

- Signed Contracts
- Vendor Due Diligence
- Clear expectations on data use, collection, sharing
- Plan for when pixels go up and down
- Central ownership
- Repeatable process
- Accurate cookie notices
- Ability to manage individual rights
- GDPR compliant
Privacy regulations

GDPR
ePrivacy Directive (update coming soon)

California Consumer Privacy Act 2018 (CCPA)
PERSONAL DATA
Examples of Online Identifiers

- Any moniker used for online presence-social media, e-mail, instant messenger
- ID number
- Geolocation
- IP addresses
- “Cookies”
- Etc.
Transparency

Say what you do, do what you say

"Before I write my name on the board, I'll need to know how you're planning to use that data."
Privacy Notice

‣ It’s a dynamic living document
‣ Should have plain language and digestible
‣ Needs to be understood beyond legal
‣ Captures data use, collection and sharing
‣ Reviewed at least annually and with each new project
‣ Available at all places where personal data is captured
EU COOKIE CONSENT:
ePrivacy Directive & GDPR

- Cookies: Short Term Memory
- Stored in Browsers
- The Cookie Law (privacy legislation)
- Requires consent from visitors
- Designed to protect online privacy
- Consumers choice
- Work out what cookies your site sets & what it is used
  - the attributes & values of each cookie found
  - their purpose & use categories
  - the 3rd parties setting cookies on your site, and what is done with them
- Tell your visitors how you use cookies
- Obtain their consent (provides control over own data)
- All websites owned in the EU or targeted towards EU citizens, are now expected to comply with the law.
Cookie Notice

- It’s a dynamic living document
- Should have plain language and digestible
- Needs to be understood beyond legal
- Captures active cookies on the site
- Separate sections for each type of cookie
- Provides users options to opt in/out
- Reviewed with each new cookie placed on the site
- Available at all places where personal data is captured
Digital Cookies Require Monitoring
In Summary

- Privacy regulation is heating up
- Ad tech is ever changing
- Pixel Governance is essential to:
  - maintain compliance
  - strong security measures
  - prevent data leakage
- Ad Tech extends beyond the marketing department
QUESTIONS?
Get in touch

Website
www.redcloveradvisors.com

Phone
+1 404-964-3762

Email
jodi@redcloveradvisors.com
Afternoon Keynote: Royalty And Payment Terms, Audits And Alternative Structures

Presented By:

Peter J. Kinsella
Perkins Coie LLP
Denver, CO
Disclaimer

This presentation is for educational purposes only and does not constitute legal advice. If you require legal advice, you should consult with your attorney.

The information provided in this presentation does not necessarily reflect the opinions of Perkins Coie LLP, its clients or even the author.
Payment Clause Basics

Payment Calculation based on some mechanism
• Limited by: creativity, antitrust laws, misuse doctrine, exhaustion and implied licenses

Valuation is typically impacted by the rights being licensed
• What does the licensor own?
  o patent, trademark, copyright applications and registrations
  o "related" applications and registrations
    ➢ continuations, continuations in part etc...
  o applications yet to be filed / common law rights (e.g. know-how)
• What precise rights are being licensed?
  o Make, use, sell, offer to sell, import, reproduce, otherwise exploit?
  o Future rights?
Traditional Categories of License Payments

- Lump Sum
- Fixed Fee Per Unit / Per amount of Time / Per Person
- Percentage Royalty on Profit (be careful!)
- Percentage Royalty on Revenue
- Royalties on Sublicenses
- Milestone Obligations & Payments
- Minimum Royalties
- Hybrid Royalties
- Multi-Country Royalties
- Reach Through Royalties
- A combination of any of the above

Lump Sum Payment

The easiest arrangement to administer
May be a single upfront payment or paid in installments (e.g., quarterly or annually)
- Installment payments may be index adjusted
One party may be economically advantaged depending on the success or failure of the license
Fixed Fee Per Unit

A fixed fee is paid each time a certain product is sold or an activity is performed.

The fixed fee may be adjusted over time:
- Escalation clause to share in profit increase in later years of the license.
- Use of various indices (e.g., CPI, PPI) to determine escalation.

Sometimes this obligation is used in combination with a royalty on revenue obligation to ensure certain minimum payments.

Percentage Royalty on “Profit”

More frequently used in entertainment field.

Allows the licensee to recover various costs before paying a royalty.

Royalty rate will typically be much higher than a revenue-based royalty.

Profits can be very difficult to calculate:
- Profit calculation is easily manipulated.
  - Costs eligible for deduction need to be precisely defined.
Percentage Royalty on Revenue

X% of sales price – perhaps the most common type of clause

Allows the parties to share the economic risks and rewards

Definition of “Revenue” is extremely important (see following slides)

---

Percentage Royalty on Revenue

Traditional Definition of "Revenue"

Revenue may be comprised of several elements:

The gross selling price (invoiced price) of any products sold by the Licensee less payments such as:

- Itemized expenses actually paid by Licensee to an unrelated third party (such as shipping and insurance)
- Taxes (sales, VAT, GST etc)
- Tariffs and duties paid to governments
- Returns or exchanges

Sometime tied to Generally Accepted Accounting Principals (GAAP)
### Percentage Royalty on Revenue - Danger of having narrow definitions

**Danger of collecting royalties only on "sales"**

FBT Productions, LLC v. Aftermath Records, 621 F.3d 958 (9th Cir. 2010)

- FBT entered into a deal with Aftermath Records (for Eminem song) pursuant to which FBT would receive:
  - between 12% and 20% of the price of "records sold in the United States through normal retail channels"; and
  - 50% of net revenues "on masters licensed for the manufacture and sale of records".
- Aftermath authorized iTunes to distribute the songs
- Court determined that because Aftermath retained title to the digital music files, the iTunes transaction was a license

### Percentage Royalty on Revenue

**Other Potential Sources of "Revenue"**

- Services revenue (e.g., Streaming, Leasing, Professional Services)
- Equity in Licensee - Licensor may take stock rather than royalty
  - May need to address dividend revenue and equity appreciation
- Value received for products or services otherwise provided (e.g., barters or giveaways)
  - Consider specifying revenue for such transactions
    - e.g., gross selling price at which devices of similar kind and quality, sold in similar quantities, are currently being offered for sale by Licensee
Percentage Royalty on Revenue "Related Entity" Transactions

Revenue from Related Entity Transactions

- In the event any Products are provided to a Related Entity, then the royalties to be paid with respect to such Products are based on the "Revenue" for such Related Entity.
- Related Entities may include:
  - Corporations under common ownership or control
  - Persons who own or control licensee
  - Any other persons or entities that have an arrangement with Licensee that allows them to obtain licensed products or services at a discount

Exemplary Language to Address Sales by Related Entities and Sublicensees

“Sale” means any sale, transfer, lease, license, distribution or other disposition (excluding sample quantities given away for no consideration) of Licensed Products by Licensor, or its Affiliate or Sublicensee to a Third Party. For clarity, dispositions between or among Licensor, its Affiliates and Sublicensees will not be deemed a Sale, except where such Person is an end user, but Sales will include subsequent final sales to Third Parties by Licensor, its Affiliates or Sublicensees.
Percentage Royalty on Revenue – Package Sales

Determining royalty for products/services sold in a package (where a royalty is not being paid on the entire package)

• Pre-establish licensor’s share
  o Based on costs?
  o Based on value of IP?
  o Cost may not = Value

• Establish a minimum royalty amount

Determining Scope of Patent obligation

• Price for limited component
• Consider using a royalty on total sales

Royalties on Sublicenses

Common mechanisms for addressing sublicenses

• A royalty is paid by the licensee based on the sale price at which the sublicensee sells the product or service

• The licensee pays a royalty rate based on the amount of revenue received from sublicensee (the royalty rate is often much higher, 25-90%, in such situations)

• A combination of the above,
  o Royalty on sales made by sublicensee
  o A split of revenue received by licensee for no-sales generated revenue (such as milestone payments)
Potential Foundry Issues

*Intel Corp. v. United States Int’l Trade Comm’n (Atmel)* 946 F.2d 821 (Fed. Cir. 1991)
- Intel granted Sanyo a “non-exclusive, world-wide royalty-free license without the right to sublicense except to Subsidiaries, under Intel Patents which read on any Sanyo [devices] for the lives of such patents, to make, use and sell such products.”
- Court construed the grant to be limited to Sanyo designed and manufactured products

*Cyrix Corp. v. Intel Corp.*, 77 F.3d 1381 (Fed. Cir. 1996)
- “IBM” used in the term “IBM Licensed Products” does not limit the rights to IBM designed and manufactured products

Milestone Obligations & Payments – 1

Licensor specifies obligations that must be achieved
- If licensee fails to achieve milestones, licensor may terminate license

Milestones may also be coupled with a payment obligation
- Particularly important in exclusive license arrangements
  - Attempts to prevent inadequate performance (e.g., no commercialization in a major market, or shelving of IP)
    - Licensor gets inadequate financial return and wants to be able to license someone else
Milestone Obligations & Payments – 2

Exemplary Pharmaceutical Milestones:
• Completion of animal studies
• Completion of collection of data for FDA filing
• Filing new drug application with FDA
• Commencement of Phase 1 Clinical Studies
• Commencement of Phase 2 Clinical Studies
• Commencement of Phase 3 Clinical Studies
• Filing of product license application (PLA) with FDA
• FDA approval of PLA
• First sale anywhere in the world

Minimum Royalty Payments

Agreement specifies a minimum amount of royalties to be paid
• The licensee must pay the higher of
  o Actual royalties, or
  o Minimum annual stipulated amount
• The amount may increase over time
• If the licensee elects not to pay, licensor may terminate
• May need to consider impact of fluctuating revenue stream
Particularly important with exclusive licenses
• Prevents inadequate performance (e.g., no commercialization in a major market, or shelving of IP)
• May allows termination mechanism if licensor gets inadequate financial return and wants ability to license someone else
Often used instead of specific performance obligations
Payment Adjustments

Caps/Rate Reductions
Upward Adjustment Mechanisms
Most Favored Licensee Clause
Royalty Stacking
Royalty Suspension
Third Party Infringement

Caps/Rate Reductions
Caps are typically negotiated on a per year and total payment basis
• Example:
  o 6% royalty up to maximum $1,000,000 per year
    ➢ Royalty Rate may be adjusted or eliminated at trigger point
  o 6% royalty up to maximum $10,000,000 during term of the license
    ➢ Royalty Rate may be adjusted or eliminated at trigger point
Upward Adjustment Mechanisms

Indexes such as (CPI, PPI)

Increased Sales

- As a product becomes more successful, and costs reduce, royalty increases
- Licensor forgoes royalties in early stages, in return for higher royalties later
- Infrequently seen

Adjustment Clauses can be Complex

The Royalty will be automatically adjusted effective the first day of each subsequent Contract Year based upon the percentage increase or decrease of the unadjusted “Producer Price Index for Finished Goods - Capital Equipment” published by the United States Bureau of Labor Statistics (the "Index") calculated using the final value of such Index for April of 2013 compared to the final value of the Index for each April prior to each such subsequent Contract Year according to the following formula:

new Royalty = the amount listed in Section 1 above * Adjustment

Where,

“Adjustment” = the final value of the Index for April prior to each subsequent Contract Year / the final value of the Index for April of 2013

For informational purposes, the final value for the Index for April 2013 was 163.0.
**Most Favored Licensee Clause -1**

Common clause in a non-exclusive licenses

- If licensor later grants a license in the same country at a lower royalty, that lower royalty will apply in lieu of the rate licensee is currently paying.

Sought by non-exclusive licensee to enable it to be better able to compete.

**Typical Provisions**

- Triggering Event
- Notice of New License
- Election Right

**Most Favored Licensee Clause -2**

Licensor will notify Licensee of any rights granted to a third party under the Patents within ten (10) business days following the execution of an applicable definitive license agreement. Such notice will include a schedule of all amounts to be paid under such other license (a "Royalty Schedule"). Within sixty (60) days of receipt of such Royalty Schedule, Licensee may elect, with effect only from and after the date of such election, to pay royalties under such Royalty Schedule discounted by ten percent (10%) by providing written notice thereof to Licensor. If such third party license agreement provides for lump-sum royalties alone or in addition to other royalties and Licensee elects to proceed under such Royalty Schedule, then Licensor will reduce the lump-sum royalty payable by Licensee under such Royalty Schedule by ten percent (10%) and Licensee will have the right to have amounts previously paid under this Agreement for Royalties credited against such reduced lump-sum and then (to the extent such previously paid Royalties exceed such reduced lump-sum, if any) any other Royalties that would be owed by Licensee under such Royalty Schedule had such Royalty Schedule applied since the Effective Date through the date of such election.
Royalty Stacking -1

Issues can typically arise in two situations

• Product to be sold needs a license to a complementary technology,
  o e.g., a delivery system
  o another active ingredient
  o a complementary product where both sold together e.g., a vaccine cocktail

• Freedom to operate – product infringes a third party patent

Potential Solution: reduce royalty by X% of royalty paid out

• up to a maximum of Y% (not the whole amount)

Royalty Stacking -2

Sample Stacking Clause:

If Company pays any Third Party a royalty, lump sum or other payment for the right to practice intellectual property in connection with the manufacture, use, sale, offer for sale, importation or other activities concerning any Products (any such payment, a “Third Party Payment”), Company may credit fifty percent (50%) of such Third Party Payment against any future amounts owed and payable by Company under Section ________ (except that in no event will such credit be applied in a manner that reduces the amounts of any payment due under section __________ by more than fifty percent (50%)).
Suspending Royalties

Licensee may attempt to suspend royalties while invalidity or re-examination proceedings are pending or while licensed IP is being infringed by a third party.

Licensees are concerned that they may be unnecessarily paying royalties if the patent is revoked.

A potential compromise position:
- Royalties are paid to a trustee
- Returned to licensee if revocation proceedings successful
- Paid to licensor if revocation proceedings unsuccessful

See next slide for addressing third party infringement.

Third Party Infringement

Becomes more important as royalty rate increases.

Numerous procedures to address this issue:
- Allow exclusive license to pay for infringement suit
  - Costs of suit may be deducted from the royalties
  - Need to address how recovery is divided
- Suspend or decrease royalty rate if material third party infringement exists
  - Rate may decrease over time
Payments – 1

When are payments due?
• Payment due dates must take into account sales reporting system

Is there an interest or other charge imposed on late payments?
• Example: A late charge will be calculated at an annual rate of the prime rate in effect at the Citibank, N.A. in New York City, New York, U.S.A. (or its successor) compounded at the beginning of each calendar quarter, or the maximum rate allowed by law, whichever is less, for the period such payment remains delinquent.

Payments – 2

Methods of securing payment
• Pre-payment (often not practical)
  • Impound Accounts
  • Factoring
  • Security interests
Two situations where the issue arises
- Calculating relevant sales
- Making royalty payments

Solution:
- Identify the currency of payment
- Identify procedures for determining exchange rates
  - Source of exchange rate calculation
  - Time of calculation
    - Average rate over a period of dates
    - Specific rate on a particular day
      - Day before payment is made
      - Exchange rate at end of payment period
Tax/Government Approvals

Licenses may have significant tax implications
- Governments often impose a withholding tax on royalties
  - The agreement should be clear as to who bears this burden
License may need to be registered and/or approved by the local government
- e.g., India will not approve license if royalty exceeds 10%
Local government may not allow cash to leave the country

Royalty Reporting

When are reports due?
- E.g., Licensee will make full and correct written reports to Licensor within thirty (30) days after the first days of January, April, July and October
- What needs to be reported?
  - Number of licensed products sold?
  - Level of specificity? (e.g., model number)
  - If no amount is accrued during any period, a written statement to that effect should still be furnished
Records & Audits – 1

Records and Audit Clauses should address the following issues:

Require licensee to keep relevant records for the audit period (longer if dispute arises)

Period of review – licensee will usually want to limit audit rights to 2-3 years – Consider going back further if a systematic error is found in audit

Frequency of Audits?

Who can Audit? Licensor? Outside Auditor?

Records & Audits – 2

Records and Audit Clauses should address the following issues (con’t):

• Allow Licensor to Access all: relevant records (physical and electronic), relevant locations and relevant employees
  o Access to all sub-licensee / sub-contractor and any other related party records and sites by the Licensor (not the licensee)
  o Right to take copies of documents?

• Obligation that licensee fully cooperate with the audit
  o Typically the licensee doesn’t have a fiduciary duty

• Recovery of audit costs if findings exceed specified $ or %

• Interest on all underpayments

• Dispute resolution procedures?
Other Limits on Licenses

Exhaustion

Antitrust/Misuse

Exhaustion - 1

- The sale of a licensed product may restrict the manufacturer's ability to restrict further uses
  - See, Precious Moments, Inc. v. La Infantil, Inc. 971 F. Supp. 66 (1997)
Exhaustion -2


- Authorized foreign sales trigger patent exhaustion in the U.S.
- “A patentee’s decision to sell a product exhausts all of its patent rights in that item, regardless of any restrictions the patentee purports to impose”
- “If the patentee negotiates a contract restricting the purchaser’s right to use or resell the item, it may be able to enforce that restriction as a matter of contract law, but may not do so through a patent infringement lawsuit”

- First Sale doctrine applies to international copyright sales

- Patent Exhaustion does not permit a farmer to plant and grow saved, patented seeds without the patent owner’s permission

Misuse

Patent Misuse
- Patent misuse claims typically arise from the general “use of patent rights to obtain or to coerce an unfair commercial advantage.” *C.R. Bard, Inc. v. M3 Sys., Inc.*, 157 F.3d 1340, 1372 (Fed. Cir. 1998); *see also Princo Corp. v. Int’l Trade Comm’n*, 616 F.3d 1318, 1328 (Fed. Cir. 2010) (“[T]he key inquiry under the patent misuse doctrine is whether ... the patentee has impermissibly broadened the physical or temporal scope of the patent grant and has done so in a manner that has anticompetitive effects.”).

Copyright Misuse
- Restriction on Licensee to “not write, develop, produce or sell computer assisted die making software, directly or indirectly without Lasercomb’s prior written consent” for the 99 year term of the agreement plus one year constituted copyright misuse. *Lasercomb America, Inc. v. Reynolds*, 911 F.2d 970 (4th Cir. 1990)
Early History of Patent Misuse

- Contractual requirement to only use particular films in film projector is beyond the legitimate scope of the patent and the patent could not be enforced against a purchaser who used the patented projector with unsanctioned films *Motion Picture Patents Co. v. Universal Film Manufacturing Co.*, 243 U.S. 502 (1917).

- It was improper for the owner of a patent on "refrigerating transportation packages" for transporting and storing dry ice to require that patent licensees purchase their dry ice from the patent owner or its affiliates *Carbice Corp. of America v. American Patents Development Corp.*, 283 U.S. 27 (1931).

- Lease of patented salt canning machine that required the canners to only use salt tablets purchased from the patentee rendered patent unenforceable. *Morton Salt Co. v. G.S. Suppiger Co.*, 314 U.S. 488 (1942).

License actions that may give rise to misuse

- Price Fixing

- Tying – (but need to have market power)

- Grant back license/assignment - typically evaluated under the rule of reason - Different rules apply abroad

- Agreement not to develop competitive goods - could constitute per se misuse, although some courts have required a showing of market power

- Paying potential infringer not to make devices
What isn't Misuse – 35 U.S.C. 271(d)

1. Deriving revenue from acts which if performed by another would constitute contributory infringement
2. Licensing others to perform acts that would constitute contributory infringement
3. Seeking to enforce rights against infringers or contributory infringers
4. Refusing to grant a license
5. Conditioning the grant of a license on the acquisition of other patent rights or a product, unless patent owner has market power

Royalty Term Length -1

Different rights have different permissible royalty term lengths

- Patents royalties must cease upon:
- Trade secret royalty obligations may continue after public disclosure of the trade secret
    - No patent was filed
    - Patent was filed but never issued
Royalty Term Length -2


“Yet parties can often find ways around *Brulotte*, enabling them to achieve those same ends. To start, *Brulotte* allows a licensee to defer payments for pre-expiration use of a patent into the post-expiration period; **all the decision bars are royalties for using an invention after it has moved into the public domain.** See 379 U. S., at 31; *Zenith Radio Corp. v. Hazeltine Research, Inc.*, 395 U. S. 100, 136 (1969). A licensee could agree, for example, to pay the licensor a sum equal to 10% of sales during the 20-year patent term, but to amortize that amount over 40 years.”

Royalty Term Length -3


- 1881 - Licensee agreed to pay “the sum of twenty dollars for each and every gross of said Listerine hereafter sold by myself, my heirs, executors or assigns.”
- 1885 - Contract amended: Licensee “agrees and contracts for itself & assigns to pay … J J Lawrence, his heirs executors & assigns, six dollars on each & every gross of Listerine … manufactured or sold by the said Lambert Pharmacal Co. or its assigns”
- Court held that “the obligation to continue payments as long as Lambert or his successors continue to manufacture or sell Listerine is plain from the language of the agreements and is implicit in their terms.”
- Therefore, the agreement isn’t of an indefinite duration
Royalty Term Length -4

Several cases involving hybrid licenses have terminated trade secret payment obligations upon expiration or invalidity of related patents if royalties are intertwined

- *St. Regis Paper Co. v. Royal Indus.*, 552 F.2d 309 (9th Cir. 1977)
- *Chromalloy American Corp. v. Fischmann*, 716 F.2d. 683, (9th Cir. 1983)
- *Span-Deck, Inc. v. Fab-Con, Inc.*, 677 F.2d. 1237 (8th Cir. 1982)
- *Pitney Bowes, Inc. v. Mestre* 701 F.2d 1365, (11th Cir. 1983)
- *Boggild v. Kenner* 776 F.2d 1315, (6th Cir. 1985)
- *Meehan v. PPG Industries, Inc.*, 802 F.2d 881. (7th Cir. 1986)

Royalty Term Length -5


“Too, post-expiration royalties are allowable so long as tied to a non-patent right—even when closely related to a patent.

…That means, for example, that a license involving both a patent and a trade secret can set a 5% royalty during the patent period (as compensation for the two combined) and a 4% royalty afterward (as payment for the trade secret alone). Finally and most broadly, Brulotte poses no bar to business arrangements other than royalties—all kinds of joint ventures, for example—that enable parties to share the risks and rewards of commercializing an invention.” [emphasis added]
Royalty Term Length -6

Hybrid License Terms – Patent Expiration

*Boggild v. Kenner, 776 F.2d 1315 (6th Cir. 1985)*

- Court determined that once a pending patent issues, enforcement of royalty provisions for other rights which conflict with and are indistinguishable from the royalties for the patent rights is precluded.
  - Court noted that the Supreme Court has only upheld enforcement of potentially conflicting state trade secret provisions in hybrid licenses only where no patents ever issued.
  - Upon issuance of the patent, however, the federal supremacy doctrine requires directly conflicting provisions to be resolved under federal patent law.
- Thus, *Boggild* stands for the proposition that a trade secret royalty cannot be charged for the exercise of rights that were protected by the patent once that patent expires.

Royalty Term Length -7

Hybrid License Recommendations

- Distinguish between patent and trade secret **subject matter**
  - *Boggild v. Kenner* 776 F.2d 1315, (6th Cir. 1985)

- Allocate between patent and trade secret royalty rates (e.g., 4% for use of patent, 3% for use of trade secrets)

- Provide provisions that address royalty rates if patents do not issue or expire or are invalidated

  - Clearly state that the trade secret “payment provisions” survive patent expiration
Limits on "Total Sales" Patent Royalties

Compare:
• Total sales royalties are illegal and constitute misuse if the patent owner coerced or conditioned the license on a total sales royalty. *Zenith Radio, with Automatic Radio Mfg. Co. v. Hazeltine Research, Inc.*, 338 U.S. 827 (1950).

• Royalties may be based on unpatented components if that provides a convenient means for measuring the value of the license. *Zenith Radio Corp. v. Hazeltine Research, Inc.*, 395 U.S. 100 (1969).
  o If convenience of the parties rather than patent power dictates the total sales royalty provision, there is likely no patent misuse.

Multiple Patent Licensing

*U.S. Phillips v. USITC*, No. 04-1361 (Fed. Cir. 2005)
• The offer of a package of essential and non-essential nonexclusive licenses for a single royalty was proper.
• The value of any patent package is largely, if not entirely, based upon the patents that are essential to the technology in question.
• Prohibiting a package license puts the owner of essential and nonessential patents at a licensing disadvantage compared to the owner of only an essential patent.

Reach-Through Royalties

Royalties are based on a product derived from the use of Licensor’s IP but are not covered by the Licensor’s IP

- Typically extend to generally foreseeable products discovered through use of the invention
- "Reach-through" products are typically identified by reference to the material or assay used to find or identify them


- Consider Applicability of *Zenith Radio Corp* and Exhaustion cases?

Limits on Multi-Country Royalties

*Scheiber v. Dolby Labs., Inc.*, 293 F.3d 1014 (7th Cir. 2002)

- Dolby licensed patented technology from Scheiber, who owned both U.S. patents (expired ’93) and Canadian patents (expired ’95)
- During settlement negotiations, in exchange for a lower royalty rate, Dolby offered to pay royalties until the expiration of Scheiber’s Canadian patent
- Because the contract required the payment of royalties after the expiration of Scheiber’s U.S. patent, the agreement violated *Brulotte*
Solutions for Multi-Country Royalties

Licensees often resist paying royalties in countries without patents or patent applications, they only desire to pay for:
- “Valid Patent Claim”
- Sales in a country where but for the license, “infringement” would occur in that country

Licensee may pay a partial royalty
- May need to distinguish patent rights from trade secret rights
- May need to distinguish royalty rates based on country of manufacture vs. country of sale
- May need to reduce royalty obligation if a competing product enters the marketplace, if it would have infringed the patent

Alternate Structures – 1

Sell the IP
- Lump Sum Payment
- Payments over time
- Stock
  - Most risky and most difficult to value
  - Requires “exit strategy”
  - May be needed in “start-up scenario”
  - Must determine your degree of control
- May include running “earn-out” from entity revenue
  - Note: may not be protected in bankruptcy
Alternate Structures – 2

Consider tying license to other non-protected products or services

  - Eliminated presumption of market power arising from a patent
  - Party must prove licensor has sufficient market power in the desired product to make a consumer take the unpatented product

Thanks!

Contact Information
Peter Kinsella
pkinsella@perkinscoie.com
303-291-2328
Ethics

Presented By:

David C. Hricik
Mercer University School of Law
Macon, GA
Legal Ethics in the Modern World

David Hricik*
Professor, Mercer University School of Law
Of Counsel, Taylor English Duma, LLP

* A portion of this is based upon the forthcoming article, David Hricik, Asya-Lorraine S. Morgan & Kyle H. Williams, The Ethics of Using Artificial Intelligence to Augment Drafting Legal Documents, __ Tex. A&M L.J. __ (2018).
# TABLE OF CONTENTS

1. Exponential Math: Humanity’s Greatest Failing ..................................................... 3

2. Drafting Services: Disruptors? ................................................................................. 4
   a. Ensuring that the Lawyer or the Lawyer’s Client Owns Intellectual Property Rights................................................................. 6
      1. Copyright Ownership.............................................................................................................. 6
      2. Ownership of Patentable Inventions ............................................................................. 7
   b. The Attorney must be Competent to Review the Work and must Remain Responsible to the Client for the Service’s Work................................. 8
   c. The Fee Must be Reasonable ......................................................................................... 8
   d. The Lawyer May Need to Inform the Client that the Lawyer is Using the Service 9
   e. The Lawyer Must Take Reasonable Care to Protect Client Confidences While the Service is Using the Client’s Information and While that Information is Going to and From the Service ................................................................. 9
   f. The Lawyer Must Take Reasonable Care to Avoid Conflicts of Interest............ 11
   g. Avoiding Assisting in the Unauthorized Practice of Law ........................................ 11

3. Common Risks ..................................................................................................... 12
   a. E-mail Confidentiality as a General Matter ................................................................. 12
   b. Communicating by Email with Clients at their Workplaces................................. 16
   c. Confidential Information on Digital Devices.............................................................. 16
   d. Cloud Storage: HIPAA and Other Statutes?............................................................ 17
   e. Phishing and More ..................................................................................................... 19

4. Conclusion ............................................................................................................ 20
1. **Exponential Math: Humanity’s Greatest Failing**

Moore’s Law is a law every lawyer should know. The speed of innovation has increased dramatically in large part because computing power has increased exponentially in accordance with Moore’s Law. Moore’s Law is the recognition made in 1965 that the number of transistors that could fit on a chip—an integrated circuit—would double every two years.\(^1\) It explains why the cost of computing power, the cost of bandwidth, and the cost of data storage have plummeted, meaning that the speed of innovation has increased. This chart\(^2\) from late 2016 captures the impact of Moore’s Law:

![Chart showing exponential decrease in cost of computing](https://dupress.deloitte.com/content/dam/dup-us-en/articles/3465_Digital-supply-network/figures/digital-supply-network-Fig1.png)

To better contextualize the meaning of this exponential decrease in cost of computing, consider this analogy:

Another way to think about Moore’s law is to apply it to a car. Intel CEO Brian Krzanich explained that if a 1971 Volkswagen Beetle had advanced at the pace of Moore’s law over the past 34 years, today “you would be able to go with that car 300,000 miles per hour. You would get two million miles per gallon of gas, and all that for the mere cost of four cents.”\(^3\)

---

2. https://dupress.deloitte.com/content/dam/dup-us-en/articles/3465_Digital-supply-network/figures/digital-supply-network-Fig1.png
Computer power enabled by Moore’s Law is reducing time-to-market for a growing number of new products by eliminating the need for humans to do a growing amount of the work, thus allowing products to be brought to market more quickly and more cheaply. Further, computer power, bandwidth, and storage allow more products to contain embedded sensors that automatically and immediately provide testing data, thus more quickly allowing it to identify needed changes. Not only will such sensors allow for testing to be shortened and more efficient, these technologies allow businesses to identify services or products the consumer does not even know it needs—Uber, the ride sharing service, illustrates this phenomenon, replacing cabs. Indeed, products that embody the innovation described by Moore’s Law are themselves examples of what Moore’s Law is permitting: no one knew they needed an iPhone until they saw one. The reduction of the time and cost needed for research and development, a significant part of time-to-market, will be profound.

An illustration of Moore’s law comes from data storage, and looking backward. This technology has rapidly morphed in just the twenty years to take various forms of storage and different variations within each type, including devices using magnetism (zip drives), light (CDs, then DVDs), and other means (thumb drives and other forms of solid state devices). Holographic storage—whatever that means—is apparently coming next.

Why did this section begin by stating that exponential math is humanity’s greatest failing? Professor Bartlett, a “famous” mathematician, observed “The greatest shortcoming of the human race is our inability to understand the exponential function.” Change has happened very rapidly: it is happening exponentially, and we cannot perceive that well. For an excellent video by Professor Bartlett on this point, see this: https://www.youtube.com/watch?v=F-OA2rkpBSY

2. Drafting Services: Disruptors?

Disruptive technology displaces existing things or creates entire new needs. Lexis/Nexis and Westlaw have not quite made law books obsolete, but they have come close. At a recent conference, I showed students pictures of Shepard’s books: none knew what the red, yellow, and white books were for.

Driverless cars seemingly will soon be ubiquitous, leading to a decline in car wrecks, medical malpractice, franchises (why stop at a hotel: just let the car drive you, and it will come full of gas), and many more economic activities – activities that lead to

---

4 See generally, Persistent Forecasting of Disruptive Technologies (2010) chapter 3, p. 3 (noting that globalization has led to a shrinking R&D cycle, faster product development in response to consumer demand, a shorter product development cycle, and a shorter product cycle).
6 See generally, id.
7 http://www.zetta.net/about/blog/history-data-storage-technology
8 Id.
legal work. Lawyers need to be aware of the potential for entire practice areas to dry up, and perhaps for new ones to arise to replace them.

Many services are already available that write legal documents. Some are “routine” such as releases, while others are complicated, like patent applications. Rocketlawyer.com and specifio.com are two such services (the latter drafts patent applications, with drawings).

It will – quickly -- become more common for clients to be able to draft even relatively complex legal documents. Lawyers need to be sure to consider what their “value add” will be in this environment. On a larger scale, the ability for computers to do what lawyers have exclusively been allowed to do will create issues for the profession broadly.

Because technology may be able to do some tasks better, or at a lower cost, or both, lawyers should use technology when it will, considering the risks, benefit clients. That obligation requires lawyers to stay “keep abreast of changes in… practice, including the benefits and risk associated with relevant technology...” Assessing the benefits and risks of a particular technology obviously requires due diligence into the practical and legal risks of the technology, and comparing that to the benefits it brings to a representation. That assessment requires applying existing ethical rules in a process that can best be analyzed as comprising two stages.

The first step requires determining whether the technology does what it is supposed to do in a reasonably competent manner. For example, just as a lawyer could not use a paralegal to use a form to create the first draft of a contract for a client if the paralegal’s work was known to be unreliable or unreasonably expensive, a lawyer cannot use an automated contract drafting service with the same shortcomings. The first step, in other words, requires reasonable efforts by the lawyer to determine the competency of the service. If the service does not provide competent assistance, the lawyer obviously cannot use it.

The second step requires determining whether a competent service can be used while complying with the ethical obligations of the lawyer, beyond competency. Just as a lawyer must ensure that non-lawyer employees maintain the confidentiality of client information consistent with the lawyer’s ethical obligations, he must do so with all services provided by third parties, including automated services. Likewise, lawyers must ensure non-lawyer assistants – even those who are independent contractors hired for

---

12 Id.
a particular matter, and not firm employees – must not have conflicts of interest or violate other ethical rules.\(^\text{13}\)

The analogy to having a machine owned by a third-party to write, or assist in writing, a brief or other legal document is analogous to outsourcing it – but to a computer, not a person. The ABA has addressed the ethical issues created by outsourcing legal work to real human beings. Its opinion provides a good roadmap to identify the issues created here.\(^\text{14}\)

An opinion from the American Bar Association (“ABA”) addressed the issues that arise when lawyers outsource legal work to third-parties to draft legal documents, and it specifically addressed outsourcing the preparation of patent applications. The ABA stated that among other things, (1) the attorney must be competent to review the work,\(^\text{15}\) and must remain responsible for work,\(^\text{16}\) (2) the fee must be reasonable,\(^\text{17}\) (3) the lawyer may need to inform the client that the lawyer is using the services\(^\text{18}\), (4) client confidences must be protected\(^\text{19}\), (5) the lawyer must take reasonable care to avoid against conflicts of interest,\(^\text{20}\) and the lawyer must avoid assisting in the unauthorized practice of law.\(^\text{21}\)

The same ethical issues arise when the work is outsourced, not to a human being, but to a computer. The ABA recognized that legal services may be outsourced to “independent service providers that are not within their direct control.”\(^\text{22}\) While the ABA made that statement when addressing whether a lawyer’s reliance on human beings to draft documents is ethical, this article examines reliance on artificial intelligence. The same ethical issues can arise, but we add to that list and begin with a critical question arising from intellectual property law: who owns something written by a computer?

a. Ensuring that the Lawyer or the Lawyer’s Client Owns Intellectual Property Rights.

1. Copyright Ownership

Under general copyright law, ownership vests initially in the creator of the work, and throughout the founding of our country until recently humans were if not the sole creators were heavily involved in creation of copyrightable works. The fact that a


\(^{16}\) See ABA Formal Op. 08-541; MRPC R. 5.1, 5.3 (2018).

\(^{17}\) See ABA Formal Op. 08-541; MRPC R. 1.5 (2018).

\(^{18}\) See ABA Formal Op. 08-541; MRPC R. 1.6 (2018).

\(^{19}\) See ABA Formal Op. 08-541; MRPC R. 1.6 (2018).

\(^{20}\) See ABA Formal Op. 08-541; MRPC R. 5.7 (2018).

\(^{21}\) See ABA Formal Op. 08-541; MRPC 5.5 (2018).

\(^{22}\) See ABA Formal Op. 08-541.
computer assists in creation of a work does not mean it was not created by a human being: presumably, copyright in a book written by a person using a computer does not belong to Microsoft simply because the author wrote the book using a computer. This issue is, however, currently being litigated in Rearden LLC v. Disney. In that case, the plaintiff contends that its software allowed various movie studios to create visual images which the defendants used in their films, without permission, thus violating the plaintiff’s copyright in the works. The defendants moved to dismiss, asserting that no copyright subsisted in the owner of the software because otherwise “Adobe or Microsoft would be deemed to be the author-owner of whatever expressive works the users of Photoshop or Word generate by using those programs.”

Plainly, the author of a document does not lose copyright protection simply because a computer is involved and makes changes – such as autocorrecting words or suggesting a structure that avoids passive voice. Drafting services create the potential for works to be created without a human providing much, if any, input. Courts generally reason that, unless a statute creates rights in a non-human, such as an animal, such rights do not exist. A recent controversy addressed whether a “selfie” taken by a monkey was subject to copyright protection, and the Ninth Circuit held that unless a statute specifically grants non-humans – in this case, animals – rights, they lacked those rights. Consistent with this, the U.S. Copyright Office previously stated that to qualify for protection, “a work must be created by a human being.”

However, as the degree of authorship moves from person to computer, and eventually transitions to computer-based creativity entirely, lawyers need to be concerned that courts may continue to insist that humans be primary author as a prerequisite to copyright protection, even though that will erode the incentive to create original works. Lawyers using services to draft documents must recognize that it may be unclear who owns any copyright in a work, and to take steps to ensure that – if anyone – the lawyer owns it.

2. Ownership of Patentable Inventions.

Services that draft patent applications create an additional wrinkle. Generally speaking, the person who invents a patentable invention owns it, though the inventor may assign the invention to someone else. A recent article observed that “it is more and

---

24 Id.
25 The Ninth Circuit recently held against the monkey, holding that only humans could enforce rights granted by the copyright act. Naruto v. Slater, __ F.3d __ (9th Cir. Apr. 23, 2018), relying on the fact that the Copyright Act did not authorize animals to file suit, and so lacked statutory standing to sue for infringement.
more likely that the AI will be the entity taking the inventive step,” and so being the “inventor” of a particular invention.\textsuperscript{29} Use of a service to write patent applications creates the potential for the system to “invent” something that is, by itself, a separate patentable invention.\textsuperscript{30} If that happens, who owns that invention?

Currently, U.S. patent laws recognize only individual human beings as inventors—not even “artificial persons” that have become somewhat recognized, such as companies,\textsuperscript{31} let alone machines.\textsuperscript{32} Thus, if the service is an “inventor” the problem becomes the fact that at least as of now only human beings can be an “inventor” under the patent laws. If the courts construe the patent act to allow for inventions by machines, then the machine owns the invention. If not the machine, then perhaps the owner of the system is the “inventor,” or, instead, the “list of possible human inventors includes the AI software and hardware developers” and others.\textsuperscript{33}

Accordingly, faced with this uncertainty, lawyers using services must address ownership of any inventions made by the system. Counsel should review the terms of service to ensure that the client owns any patentable inventions. Due diligence may require ensuring all patentable inventions conceived of by the system are assigned to the lawyer’s client, or at minimum to the lawyer.

b. The Attorney must be Competent to Review the Work and must Remain Responsible to the Client for the Service’s Work.

As noted at the outset, a separate step of due diligence is ensuring that the service provides competent work because this is a fact- and practice-specific area. Given that the lawyer must be liable to the client for the work, lawyers should ensure that they are competent to review the work of the system. In addition, the lawyer should review the terms of service to determine whether, and to what extent, the lawyer may have a claim against the service.

c. The Fee Must be Reasonable

Perhaps the most unusual consequence of applying ethical principles governing human outsourcing to machines concerns money. In addressing outsourcing to humans, the ABA stated that a law firm could charge a client more than the actual cost it paid for a contract lawyer, or non-lawyer. The ABA reasoned that doing so was “not substantively different from the manner in which a conventional law firm bills for the services of its lawyers” because the client does not know the lawyer’s salary, benefits, and so on. Yet,

\textsuperscript{29} Susan Y. Tull, \textit{Patenting the Future of Medicine: The Intersection of Patent Law and Artificial Intelligence in Medicine}, 10 Landslide No. 3 40, 42 (Jan/Feb 2018).


\textsuperscript{31} Tull at 42.


\textsuperscript{33} Tull at 42.
the ABA warned that if a firm “decides to pass those costs through to the client as a disbursement, however, no markup is permitted” unless the client agreed otherwise.

Because a lawyer must review the work of an augmented service to ensure its competency—and because the total fee must be reasonable—the first step in the analysis is to ensure that the charge for the service, when combined with the lawyer’s fee to review, is reasonable as a whole. To the extent that the lawyer can remain within that overall cap and charge more than the actual cost of the service, the lawyer must have the client agree to those charges.

d. The Lawyer May Need to Inform the Client that the Lawyer is Using the Service

Under some circumstances a lawyer may be required to disclose to a client that it is using third parties to provide legal services. Particularly where a lawyer intends to use an augmented drafting service that is new and unproven, a lawyer should consider carefully whether disclosure is, even if not required, good practice.

e. The Lawyer Must Take Reasonable Care to Protect Client Confidences While the Service is Using the Client’s Information and While that Information is Going to and From the Service

When client confidential information is with the service provider and being processed, it is subject to two risks: hacking by third parties (including unauthorized use by employees of the service) or use by the service that is inconsistent with the lawyer’s obligation of confidentiality. In discussing human outsourcing, the ABA reminded lawyers to “act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer’s supervision.” This is because lawyers have a duty under Model Rule 5.3 to make reasonable efforts to ensure that the conduct of non-lawyers under the attorney’s supervision is compatible with the professional obligations of the attorney.

When lawyers outsource work and use human beings to perform non-legal services to assist in the practice of law, the ABA advises lawyers to “consider conducting reference checks and investigating the background of . . . any nonlawyer intermediary involved, such as a placement agency or service provider.” Lawyers may take into account: the education, experience, and reputation of the non-lawyer; the nature of the services provided; the terms of any arrangements concerning the protection of client information; and the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality.

---

34 Formal Op. 08-451, supra note 23.
36 Id.
37 Id.
38 MODEL RULES OF PROF’L CONDUCT r. 5.3 cmt. 3 (1983).
Obviously, those obligations are subject to the general rule of reasonableness. The ABA stated that this requires lawyers “to recognize and minimize the risk that any outside service provider may inadvertently – or perhaps even advertently – reveal client confidential information to adverse parties or to others who are not entitled to access.” 39

In this regard, while “[w]ritten confidentiality agreements are strongly advisable in outsourcing relationships,” 40 blindly relying on a paper policy without some understanding of the reputation and track record of the business is also clearly insufficient. But the terms of service should be reviewed.

For example, patent-application drafting service Specifio explains how it uses information:

We may keep and use obscured content-stripped versions of your Confidential Information; however, the content words will be removed from the documents and replaced with nonspecific symbols so that the meaning of the text cannot be ascertained. For example:

The statement

The present disclosure relates to systems and methods for facilitating review of a confidential document by a non-privileged person by stripping away content and meaning from the document without human intervention such that only structural and/or grammatical information of the document are conveyed to the non-privileged person

would look something like this:

the p0018 d0017 r0019s to systems and methods for f0000ing r0001 of a c0002 d0003 by a n0004 p0005 by s0006ing a0007 c0008 and m0009 from the d0003 without h0010 i0011 such that only s0012 and/or g0013 i0014 of the d0003 are c0015ed to the n0004 p0005.

We use these obscured content-stripped versions for limited internal purposes only, such as to analyze document structures and word forms, which helps use do things like provide you with better support services and improve the Services.

In addition, Specifio does not train its machine-learning models on the content of any Confidential Information. This helps ensure there is never “cross pollination” between patent applications.

39 Id.
40 Id.
We will not disclose to anyone that you are a Specifio customer or that you are using the Services, without your prior written consent in each instance.\textsuperscript{41}

\textbf{f. The Lawyer Must Take Reasonable Care to Avoid Conflicts of Interest}

In discussing outsourcing to humans, the ABA recognized that where the vendor represented a client’s adversary, there was the potential for misuse of information. Accordingly, it warned that “to minimize the risk of potentially wrongful disclosure, the outsourcing lawyer should verify that the outside service provider does not also do work for adversaries of their clients on the same or substantially related matters; in such an instance, the outsourcing lawyer could choose another provider.”\textsuperscript{42} When vetting outside human vendors, lawyers should also consider the vendor’s conflict check system in order to make a reasonable effort to avoid conflicts of interest.\textsuperscript{43}

Applying these principles to augmented services runs into the fact that a machine does not have loyalties. Consequently, the reasons why conflict of interest rules exist do not necessarily apply to machines; a machine can be asked by the lawyer for the plaintiff to write a motion to dismiss and then by the lawyer for the defendant to write a response, and the machine will do as good a job as it can for both. Divided loyalties and data are mutually exclusive.

However, if two parties are using the same system, and if the machine uses confidential information from one party in forming the work product for the other, misuse of confidences—which is one aspect of the duty of loyalty—can be implicated. As noted above, the service’s assurances that confidences will not be disclosed—and client identities not revealed—may address most of the policy concerns underlying conflicts of interest rules.

\textbf{g. Avoiding Assisting in the Unauthorized Practice of Law}

Using augmented drafting services also creates the potential for the unauthorized practice of law.\textsuperscript{44} However, usually “an individual who is not admitted to practice law in a particular jurisdiction may work for a lawyer who is so admitted, provided that the lawyer remains responsible for the work being performed and that the individual is not held out as being a duly admitted lawyer.”\textsuperscript{45} Thus, just as a lawyer can have a non-lawyer paralegal draft a will or other legal document without assisting with the unauthorized

\textsuperscript{42} \textit{Id.}
\textsuperscript{43} See \textit{id.}; \textit{MODEL RULES OF PROF’L CONDUCT r. 5.7 (AM. BAR ASS’N 1983)}.
\textsuperscript{45} Formal Op. 08-451.
practice of law, so too can a lawyer use a non-lawyer augmented system to do so. That, however, again raises the need for the lawyer to be competent with the work product of the service.

3. Common Risks.

a. E-mail Confidentiality as a General Matter.

A long time ago, I wrote an article which explained that as things then were, it was difficult – if not impossible – to intercept emails, at least in any meaningful way where the risk of revelation of confidential information was real. David Hricik, Lawyers Worry Too Much about Transmitting Client Confidences by Internet E-mail, 11 Geo. J. Legal Ethics 459 (1996). The article, I am proud to say, led bar associations and courts to hold there was a reasonable expectation of privacy over e-mail, and so lawyers could ethically use it. In part, their conclusion and mine, was based on the fact that the alternative – encrypting e-mail – was difficult to implement, and the risk of interception was low.

Fast forward and bar associations are reconsidering that cost benefit analysis. A Texas opinion in 2015, Tex. Prof’l Ethics Comm. Op. 648 (2015), identified six situations in which a lawyer should consider whether to encrypt or use some other safeguard:

• communicating highly sensitive or confidential information via email or unencrypted email connections;
• sending an email to or from an account that the email sender or recipient shares with others;
• sending an email to a client when it is possible that a third person (such as a spouse in a divorce case) knows the password to the email account, or to an individual client at that client’s work email account, especially if the email relates to a client’s employment dispute with his employer…;
• sending an email from a public computer or a borrowed computer or where the lawyer knows that the emails the lawyer sends are being read on a public or borrowed computer or on an unsecure network;
• sending an email if the lawyer knows that the email recipient is accessing the email on devices that are potentially accessible to third persons or are not protected by a password; or
• sending an email if the lawyer is concerned that the NSA or other law enforcement agency may read the lawyer’s email communication, with or without a warrant.

Id.

---

More recently, the ABA reconsidered its opinion early opinion from 1997, which cited to my very old article, in May 2017 when it issued ABA Formal Eth. Op. 477R. The ABA opinion stated that not every form of communication was appropriate for highly sensitive information:

In the technological landscape of Opinion 99-413, and due to the reasonable expectations of privacy available to email communications at the time, unencrypted email posed no greater risk of interception or disclosure than other non-electronic forms of communication. This basic premise remains true today for routine communication with clients, presuming the lawyer has implemented basic and reasonably available methods of common electronic security measures. Thus, the use of unencrypted routine email generally remains an acceptable method of lawyer-client communication.

However, cyber-threats and the proliferation of electronic communications devices have changed the landscape and it is not always reasonable to rely on the use of unencrypted email. For example, electronic communication through certain mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, constantly analyze how they communicate electronically about client matters, applying the Comment [18] factors to determine what effort is reasonable.

The opinion then pointed lawyers to a recently added comment to the Model Rules to help them identify when additional security measures might be required:

- The sensitivity of the information;
- The likelihood of disclosure if additional measures are not used;
- The cost of employing additional measures;
- The difficulty of implementing those measures; and
- The extent to which they adversely affect the lawyer’s ability to represent clients (e.g., making a device excessively difficult to use, given the risk).

See Model Rule 1.6, cmt. 18. The committee recommended that lawyers consider the following steps:

1. Understand the Nature of the Threat.

Understanding the nature of the threat includes consideration of the sensitivity of a client’s information and whether the client’s matter is a higher risk for cyber intrusion. Client matters involving proprietary information in highly

---

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_opinion_477.authcheckdam.pdf
sensitive industries such as industrial designs, mergers and acquisitions or trade secrets, and industries like healthcare, banking, defense or education, may present a higher risk of data theft. “Reasonable efforts” in higher risk scenarios generally mean that greater effort is warranted.

2. Understand How Client Confidential Information is Transmitted and Where It Is Stored.

A lawyer should understand how their firm’s electronic communications are created, where client data resides, and what avenues exist to access that information. Understanding these processes will assist a lawyer in managing the risk of inadvertent or unauthorized disclosure of client-related information. Every access point is a potential entry point for a data loss or disclosure. The lawyer’s task is complicated in a world where multiple devices may be used to communicate with or about a client and to store those communications. Each access point, and each device, should be evaluated for security compliance.

3. Understand and Use Reasonable Electronic Security Measures…

A lawyer should understand and use electronic security measures to safeguard client communications and information. A lawyer has a variety of options to safeguard communications including, for example, using secure internet access methods to communicate, access and store client information (such as through secure Wi-Fi, the use of a Virtual Private Network, or another secure internet portal), using unique, complex passwords, changed periodically, implementing firewalls and anti-Malware/Anti-Spyware/Antivirus software on all devices upon which client confidential information is transmitted or stored, and applying all necessary security patches and updates to operational and communications software. Each of these measures is routinely accessible and reasonably affordable or free. Lawyers may consider refusing access to firm systems to devices failing to comply with these basic methods. It also may be reasonable to use commonly available methods to remotely disable lost or stolen devices, and to destroy the data contained on those devices, especially if encryption is not also being used. …


Different communications require different levels of protection. At the beginning of the client-lawyer relationship, the lawyer and client should discuss what levels of security will be necessary for each electronic communication about client matters. Communications to third parties containing protected client information requires analysis to determine what degree of protection is appropriate. In situations where the communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required. For example, if client information is of sufficient sensitivity, a lawyer
should encrypt the transmission and determine how to do so to sufficiently protect it, and consider the use of password protection for any attachments. Alternatively, lawyers can consider the use of a well vetted and secure third-party cloud based file storage system to exchange documents normally attached to emails.

A lawyer also should be cautious in communicating with a client if the client uses computers or other devices subject to the access or control of a third party. If so, the attorney-client privilege and confidentiality of communications and attached documents may be waived. Therefore, the lawyer should warn the client about the risk of sending or receiving electronic communications using a computer or other device, or email account, to which a third party has, or may gain, access.

5. Label Client Confidential Information.

Lawyers should follow the better practice of marking privileged and confidential client communications as “privileged and confidential” in order to alert anyone to whom the communication was inadvertently disclosed that the communication is intended to be privileged and confidential. This can also consist of something as simple as appending a message or “disclaimer” to client emails, where such a disclaimer is accurate and appropriate for the communication.


Model Rule 5.1 provides that a partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

In the context of electronic communications, lawyers must establish policies and procedures, and periodically train employees, subordinates and others assisting in the delivery of legal services, in the use of reasonably secure methods of electronic communications with clients. Lawyers also must instruct and supervise on reasonable measures for access to and storage of those communications. Once processes are established, supervising lawyers must follow up to ensure these policies are being implemented and partners and lawyers with comparable managerial authority must periodically reassess and update these policies. This is no different than the other obligations for supervision of office practices and procedures to protect client information.

7. Conduct Due Diligence on Vendors Providing Communication Technology.
Consistent with Model Rule 1.6(c), Model Rule 5.3 imposes a duty on lawyers with direct supervisory authority over a nonlawyer to make “reasonable efforts to ensure that” the nonlawyer’s “conduct is compatible with the professional obligations of the lawyer.”

*Id.* (some footnotes omitted).

**b. Communicating by Email with Clients at their Workplaces.**

Here’s the fact pattern: your client is emailing you from their work email account, or your client is using a computer that its employer owns. (Your client is not the employer, but an individual.) Whether your client is in litigation with its employer — or someone else! — if the employer has policies in place and in use that allow it to monitor employee email or the computer itself, there likely is no reasonable expectation of privacy in those emails or in the files on the computer and, if so, no privilege.

Several cases have addressed this problem. See, e.g., Scott v. Beth Israel Med. Center, Inc., Civ. A. No. 3:04 - CV - 139 - RJC - DCK, 847 N.Y.S.2d 436 (Sup. Ct. 2007); Mason v. ILS Tech., LLC, 2008 WL 731557, 2008 BL 298576 (W.D.N.C. 2008); Holmes v. Petrovich Dev Co., LLC, 191 Cal. App. 4th 1047 (2011) (no privilege over employee communications with lawyer over company owned computer); Bingham v. BayCare Health Sys., 2016 WL 3917513, 2016 BL 233476 (M.D. Fla. July 20, 2016) (collecting cases addressing privilege waiver over emails sent or received through an employer’s server). Despite its repetitive nature, the problem persists and clients continue to be harmed through privilege waiver.

A New York decision adds the twist of the employee using an employer’s laptop to communicate with his lawyer where the employee was suing his employer. The applied the leading test to determine whether the employee knew that monitoring was allowed, and in fact occurred, and found the employee—former general counsel — could not withhold more than 106 files that he had created after he had been fired by the company on its laptop. Miller v. Zara USA, Inc., (N.Y. App. Div. June 6, 2017). The appellate court remanded the case to the trial court to determine if any of the documents were, although not privileged, nonetheless protected by work product.

It is important to recognize that -- even if the dispute is between your client and some third party, not an employer-employee dispute -- that third party can also rely on the lack of a reasonable expectation of confidentiality to show there is no privilege. And, finally, lawyers who draft these policies for clients may want to the unintended consequence of these policies is to deny the client’s employees the ability to claim privilege even in private disputes not involving the employer.

**c. Confidential Information on Digital Devices**

New York City Bar Opinion 2017-5 (July 2017) provides some interesting information about the care lawyers must take before allowing a lawful search of an
attorneys’ smartphone, laptop, or the like. The opinion is obviously important given the international nature of intellectual property practice and the growing frequency (still small, though) with which Customs officials ask for passwords that could reveal client confidences.

The opinion states lawyers should consider not carrying electronic devices that could permit disclosure to sensitive client information when traveling abroad, and, if asked upon return to provide access to the device, the opinion states:

At the border, if government agents seek to search the attorney’s electronic device pursuant to a claim of lawful authority, and the device contains clients’ confidential information, the attorney may not comply unless “reasonably necessary” under Rule 1.6(b)(6), which permits disclosure of clients’ confidential information to comply with “law or court order.” Under the Rule, the attorney first must take reasonable measures to prevent disclosure of confidential information, which would include informing the border agent that the device or files in question contain privileged or confidential materials, requesting that such materials not be searched or copied, asking to speak to a superior officer and making any other lawful requests to protect the confidential information from disclosure. To demonstrate that the device contains attorney-client materials, the attorney should carry proof of bar membership, such as an attorney ID card, when crossing a U.S. border.

Finally, if the attorney discloses clients’ confidential information to a third party during a border search, the attorney must inform affected clients about such disclosures pursuant to Rule 1.4.

d. Cloud Storage: HIPAA and Other Statutes?

Files are stored today in digital context, but not often only on a laptop or device. Instead, files are in the “cloud.” See generally, Jason Tashea, Cloudy Ethics, A.B.A. J. 30 (Apr. 2018).

For context, lawyers should analogize storage of files with these vendors with utilization of “real world” storage facilities for storage of paper files. In ABA Formal Opinion 08-451 (2008), the ABA joined other authorities and reemphasized that in selecting vendors who will receive client confidences, lawyers should examine whether the provision of confidences to the vendor is compatible with the lawyer’s duty of confidentiality to the client. The ABA stated that in the context of storing electronic data, lawyers should consider these steps:

- reference checks and vendor credentials;
- vendor’s security policies and protocols;
- vendor’s hiring practices;
- the use of confidentiality agreements;
- vendor’s conflicts check system to screen for adversity; and
• the availability and accessibility of a legal forum for legal relief for violations of the vendor agreement.

Other state bar associations have reached similar conclusions. E.g., Fl. St. B. Ass’n. Eth. Op. 12-3 (Jan. 25 2013) (collecting numerous opinions).

It is imperative to use password protection for all stored files, regardless of the security of the vendor. In a recent case, the investigator for a party used a cloud storage service and opposing party was mistakenly given access to it by a link, and the entire plaintiff’s file was made available. See Jason Tashea, Cloudy Ethics, A.B.A. J. 30 (Apr. 2018) (discussing this case, Harlesville Ins. Co. v. Holding Funeral Home). Luckily, because the investigator had used password protection – the link was direct – the district court held privilege had not been waived despite the inadvertent disclosure.

Statutes impact different practitioners depending on their practice. HIPAA, patent practice, and others can create specific and additional requires.48 A recent article concerning HIPAA gave this checklist:

Is your healthcare cloud actually storing patient health information?

De-identified data is not PHI, but encrypted PHI is still PHI. Most, if not all, commercial CSPs willing to sign a BAA with a CE will require that PHI be encrypted before being stored on the infrastructure.

What are a healthcare CSP’s obligations with respect to encrypted PHI?

The CSP is responsible, under the HIPAA regulations, for maintaining the integrity and availability of the PHI. That does not change if the PHI is encrypted.

What does a CE need to do to confirm that a healthcare CSP is in compliance?

A CE must confirm to its satisfaction that technical issues, such as potential malware attacks, are dealt with appropriately and that administrative and

48 Patent practitioners should consider this advice in light of two particular risks of patent practice: (a) information could be revealed which would result in loss of novelty rights or loss of trade secret protection, and (b) patent practitioners who rely upon cloud-based storage companies who store the information outside the United States may need to consider the Export Administration Regulations and similar laws. See generally, Thomas L. Kundert, Invention Secrecy Guide: Foreign Filing Licenses, Secrecy Orders, and Exports of Technical Data, 88 J. Pat. Off. Soc’y 664 (Aug. 2006). Among other things, regulations exempt export of covered data only if certain security measures are kept: “Such security precautions may include encryption of the technical data; the use of secure network connections, such as virtual private networks; the use of passwords or other access restrictions on the electronic device or media on which the technical data is stored; and the use of firewalls and other network security measures to prevent unauthorized access.” 22 C.F.R. 125.4(b)(9)(ii).
physical safeguards are in place regarding physical security and contingency planning (for example, data center redundancy to deal with potential natural disasters or other emergencies). Not everyone is welcome to inspect the cloud storage facilities, so CSPs commonly conduct third-party audits and share the reports (such as system and organization controls reports) with customers.

Is there anything else to consider?

A CE needs to confirm that a CSP’s service-level agreement does not conflict with HIPAA compliance. For example, if the SLA does not guarantee near-100 percent uptime, is the CE maintaining “availability” of PHI as it must? Does the SLA include sufficient protections against the potential effects of a ransomware attack?

Speaking of ransomware, should a CE maintain an “air-gapped” backup, separate from its main cloud instance, just in case? Does the CSP agreement provide adequate assurances that the CE’s access to its records, its patients’ PHI, will not be blocked or terminated? Where is the data center located? If it is offshore, that may be fine from a regulatory perspective, but be sure to think about how easy or difficult it may be to enforce your rights in a foreign justice system.

Keep Other Regulations in Mind When Storing PHI in the Cloud

Finally, it is important to remember that cloud storage of health data is not always, or only, a HIPAA issue.

Depending on the type of data, the parties involved, and the way in which they are contracting regarding the storage and use of the data, a number of other regulatory schemes may be implicated.

For example, it may be necessary to consider the Title 42 of the Code of Federal Regulations Part 2 approach to confidentiality, the Federal Trade Commission approach to regulating individual data privacy rights, individual states’ approaches to regulating the storage and use of health data, or even other countries’ approaches (for example, the European Union’s General Data Protection Regulation).

David Harlow, How to Ensure your Cloud Storage is HIPAA Compliant (July 25, 2018) (available here: https://healthtechmagazine.net/article/2018/07/how-ensure-your-healthcare-cloud-storage-stays-hipaa-compliant-percon)

e. Phishing and More

Of course, the weakest link in cybersecurity remains the human component. Employees who download malware, or who click on phishing emails are the common
culprits, allowing “ransomware” and more to occur. See Mary Ellen Egan, *Cyberthreats 101*, A.B.A. J. 30 (March 2018).

4. **Conclusion**

Because of Moore’s Law, soon lawyers will be able to provide with greater efficiency a broader range of services on line than are currently available. Each new technological advance creates new ethical issues, however, that lawyers must take care to examine and respond to.
Big Data And Protected Data: Legal Ethics Issues Around The Handling By And For Clients

Presented By:

Ann Moceyunas
Surgical Information Systems, LLC
Alpharetta, GA
Big Data and Protected Data:

Legal Ethics Issues Around Handling by and for Clients

By Ann K. Moceyunas

Presented to the Privacy & Technology Law Institute,
State Bar of Georgia Privacy & Technology Law Section,
October 19, 2018, Atlanta, Georgia.
TABLE OF CONTENTS

1. Introduction - Big Data and Protected Data ...................................................... 1

2. Legal Ethics Obligation: Technology Competence ......................................... 3
  2.1. Adopted by most US States .......................................................................... 3
  2.2. Not Yet Adopted in Georgia, but Relevant .................................................. 5

3. Legal Ethics Obligation: Client Confidentiality and Technology ...................... 6

4. Example: Obligations of Lawyer as Business Associate ................................ 9
  4.1. When a Lawyer is a Business Associate ..................................................... 9
  4.2. Engaging Downstream Business Associates ............................................. 10
  4.3. Special Ethical Issues when Lawyer is a Business Associate ..................... 11
  4.4. Case Study: AETNA Class Action Lawsuit .............................................. 14

5. Data Privacy Ethical Frameworks .................................................................... 16
  5.1. Privacy as a Right ...................................................................................... 16
  5.2. Big Data Collection and Use “Best Practices” ......................................... 17

6. Conclusion – Legal ethics continues to lag other professions with respect to data collection ethics ................................................................................................. 21

Appendix 1 - State Survey of Rules of Professional Conduct – Technology Competence ................................................................................................................. 22

Appendix B .......................................................................................................... 24
Big Data and Protected Data: Legal Ethics Issues Around Handling by and for Clients

By Ann K. Moceyunas¹

1. Introduction - Big Data and Protected Data.

A lawyer, whether solo, law firm, in-house, or government, is encountering “big data” and “protected data” either for the business (for example in marketing or business analytics) or for a client (whether collecting data from primary sources or handling a client’s data). The ABA has defined “big data” as “data of sufficient volume, complexity or velocity that it exceeds the capability of conventional current technology or methodology to process or analyze conventionally.”² “Protected Data” for purpose of this paper is defined as data that is subject to legal protection whether by statute, regulation, or contract, such as personally identifiable data or protected health information. Bar associations and courts have addressed the professional ethics issues raised by lawyers using technology in practice for years. However, there are not

¹ © 2018 Ann K. Moceyunas. Ann K. Moceyunas is an attorney in Atlanta, Georgia, with extensive experience in technology law and business. She is General Counsel for Surgical Information Systems, LLC, a software and services company for hospitals and ambulatory surgery centers. Her prior legal experience includes serving as general counsel for two other technology companies in Atlanta, prior to which time she litigated commercial matters including intellectual property disputes. Ms. Moceyunas has taught the topics of technology law and ethics as an Assistant Professor for the Siegel Institute of Law, Ethics, and Character and the CS/IS Department at Kennesaw State University. She earned her B.A. with honors from Binghamton University in 1981 and her J.D. from University of Buffalo School of Law in 1984. Ann can be reached at ann@moceyunas.com. The comments in this paper reflect Ms. Moceyunas’ personal views and do not reflect the views of her client.

corresponding professional rules of conduct for the collection and use of Big Data and Protected Data that is other than the client’s confidential information.

Rene Knake, in a 2016 article\(^3\) outlines legal ethics obligations (using the ABA Model Rules) relevant to big data, among which are:

- to **communicate** with the client about how the lawyer will accomplish the client’s objectives. ABA Model Rule 1.4;

- to **maintain technology competence**. ABA Model Rule 1.1; Comment 8;

- to **protect confidentiality** of all information related to the representation of the client. ABA Model Rule 1.6;

- to **maintain and preserve client records** and promptly **return** upon request. ABA Model Rule 1.15 and 1.16; and

- **supervise** all non-lawyers that provide assistance. ABA Model Rule 5.3.

Several bar associations and courts have addressed some of these issues with a clear direction. However, Professor Knake also suggests that lawyers need to grapple with ethical issues that are not currently addressed by rules of professional conduct including:

- whether there should be a duty of notice and consent for collection of personally identifiable data and issues arising out of secondary use;

- access and ownership of data, including the original data and the compiled data;

---

\(^3\) How Big Data Analytics is Changing Legal Ethics (Perspective), by Renee Knake, Professor of Law, University of Houston Law Center, August 9, 2016. [https://biglawbusiness.com/how-big-data-analytics-is-changing-legal-ethics/]
- whether there should be a duty to anonymize personally identifiable or sensitive data;
- reliability and integrity of data sources;
- data security beyond the professional obligation to maintain client confidentiality; and
- technology competency around the process of data collection and analytics.

Ethical frameworks for the collection and use of data are embodied in laws and regulations in the U.S. and other countries. Industry trade groups and professional groups other than bar associations promulgate ethical codes for collecting and using personally identifiable data. The professional rules of conduct for lawyers have evolved to address technology competence, but have not done so with respect to ethical standards for collection and use of big data, most particularly, personally identifiable data.

2. Legal Ethics Obligation: Technology Competence.

2.1. Adopted by most US States.

Two thirds of U.S. states require a lawyer to maintain technology competence as an ethical matter. In 2012, the American Bar Association approved an amendment to a comment to Model Rule of Professional Conduct 1.1 regarding the ethical obligation of competence⁴ that mandates technology competence as well as legal competence:

⁴ Model Rule 1.1. “A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” (available at https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html)
To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject [emphasis added].

Thirty states have adopted Comment 8 to the ABA Model Rule 1.1, three states have enacted their own technical competency requirement, and seventeen states and the District of Columbia have not adopted a technology competence requirement. 5

New Hampshire, as one of the three with its own policy, has taken a more practical approach to this technology competence requirement, employing a “reasonable” standard of care measured by “similarly situated” lawyers:

ABA comment [8] (formerly Comment [6]) requires that a lawyer “should keep abreast of . . . the benefits and risks associated with relevant technology.” This broad requirement may be read to assume more time and resources than will typically be available to many lawyers. Realistically, a lawyer should keep reasonably abreast of readily determinable benefits and risks associated with applications of technology used by the lawyer, and benefits and risks of technology lawyers similarly situated are using.

New York, another of the three states with its own policy, specifically calls out the storage and transmission of confidential information as part of technology competence:

5 See Appendix 1 for references.

6 Outside the Rules of Professional Conduct, the New York trial courts require e-discovery competence (“[C]ounsel for all parties who appear at the preliminary conference must be sufficiently versed in matters relating to their clients' technological systems to discuss competently all issues relating to electronic discovery: counsel may bring a client representative or outside expert to assist in such e-discovery discussions. Uniform Rules for N.Y. State Trial Courts, Section 202.12 Preliminary conference.)
store or transmit confidential information, and (iii) engage in continuing study and education and comply with all applicable continuing legal education requirements under 22 N.Y.C.R.R. Part 1500 [emphasis added].

2.2. Not Yet Adopted in Georgia, but Relevant.

Georgia has not yet adopted a requirement for technology competence in the Georgia Rules of Professional Conduct. The ABA explained that its inclusion of “technology competence” to the comments of Model Rule 1.1 made explicit an implicit obligation: “it is important to make this duty explicit because technology is such an integral – and yet at times invisible – aspect of contemporary law practice.”7 Technology competence is implicit and unavoidable for a Georgia lawyer who wants to use technology to provide better, more efficient, and more cost-effective results for clients, for example, eFiling in Georgia Courts8 and U.S. Federal Courts9, ediscovery, and use of email and electronic file storage. The ethical obligation to maintain the confidentiality of information gained in the professional relationship with a client10 implies an obligation to evaluate and determine whether an electronic communication tool will meet the

---

8 eFiling in Georgia Courts, State Bar of Georgia. https://www.gabar.org/efiling.cfm
10 “(a) A lawyer shall maintain in confidence all information gained in the professional relationship with a client, including information which the client has requested to be held inviolate or the disclosure of which would be embarrassing or would likely be detrimental to the client, unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, or are required by these Rules or other law, or by order of the Court.” Georgia Rule 1.6 Confidentiality of Information.
confidentiality obligations. Additionally, as discussed below, the Georgia lawyer may have legal obligations with respect to the security of certain types of data protected by law and regulations. As recognized by the ABA, “[a]t the intersection of a lawyer’s competence obligation to keep ‘abreast of knowledge of the benefits and risks associated with relevant technology,’ and confidentiality obligation to make ‘reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client,’ lawyers must exercise reasonable efforts when using technology in communicating about client matters.”

3. Legal Ethics Obligation: Client Confidentiality and Technology.

ABA Model Rule 1.6 requires an attorney to protect the confidentiality of information “relating to the representation of a client” with certain exceptions. It further states that “[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”

The comments address security standards and the interplay of privacy laws:

[18] . . . A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client’s information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules [emphasis added].

---

12 ABA Model Rule 1.6 (c).
When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules [emphasis added].

Georgia Professional Rules of Conduct 1.6 is similar but does not include any comments addressing security or privacy, other than a reference to “another provision of law.”

The ABA and other states have examined the ethical issues with technology in the context of maintaining client confidential information, such as:

(a) Email. In 2017, the ABA revised its opinion about email:

A lawyer generally may transmit information relating to the representation of a client over the internet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.13

(b) Remote access to computers. In 2014, the New York State Bar Association Committee on Professional Ethics issued an opinion that a law firm could ethically permit remote access to its computer system by its workforce, but should “determine that the technology it will use to provide remote access (as well as the devices that firm lawyers will use to effect remote access), provides reasonable assurance that confidential client information will be protected,” and that, if it could not reach that conclusion, the law firm could request the client’s informed consent.\(^{14}\)

(c) Cloud storage. In 2016, the Illinois State Bar Association issued an Advisory Opinion concluding:

A lawyer may use cloud-based services in the delivery of legal services provided that the lawyer takes reasonable measures to ensure that the client information remains confidential and is protected from breaches. The lawyer’s obligation to protect the client information does not end once the lawyer has selected a reputable provider.\(^{15}\)

But these opinions and rules address the security and confidentiality of data after it has been “collected”. They also do not address ethics at the point of collection and use involving personally identifiable information.

---


4. Example: Obligations of Lawyer as Business Associate.

The ethical obligations of technology competence and confidentiality meet up with legal obligations when a lawyer serves in the capacity of a business associate handling a client’s protected health information.

4.1. When a Lawyer is a Business Associate

A lawyer becomes a “business associate”\(^{16}\) under the HIPAA Privacy Rule when she has more than incidental access to protected health information of a client that is a covered entity (health plans, health care clearinghouses, and certain health care providers) in connection with the legal services.\(^{17}\) The HIPAA Privacy Rule\(^{18}\) imposes, by law, the obligations of a business associate on the lawyer, whether the lawyer is aware that it has had access to protected health information in the capacity of a business associate and must comply with the HIPAA Privacy Rule and the HIPAA Security Rule.\(^{19}\)

The business associate role can arise in several types of legal representation, for example:

1. Medical malpractice defense;

---

\(^{16}\) 45 C.F.R. §160.103.


\(^{18}\) Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E

\(^{19}\) Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Parts 160, 162 and 164. This paper does not examine all the requirements imposed by HIPAA Privacy Rule and Security Rule on the lawyer as business associate.
2. Patient bill collections;

3. Providing advice on HIPAA compliance such as responding to a data breach;

or

4. Other litigation where discovery may include access to patient records.

The engagement can be as direct counsel to the covered entity, as counsel to another business associate, or as co-counsel to either. The lawyer as business associate must have a business associate agreement with the other party that gives rise to the business associate relationship\(^\text{20}\) as well as compliance with HIPAA Security Rule standards.

4.2. Engaging Downstream Business Associates.

If the lawyer engages any outside service provider that will handle the protected health information, that outside service provider likewise becomes a downstream business associate to the lawyer. For litigation matter, those providers could include other legal counsel, jury experts, document or file managers, investigators, and litigation support personnel.\(^\text{21}\) But general service providers can also be business associates, whether nor not engaged for a specific legal matter, such as:

- Email service if email is stored by the ISP (such as Office365)
- Teleconferencing service (such as Webex)


- Paper Shredding company
- Printer/Copier repair or leasing company if copier retains PHI
- Record storage company
- Cloud storage company (such as Office365 or iCloud)
- Printing Services company
- IT service company (such as for system security monitoring, backup, disaster recovery).

A “conduit” such as US Postal Service, FedEx, UPS, courier service will not be business associates, as well as those services that are not intended to have access to PHI, such as the office cleaning service.\textsuperscript{22} If a law firm expects to be handle matters that create a business associate relationship with a client or other lawyer, the law firm must have an ongoing security program.\textsuperscript{23} As part of that program, the law firm has to evaluate each vendor, whether the vendor will handle PHI, and if so, have an appropriate business associate agreement and further evaluation of the vendor’s own security program.

4.3. Special Ethical Issues when Lawyer is a Business Associate.

The legal obligations as business associate raises some potential conflicts with the ethical obligations as lawyer.

1. Business Associate Agreement. Entering into the business associate agreement with the client invokes the requirements to avoid conflicts of interest. Under Georgia Rule of Professional Conduct 1.8, the lawyer would be required to: (a) negotiate a business associate agreement that is “fair and

\textsuperscript{22} See footnote 17, \textit{supra}.
\textsuperscript{23} 45 CFR § 164.314(a)(2).
reasonable to the client”; (b) fully disclose the agreement “in a manner which can be reasonably understood by the client”; (c) advise the client “in writing of the desirability of seeking and is given reasonable opportunity to seek the advice of independent counsel”; and (d) confirm that the “client gives informed consent, in a writing signed by the client, to the essential terms of the transition and the lawyer’s role in the transaction.”

2. **Malpractice Claims.** Often, business associates seek to limit liability to the covered entity (or upstream business associate). However, Georgia Rule of Professional Conduct 1.8 would appear to limit the lawyer’s ability to limit liability in the business associate agreement: “A lawyer should not seek prospectively, by contract or other means, to limit the lawyer’s individual liability to a client for the lawyer's malpractice.”24 The lawyer may also want to confirm with the lawyer’s malpractice insurer whether failure to comply with the HIPAA Privacy and Security Rule and other data breaches will be covered by professional liability coverage.

3. **Access to Records.** A business associate must “make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary [of HHS] for purposes of determining the covered entity's compliance. . .”25 The business associate agreement must include this obligation, so it would appear that the client has

---

24 Comment 8.
25 45 C.F.R. § 164.504(e)(2)(ii)(i).
consented to such disclosure, per Georgia Rule of Professional Conduct 1.6 (Confidentiality of Information). HHS declined to make an exception for attorneys from this access requirement, explaining in the 2002 comments to the Privacy Rule, “[t]he Privacy Rule is not intended to interfere with attorney-client privilege. Nor does the Department anticipate that it will be necessary for the Secretary to have access to privileged material to resolve a complaint or investigate a violation of the Privacy Rule.”

4. **Patient Requests.** A business associate is also required to provide an accounting of disclosures to the covered entity who has an obligation to provide such accounting to and upon request of a patient. The definition of “disclosure” has been unclear since 2011 when the Office for Civil Rights issues a notice proposed rulemaking that would have required an accounting of not only disclosures and access (which includes workforce and subcontractors). Such an accounting could impinge on attorney-client confidential communications (as between the covered entity client and lawyer business associate) or attorney work product (as between the lawyer business associate and a service provider business associate such as an expert witness). HHS has recently published notice that it intends to solicit public comment on

---

27 45C.F.R. §164.528
modifying the accounting rule and withdraw the prior notice of proposed rulemaking.  

4.4. Case Study: AETNA Class Action Lawsuit

In January 2018, Aetna settled a federal class action lawsuit that alleged a HIPAA disclosure violation by a mailing to 13,487 class action members related to settlement of prior class action lawsuits. The mailing disclosed the HIV status of the Aetna customer in a large envelope window that revealed the contents of the notice letter. The New York Attorney General opened its own investigation for the 1,460 New York Aetna members who were sent the mailer. The actions alleged that Aetna provided the protected health information to its outside counsel, who in turn provided it to a third-party settlement administrator to handle the mailers. While Aetna had a business associate agreement with the law firm, neither the law firm or Aetna had a business associate agreement with the third-party settlement administrator. In the federal settlement, Aetna agreed to pay $17.2 million into a settlement fund and agreed to develop and implement a “best practices” policy for use of protected health information in litigation (see the policy attached in

---

29 https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201804&RIN=0945-AA00  
Appendix B to this paper). The federal settlement also outlined specifically the steps Aetna must take to maintain confidentiality of customers in a subsequent mailing. In the New York settlement, Aetna agreed to pay $1.15 million.

The story is further developing. In February 2018, Aetna sued the third party settlement administrator, Kurtzman Carson Consultants (KCC), in a Philadelphia federal court, alleging that KCC negligently sent the mailers in windowed envelopes, despite a proposal to use a standard envelope. KCC filed its own lawsuit in a Los Angeles federal court against Aetna. In May 2018, Aetna sued the law firm, Whatley Kallas, LLP, and consumer advocacy group that brought the initial class-action lawsuit, alleging that they were the ones who suggested using KCC, that KCC’s proposal for the mailing identified Whatley Kallas the client, not Aetna’s law firm, and that Whatley Kallas supervised the work of KCC and failed to review the final proofs of the mailer.

This sad tale highlights key requirements for HIPAA compliance:


1. **BAA** - Law firm that engages a subcontractor that will handle the client’s protected health information must have a business associate agreement with the subcontractor.

2. **Disclosures** – unauthorized disclosures don’t just happen with electronic protected health information. All links in the communication chain must comply, even mailing envelopes.

3. **Security** – one of the allegations was that the law firm sent the data file with patient names to the printer in an unencrypted manner. HIPAA security rule requires encryption or similar security measures to prevent unauthorized access and preserve data integrity.

5. **Data Privacy Ethical Frameworks.**

   U.S. data privacy law, particularly state law, has been evolving, with an increase in the pace over the past two years, but still without a comprehensive national standard. There are some state and federal laws that address the legality of the collection and use of data; all fifty states have some law on notices for a data breach (mostly limited). None of the professional rules of conduct have explicit ethical standards with respect to the collection and use of personally identifiable data that is not related to a client’s confidential, even while other professions have included data privacy in their ethics codes.

   5.1. **Privacy as a Right.**

   The definition of and respect for “privacy” as a human right has evolved, but more quickly with the development of computers and the Internet. In Euro-US culture, a “right” of privacy grew out of an extension of territorial-spatial (“property”) rights to
include personal life-space. Warren and Brandeis in their famous 1890 Harvard Law Review article, “The Right to Privacy”, described the evolution of the law of privacy from property to protection of human inner space: “This development of the law was inevitable... Thoughts, emotions, and sensation demanded legal recognition and the beautiful capacity for growth which characterizes the common law enable the judges to afford the requisite protection, without the interposition of the legislature.” They argued the law should continue to evolve to protect the right to be let alone. In 1965, the U.S. Supreme Court found an implicit right to privacy within the U.S. Constitution (in the context of birth control). The twenty first century would bring into sharp focus the benefits and harm to be caused using technology that could collect, compile, analyze, store, retrieve data about individuals on a massive scale.

5.2. Big Data Collection and Use “Best Practices”.

The US and Europe have recognized a “right of privacy” from opposite views: US recognizing a “right” and codifying it in a patchwork of situations, Europe recognizing it as a fundamental human right codified in an overarching limitation on collection and use by all data collectors. In 1973, the US government issued its first significant step toward codification of ethical standards around “record-keeping practice in the computer age,”

proposing a “Code of Fair Information Practice” which Congress codified in the Privacy Act of 1974. In 1980, the Organisation for Economic Co-operation and Development issued guidelines for the protection of privacy of personal data, calling for eight guiding principles including: knowledge and consent of data subject, relevancy to purpose, limitation on use, security transparency, and individual participation rights. The personal data ethical principles have driven a patchwork of laws in the US, but no comprehensive scheme yet. In contrast, the European Union issued its privacy directive in 1995 and recently replaced by the General Data Protection Regulation that

---

embodied similar principles, beginning a fierce global wrangling over the treatment of personal data, that continues up to today.46

The best practices of these laws, whether US or Europe, have in common the following obligations of the data collector of personally identifiable information:

1. Notice and consent to the data subject;
2. Limitation on collecting the minimum necessary;
3. Implementation of security to prevent unauthorized disclosure;
4. Right of data subject to review and correct data; and
5. Duty to retain for minimum necessary time.

In the US, industry groups other than lawyers have adopted these best practices into their ethics codes, for example, marketing47, software engineering48, data sciences49 and medical research50.

Several U.S. states have laws that establish standards for the security of personal information.51 More importantly all fifty state laws have laws that require notice of data

---

46 For comparative analysis of data protection globally, see Data Protection Laws of the World, DLA Piper. https://www.dlapiperdataprotection.com/
48 Association for Computing Machinery, Code of Ethics and Professional Conduct, https://ethics.acm.org/
51 See for example, California Consumer Privacy Act of 2018, Assembly Bill No. 375; Colorado, HB18-1128, Protections For Consumer Data Privacy (eff. 9/1/2018); Massachusetts 201 C.M.R. 17, Standards for the Protection of Personal Information of Residents of the Commonwealth; Nebraska, LB 757 (eff. 7/18/2018); and Vermont H. 764 passed May 2018.
breach of personally identifiable information, although the breadth and width of what data is protected and notice varies greatly. Most of these laws are primarily focused on mitigating identity theft of personally identifiable information in electronic form and related data (such as financial information). In Georgia, the data breach notification law applies to “Data collectors” (a state or local agency) and “information brokers”. A “information broker” means:

“any person or entity who, for monetary fees or dues, engages in whole or in part in the business of collecting, assembling, evaluating, compiling, reporting, transmitting, transferring, or communicating information concerning individuals for the primary purpose of furnishing personal information to nonaffiliated third parties, but does not include any governmental agency whose records are maintained primarily for traffic safety, law enforcement, or licensing purposes.”

The Georgia law requires a Data Collector or Information Broker to provide notice of a breach in the security of computerized data to all affected residents of Georgia. Any person or business that maintains that type of computerized data for a Data Collector or Information Broker must notify the Data Collector or Information Broker of a data security breach with 24 hours of discovery. A Georgia law firm that either collects such data on its own or is holding such data for an information broker client would have an obligation to report a data security breach, which implies that the law firm 1) is aware of the collection/storage activity, 2) has processes in place to detect a data security breach, and 3) has processes for responding to and reporting a data security breach.

See, interactive Summary of U.S. State Data Breach Notification Statutes, Davis Wright Tremaine LLP. https://www.dwt.com/statedatabreachstatutes/

52 O.C.G.A.§10-1-911(3).
53 O.C.G.A. §10-1-912(a).
54 O.C.G.A. §10-1-912(b).
55 O.C.G.A.§10-1-912(b).
6. **Conclusion** — Legal ethics continues to lag other professions with respect to data collection ethics.\footnote{Universal principles of data ethics, 12 guidelines for developing ethics codes. Accenture. https://www.accenture.com/t20160629T012639Z_w_/us-en/acnmedia/PDF-24/Accenture-Universal-Principles-Data-Ethics.pdf}

Lawyers are obligated to compliance with rapidly changing state and federal laws regarding data collection. Technology competence, as the ABA concluded, would seem to be an obvious standard to add to the lawyer’s obligation of legal competency. Not so obvious are adding standards around data collection, particularly personally identifiable data as ethical requirements. Lawyers will need to respond to the practical effects of the European GDPR and the handful of states that have data security standards as well as the security breach notice requirements in all fifty states with internal policies and procedures that meet the least common denominator. The HIPAA Privacy Rule and Security Rule can serve as a model for those policies and procedures. But until the US has a national and comprehensive data protection law, the legal profession is likely to continue to lag other professions to apply ethical standards that exceed legal standards to personally identifiable information.

A. No requirement for technology competence (17 states and DC).

1. Alabama
2. District of Columbia
3. Georgia
4. Hawaii
5. Louisiana
6. Maine
7. Maryland
8. Michigan
9. Mississippi
10. Montana
11. Nevada
12. New Jersey
13. Oregon
14. Rhode Island
15. South Carolina
16. South Dakota
17. Texas
18. Vermont

B. States that have adopted Comment 8 to Rule 1.1.

1. Alaska
2. Arizona
3. Arkansas
4. Colorado
5. Connecticut
6. Delaware
7. Florida
8. Idaho
9. Illinois
10. Indiana
11. Iowa
12. Kansas
13. Kentucky
14. Massachusetts
15. Minnesota
16. Missouri
17. Nebraska
18. New Mexico
19. North Carolina
20. North Dakota  
21. Ohio  
22. Oklahoma  
23. Pennsylvania  
24. Tennessee  
25. Utah  
26. Virginia  
27. Washington  
28. West Virginia  
29. Wisconsin  
30. Wyoming

C. Technology Competency Requirement Other than Model Comment (3 states).

California

“An attorney’s obligations under the ethical duty of competence evolve as new technologies develop and become integrated with the practice of law. The State Bar of California Standing Committee on Professional Responsibility and Conduct Formal Opinion No. 2015-193.”


New Hampshire

“ABA comment [8] (formerly Comment [6]) requires that a lawyer should keep abreast of . . . the benefits and risks associated with relevant technology.” This broad requirement may be read to assume more time and resources than will typically be available to many lawyers. Realistically, a lawyer should keep reasonably abreast of readily determinable benefits and risks associated with applications of technology used by the lawyer, and benefits and risks of technology lawyers similarly situated are using.” https://www.courts.state.nh.us/rules/pcon/pcon-1_1.htm

New York

“To maintain the requisite knowledge and skill, a lawyer should (i) keep abreast of changes in substantive and procedural law relevant to the lawyer’s practice, (ii) keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information, and (iii) engage in continuing study and education and comply with all applicable continuing legal education requirements under 22 N.Y.C.R.R. Part 1500.

Appendix B

AETNA Use of Protected Health Information In Litigation – Best Practices Policy
Use of Protected Health Information in Litigation – Best Practices Policy

<table>
<thead>
<tr>
<th>Procedure Name:</th>
<th>Use of Protected Health Information in Litigation – Best Practices Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Procedure Number:</td>
<td>###</td>
</tr>
<tr>
<td>Effective Date:</td>
<td></td>
</tr>
<tr>
<td>Business Unit Name:</td>
<td>Litigation</td>
</tr>
<tr>
<td>Business Owner:</td>
<td></td>
</tr>
<tr>
<td>Department Head:</td>
<td></td>
</tr>
<tr>
<td>Approval Date:</td>
<td></td>
</tr>
<tr>
<td>Type</td>
<td>New</td>
</tr>
<tr>
<td>Applicable Business</td>
<td>Litigation</td>
</tr>
</tbody>
</table>

Document Control and Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Effective Date</th>
<th>Author</th>
<th>Comments</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For Aetna Use Only
Table of Contents

Document Control and Version History................................................................. 1
Background ........................................................................................................ 3
Purpose ............................................................................................................... 3
Scope ................................................................................................................ 4
Definitions........................................................................................................ 4
Use of PHI in Litigation – Best Practices ......................................................... 5
Background

Aetna, Inc., Aetna Life Insurance Company and Aetna Specialty Pharmacy, LLC ("collectively, "Aetna is a "covered entity" as defined in the Health Insurance Portability and Accountability Act of 1996, as amended ("HIPAA"), and its implementing rules and regulations, including the Standards for Privacy of Individually Identifiable Health Information (the “HIPAA Rules”). As a covered entity, Aetna has certain legal obligations regarding the use and disclosure of protected health information ("PHI") in its possession. In general, Aetna may not use or disclose an individual’s PHI for purposes unrelated to treatment, payment or health care operations (which includes conducting or arranging for litigation services), without first obtaining the individual’s signed authorization. This general rule is subject to certain specified exceptions. One of those exceptions covers the use and disclosure of an individual’s PHI in judicial and administrative proceedings.

The obligations relating to the use and disclosure of PHI apply not only to covered entities like Aetna, but also to their business associates. A “business associate” is, among other things, a person or entity who “creates, receives, maintains, or transmits” PHI in the course of performing services on behalf of the covered entity. Thus, retained litigation counsel for Aetna is a business associate if it “creates, receives, maintains, or transmits” PHI in the course of its representation of Aetna. As explained below, it is Aetna’s policy that all retained litigation counsel for Aetna must execute an Aetna-approved business associate agreement ("BAA") with Aetna or sub-BAA with litigation counsel before it may perform legal services. Aetna-approved BAAs require Aetna’s business associates to keep PHI secure and to only use and disclose PHI for the purposes for which they are engaged.

In addition, Aetna has certain additional legal obligations relating to the use and disclosure of specific classes of PHI, including information relating to health plan members’ HIV status and behavioral health and substance use disorder treatment. These requirements apply equally to retained litigation counsel who have access to these classes of PHI.

Purpose

The purpose of this Use of Protected Health Information in Litigation – Best Practices Policy ("Best Practices Policy") is to implement comprehensive, best practices policies and procedures for the use of PHI in litigation in which Aetna is a party, and establish specialized processes for litigation involving heightened privacy concerns, including health plan members’ HIV-related and behavioral health and substance use disorder information. This Best Practices Policy also sets forth policies and procedures for the disclosure of PHI when Aetna is not a party to an action. This Best Practices Policy is designed to provide best practices in addition to satisfying any legal requirements that may exist.
Scope

This Best Practices Policy applies to all litigation managed by Aetna’s litigation group supervised by Aetna’s Head of Litigation ("Head of Litigation;" currently, Ed Neugebauer).

Definitions

**BA:** Business Associate. A business associate is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity.

**BAA:** Business Associate Agreement. A business associate agreement is a contract between a covered entity (such as a health plan) and a BA. The BAA protects PHI in accordance with HIPAA Rules.

**CE:** Covered Entity. A covered entity is any entity that is (i) a health care provider that conducts certain transactions in electronic form (called here a “covered health care provider”); (ii) a health care clearinghouse; or (iii) a health plan. Aetna is a CE because it is a health plan.

**HIPAA Rules:** HIPAA Rules is defined herein as HIPAA and its implementing rules and regulations, including the Standards for Privacy of Individually Identifiable Health Information (“Privacy Rule”).

**PHI:** Protected Health Information, or PHI, as defined in 45 C.F.R. 160.103, includes information maintained by Aetna or one of its BAs that identifies an individual and relates to the individual’s health condition, medical treatment or payment for health care. As explained below, PHI can be part of many different types of records, such as claims data, medical records and pre-certification information. PHI also includes demographic information such as dates of birth or zip codes that are part of a data set that has been derived from records containing health information, even if no health information remains in that data set.

**QPO:** Qualified Protective Order. A Qualified Protective Order is an order from a court that limits use and disclosure of PHI in litigation. Pursuant to 42 C.F.R. 164.512(e)(1)(v), a QPO must meet the following requirements: (1) prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding; and (2) requires the return to the covered entity or destruction of the PHI at the end of the litigation or proceeding.
Use of PHI in Litigation – Best Practices

Consistent with Aetna’s Guide for Outside Counsel and related addenda (the “Guide”), it is critical that
Aetna and retained litigation counsel follow federal laws, including HIPAA Rules, and applicable state
laws regarding the use, disclosure and handling of PHI, including information related to HIV, behavioral
health, and substance use. Aetna may use or disclose PHI without the written authorization of the
individual referenced in the PHI in limited situations such as in connection with judicial proceedings,
subject to specific rules and limitations. This Best Practices Policy summarizes “best practices” that
Aetna and retained litigation counsel must follow in connection with the use and disclosure of PHI in
judicial proceedings and pre-litigation negotiations.

1. All Retained Litigation Counsel Must Sign An Aetna-Approved BAA

All retained litigation counsel who work on Aetna litigation matters must sign an Aetna-approved BAA or
sub-BAA before starting work, regardless whether PHI may or may not be disclosed as part of the
matter. Exceptions to this rule may be granted only in limited circumstances with the express written
approval by Aetna’s Head of Litigation.

Aetna will establish a SharePoint with signed BAAs for retained litigation counsel. Aetna personnel must
verify that a signed Aetna-approved BAA is in place before retained litigation counsel may commence
work. Aetna will, on a periodic basis (and at least once annually) perform audits to ensure compliance
with this section.

Aetna will notify retained litigation counsel when additional agreements are required under federal
and/or state laws governing the confidentiality of certain types of sensitive health information, such as
health plan members’ HIV and behavioral health status and substance use disorder information.

2. De-identified Member Information

As a general matter, it is Aetna’s policy to limit, whenever possible, the use and/or disclosure of health
information in all litigation to only de-identified member information. Aetna and/or retained litigation
counsel must take all reasonable steps to avoid the use and disclosure of PHI in litigation matters.

Health information is “individually identifiable” if it includes any of the 18 types of identifiers for an
individual or for the individual’s employer or family member, or if the provider or researcher is aware
that the information could be used, either alone or in combination with other information, to identify an
individual. These identifiers include, among others, name, address (all geographic subdivisions smaller
than state, including street address, city, county, or ZIP code), all elements (except years) of dates
related to an individual (including birth date, admission date, discharge date, date of death, and exact
age if over 89), telephone or fax numbers, medical record or health plan beneficiary numbers, license
plate numbers, email address, Social Security number, certificate/license number, and any other unique
identifying number, characteristic, or code. 45 C.F.R. 160.103.
3. **Minimum Necessary Standard**

If PHI is required to be used or disclosed in litigation, it is Aetna’s policy to limit the use or disclosure of PHI to the minimum necessary to accomplish the intended purpose of the use or disclosure (the “Minimum Necessary Standard”). Thus, if PHI is required to be used or disclosed in litigation, Aetna and/or retained litigation counsel must take all reasonable steps to limit the use and disclosure of PHI in litigation to the Minimum Necessary Standard prior to its use or disclosure.

This practice applies regardless whether Aetna is using PHI in litigation for its own purposes or is responding to a subpoena, document request or other lawful process. This Best Practices Policy does not, however, require Aetna to move to quash or limit any discovery request or subpoena that calls for the production of PHI.

4. **Best Practices Regarding Aetna’s Use / Disclosure of PHI in Litigation**

In general, Aetna may use or disclose PHI for treatment, payment, or health care operations. “Health care operations” includes conducting or arranging for legal services. Thus, Aetna may use or disclose PHI in connection with litigation, subject to the limitations set forth herein.

a. **Use of Business Associates By Aetna to Assist It in Litigation**

Aetna is entitled to use BAs to assist it in litigation. As noted above, retained litigation counsel is a BA and is required to execute a BAA prior to starting work. Retained litigation counsel may also hire other counsel (e.g., local counsel), subcontractors and/or vendors to assist it in litigation. If those subcontractors or vendors will have access to PHI, they must also sign a BAA directly with Aetna, or sign a sub-BAA with retained litigation counsel, prior to starting work. It is Aetna’s practice for Aetna-retained experts and consultants, as well as Aetna-retained litigation support vendors (including, for example, court reporters, mail vendors, claims or settlement administrators, copy services and the like) to execute a BAA (if retained directly by Aetna) or a sub-BAA (if retained by litigation counsel), before PHI is disclosed to them by Aetna or litigation counsel.

If Aetna or an Aetna BA retains a litigation support vendor (including a claims or settlement administrator) to communicate directly to Aetna members, Aetna or an Aetna BA must obtain a BAA or sub-BA with the Aetna-retained vendor and comply with the provisions of Sections 5-11 of the Best Practices Policy below. Aetna shall also require the entry of a QPO for disclosure of PHI to any Aetna-retained vendor.
If, however, Aetna is ordered by a Court to provide PHI to a litigation support vendor (including a claims or settlement administrator), either directly or through a third party, Aetna is not required to obtain a BAA with that vendor, but is required to disclose only the PHI expressly authorized by the Court in the manner the Court so orders, and shall request entry of a QPO or other appropriate order to govern the transmission of the PHI.

An Aetna-approved form BAA and an Aetna-approved sub-BAA are attached to the Guide.

Aetna will establish a SharePoint with a list of Aetna-approved expert and consulting firms and litigation support vendors with which Aetna has already entered into a BAA. Aetna and/or retained litigation counsel shall ensure that any experts, consultants or litigation support vendors it intends to use in litigation has signed a BAA or sub-BAA prior to the disclosure of PHI to them.

In addition, it is Aetna’s policy to require Aetna-retained experts, consultants and litigation support vendors to also sign an affidavit or declaration agreeing to the terms of the QPO (see below) that has been entered in the litigation prior to starting work. This requirement is not in lieu of obtaining a BAA, but is in addition to obtaining a BAA, with Aetna-retained experts, consultants and litigation support vendors.

Any disclosure of PHI to experts, consultants or litigation support vendors should be memorialized and monitored by Aetna and retained litigation counsel pursuant to the chain of custody requirements discussed below in Section 8 below.

Further, in cases involving specific classes of PHI, including information relating to a health plan member’s HIV status or behavioral health or substance use, Aetna and retained litigation counsel must assess all applicable federal and state-specific laws and regulations addressing those specific classes of PHI to ensure compliance with those laws and regulations before using or disclosing such PHI to Aetna-retained experts, consultants or litigation support vendors (including claims and settlement administrators).

b. **Minimum Necessary Standard**

The Minimum Necessary Standard described above applies to all uses and disclosures of PHI by Aetna or its business associates in litigation.

c. **Use / Disclosure of PHI By Aetna in Court Proceedings**

It is Aetna’s policy not to file PHI with any court unless reasonably necessary. If necessary to file, Aetna and/or retained litigation counsel must take all reasonable steps to protect against the public disclosure of PHI through redacting PHI from public filings and/or filing documents that contain PHI under seal or in camera, in compliance with court rules. Aetna and/or retained litigation counsel shall work with courts to protect the public disclosure of PHI in trials or other proceedings. In cases involving specific classes of PHI, including information relating to a health plan member’s HIV status or behavioral health or
substance use, Aetna and/or retained litigation counsel must assess all applicable federal and state-specific laws and regulations addressing those specific classes of PHI to ensure compliance with those laws and regulations, and may be required to take additional steps to protect against the public disclosure of PHI.

5. **Best Practices Regarding Disclosure of PHI to Opposing Party or Requesting Third Party**

Aetna may not produce PHI to an opposing party or a requesting third party, except as set forth below.

a. **HIPAA Authorization**

In any litigation or settlement, or pre-litigation matter involving an individual member (or individual members), if requested by the member’s attorney (or other designated representative), Aetna and/or outside litigation counsel may disclose member PHI to them if the member(s) have signed a HIPAA Authorization permitting the disclosure pursuant to HIPAA Rules. A copy of Aetna’s standard HIPAA Authorization form is attached to the Guide.

In situations where specific classes of PHI, including information relating to a health plan members’ HIV status and behavioral health and substance use, could potentially be used or disclosed to a member’s counsel, Aetna and retained litigation counsel must assess applicable federal and state-specific laws to ensure that the authorization form complies with those laws prior to disclosing the member’s PHI to the member’s attorney or other third party.

This “best practice” applies regardless whether or not Aetna is a party to an action.

b. **Disclosures Pursuant to Lawful Process**

In addition, Aetna and retained litigation counsel may disclose PHI in the course of a judicial proceeding under the following circumstances only (42 C.F.R. 164.512(e)):

1. In response to an order of a court or administrative tribunal, provided that Aetna only discloses the PHI expressly authorized by the order, and if the order does not contain a QPO, Aetna shall request a QPO or other appropriate order;

2. In response to a subpoena, discovery request, or other lawful process propounded by an opposing party or requesting third party if: (i) Aetna receives satisfactory assurances that the party seeking the information has made reasonable efforts to ensure that the individual who is the subject of the PHI has been given notice of the request, or (ii) the party seeking the information has secured a QPO. Aetna and/or retained litigation counsel must make reasonable efforts to meet and confer with the requesting party to narrow the scope of the requested PHI to the Minimum Necessary Standard, consistent with Section 4(b) above.
Further, in cases involving specific classes of PHI, including information relating to health plan members' HIV status or behavioral health or substance use, Aetna and/or retained litigation counsel must assess relevant laws and regulations addressing those specific classes of PHI to ensure compliance with those laws and regulations prior to use or disclosure in litigation.

c. Entry of QPO

In any case in which PHI may be used or disclosed to an opposing party in litigation, it is Aetna’s policy to require the entry of a QPO at the earliest possible time in the litigation. Attached to the Guide is a form QPO that may be used in litigation, subject to court- or state-specific requirements.

In cases involving specific classes of PHI, including information relating to health plan members' HIV status or behavioral health or substance use, Aetna and/or retained litigation counsel must assess and, where applicable, modify the form QPO to ensure compliance with laws and regulations that address those specific classes of PHI.

In individual member litigation, a QPO is not required to produce member PHI to a member’s attorney (or designated representative), if that member executes a valid authorization form prior to disclosure. That said, it is Aetna’s policy to ensure that a QPO is entered in all cases in which PHI may be used or disclosed, prior to use or disclosure. In individual member cases, retained litigation counsel should consult with and obtain approval from Aetna prior to disclosing member PHI to a member’s attorney and must take reasonable steps to ensure that a QPO is entered at the earliest possible time. Aetna’s retained litigation counsel must memorialize efforts taken to ensure entry of a QPO in individual member cases. No PHI may be disclosed in individual member cases if Aetna has not obtained either a HIPAA Authorization or if a QPO is not in place.

6. Transmission of PHI in Litigation

The transmission of PHI to opposing counsel or to any third party consistent with the above must be done in a HIPAA-compliant manner, pursuant to 45 C.F.R. § 164.312.

Further, in cases involving specific classes of PHI, including information relating to health plan members' HIV status or behavioral health or substance use, Aetna and/or retained litigation counsel must assess relevant laws and regulations addressing those specific classes of PHI to ensure compliance with those laws and regulations prior to transmission of PHI in litigation.

7. Chain of Custody Documentation

Each disclosure of PHI must have a complete chain of custody documented in the case file. For example, Aetna must have a BAA between Aetna and retained litigation counsel before sending any PHI to the law firm, and any PHI disclosed to retained litigation counsel should be recorded in the case file.
In addition, before any PHI is disclosed to an Aetna-retained expert or consultant, Aetna and/or retained litigation counsel must have a BAA or sub-BAA with the expert or consultant. Further, before any PHI is disclosed to an Aetna-retained litigation support vendor, Aetna and/or retained litigation counsel must have a BAA or sub-BAA with the vendor. As noted above in Section 4, it is Aetna’s policy to require Aetna-retained experts, consultants and litigation support vendors to also execute an affidavit or declaration agreeing to comply with the terms of the QPO. It is Aetna’s policy to maintain a record of each disclosure of PHI by Aetna and retained litigation counsel to ensure compliance with this Best Practices Policy.

Further, before any PHI is disclosed to an opposing party by Aetna and/or retained litigation counsel, a QPO (and/or a signed HIPAA Authorization, in individual member cases) must be on file with Aetna prior to disclosure. Aetna’s form QPO prohibits opposing counsel from disclosing PHI to any third party unless and until the third party executes an affidavit or declaration agreeing to comply with the terms of the QPO. As noted above, retained litigation counsel should also attempt to obtain agreement from opposing counsel that any subsequent disclosures of PHI by opposing counsel to any third party require prior notification by opposing counsel to Aetna of the disclosure, including to whom the disclosure is being made and the purpose of the disclosure.

Aetna will engage in periodic audits of case files to ensure compliance with this section.

8. Communications with Members

In any matter in which a communication will be sent by Aetna or on Aetna’s behalf, retained litigation counsel and/or an Aetna-retained consultant or vendor to members who are not a named party to the lawsuit (e.g., putative class members or class members) and the communication includes any suggestion of a member’s health condition or treatment or otherwise contains any member PHI, the substance and form of the communication must first be approved in writing by both the Court and by Aetna’s Privacy Office, and any vendor to be used for the communication and any follow-up communications must be approved by Aetna in writing. It is a best practice in all communications with members (regardless of whether the member is a named party) to limit the inclusion of a member’s health condition or treatment or PHI to the minimum necessary.

9. Government Investigations

This Best Practices Policy also applies to government investigations, as appropriate under the circumstances. Aetna must receive adequate assurances from government agencies demanding PHI, prior to disclosure, that PHI will be subject to the highest degree of protection and will not be disclosed or transmitted to any third party without advance notice to Aetna and an opportunity to take action.

10. Return or Certification of Destruction of PHI

At the conclusion of each litigation matter, Aetna and/or retained litigation counsel must obtain the return, or a written certification of destruction, of PHI by opposing counsel and all third parties to whom
11. Mandatory Education and Training

Aetna shall implement initial and annual training of the best practices in handling PHI in litigation for Aetna’s litigation staff and retained litigation counsel on Aetna matters. Relevant litigation staff includes all personnel who may receive or transmit PHI, or who are responsible for the maintenance of records containing PHI, and may include non-lawyers.

12. No Admission or Waiver

Nothing in this Best Practices Policy shall be deemed an admission by Aetna of its legal requirements or a waiver of any of Aetna’s rights, remedies or defenses.

* * * * * * *

Any questions regarding this policy may be directed to Aetna’s Head of Litigation (“Head of Litigation;” currently, Ed Neugebauer).
Appendix
## ICLE BOARD

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Term Expires</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carol V. Clark</td>
<td>Member</td>
<td>2019</td>
</tr>
<tr>
<td>Harold T. Daniel, Jr.</td>
<td>Member</td>
<td>2019</td>
</tr>
<tr>
<td>Laverne Lewis Gaskins</td>
<td>Member</td>
<td>2021</td>
</tr>
<tr>
<td>Allegra J. Lawrence</td>
<td>Member</td>
<td>2019</td>
</tr>
<tr>
<td>C. James McCallar, Jr.</td>
<td>Member</td>
<td>2021</td>
</tr>
<tr>
<td>Jennifer Campbell Mock</td>
<td>Member</td>
<td>2020</td>
</tr>
<tr>
<td>Brian DeVoe Rogers</td>
<td>Member</td>
<td>2019</td>
</tr>
<tr>
<td>Kenneth L. Shigley</td>
<td>Member</td>
<td>2020</td>
</tr>
<tr>
<td>A. James Elliott</td>
<td>Emory University</td>
<td>2019</td>
</tr>
<tr>
<td>Buddy M. Mears</td>
<td>John Marshall</td>
<td>2019</td>
</tr>
<tr>
<td>Dean Daisy Hurst Floyd</td>
<td>Mercer University</td>
<td>2019</td>
</tr>
<tr>
<td>Cassady Vaughn Brewer</td>
<td>Georgia State University</td>
<td>2019</td>
</tr>
<tr>
<td>Carol Ellis Morgan</td>
<td>University of Georgia</td>
<td>2019</td>
</tr>
<tr>
<td>Hon. Harold David Melton</td>
<td>Liaison</td>
<td>2019</td>
</tr>
<tr>
<td>Jeffrey Reese Davis</td>
<td>Staff Liaison</td>
<td>2019</td>
</tr>
<tr>
<td>Tangela Sarita King</td>
<td>Staff Liaison</td>
<td>2019</td>
</tr>
</tbody>
</table>
GEORGIA MANDATORY CLE FACT SHEET

Every “active” attorney in Georgia must attend 12 “approved” CLE hours of instruction annually, with one of the CLE hours being in the area of legal ethics and one of the CLE hours being in the area of professionalism. Furthermore, any attorney who appears as sole or lead counsel in the Superior or State Courts of Georgia in any contested civil case or in the trial of a criminal case in 1990 or in any subsequent calendar year, must complete for such year a minimum of three hours of continuing legal education activity in the area of trial practice. These trial practice hours are included in, and not in addition to, the 12 hour requirement. ICLE is an “accredited” provider of “approved” CLE instruction.

Excess creditable CLE hours (i.e., over 12) earned in one CY may be carried over into the next succeeding CY. Excess ethics and professionalism credits may be carried over for two years. Excess trial practice hours may be carried over for one year.

A portion of your ICLE name tag is your ATTENDANCE CONFIRMATION which indicates the program name, date, amount paid, CLE hours (including ethics, professionalism and trial practice, if any) and should be retained for your personal CLE and tax records. DO NOT SEND THIS CARD TO THE COMMISSION!

ICLE will electronically transmit computerized CLE attendance records directly into the Official State Bar Membership computer records for recording on the attendee’s Bar record. Attendees at ICLE programs need do nothing more as their attendance will be recorded in their Bar record.

Should you need CLE credit in a state other than Georgia, please inquire as to the procedure at the registration desk. ICLE does not guarantee credit in any state other than Georgia.

If you have any questions concerning attendance credit at ICLE seminars, please call: 678-529-6688