Ethics and Risks of New Technologies in the Legal Profession

September 23, 2016
This page intentionally blank
Ethics and Risks of New Technologies in the Legal Profession
September 23, 2016

Agenda

8:30am – 9:00am Registration

9:00am – 9:50am Introduction to Law & Technology
Associate Dean Antony Haynes
Prof. Robert A. Heverly

9:50am – 10:00am Break

10:00am – 10:50am Law & Technology: Particular Legal Concerns
Prof. Robert A. Heverly

10:50am – 11:00am Break

11:00am – 12:15pm Social Media and Legal Ethics: Lawyers Online
Prof. Robert A. Heverly

12:15pm – 1:30pm Lunch

1:30pm – 2:45pm Technology and Security
Associate Dean Antony Haynes

2:45pm – 3:00pm Break

3:00pm – 3:50pm Risks and Legal Ethics of Technology and Legal Practice
Associate Dean Antony Haynes
This page intentionally blank
SPEAKER BIOGRAPHIES

DEAN ANTONY HAYNES joined Albany Law School in December 2015 as Associate Dean for Strategic Initiatives and Information Systems, Assistant Professor, and Executive Director of the Schaffer Law Library. He teaches a seminar on Cybersecurity Law and Policy designed to introduce students to the issues involved in cyber security law, both from a national policy standpoint and from a corporate counsel view. Dean Haynes has extensive litigation experience in the intellectual property, securities, and criminal defense areas. He served as Associate at the law firm Quinn Emanuel Urquhart & Sullivan, LLP, in Washington, D.C., and before that at Williams & Connolly LLP, in Washington, D.C. Prior to practicing law, Dean Haynes was an Assistant Professor of Computer Science at the U.S. Air Force Academy, where he taught courses in programming, developed the Academy’s Information Assurance curriculum, and created the intercollegiate Cyber Defense Exercise. He has extensive experience with a host of software and hardware technologies. After the Air Force Academy, he was an associate at Chatham Financial Corporation, Capital Markets, Kennett Square, PA, where he led a company-wide software effort, wrote financial software and coordinated technical developers. As CEO and President of Exaprime LLC – a company he founded in Chadds Ford, PA, to provide technology consulting to academic institutions – he developed an on-line survey-system for the University of Pennsylvania Center for Clinical Epidemiology and Biostatistics. Dean Haynes received a J.D., *cum laude*, from Georgetown University Law Center, where he was a Lane Fellow, a Legal Writing Fellow, and Best Oralist for the Cardozo Moot Court Competition. He received an M.S. in Computer Science from the University of Illinois at Urbana-Champaign, where his thesis focused on machine learning and expert systems. He is a distinguished graduate of the U.S. Air Force Academy, where he was recognized as the top computer science graduate. Dean Haynes is an entrepreneur who leverages his background in computer science, technology, business and the law to advise startup companies. In addition to advising startups, he has spent time acquiring and growing companies.

ROBERT A. HEVERLY is an Associate Professor of Law at Albany Law School of Union University. He has taught as a visiting professor at Michigan State University College of Law, taught in and directed a Masters in Law Program at the University of East Anglia’s Norwich Law School in the UK, has taught in Trier, Germany as a Guest Professor of the Common Law, and regularly teaches Internet Law as part of the George Washington University School of Law’s Munich Intellectual Property Summer Program. Professor Heverly earned his LL.M. from Yale Law School, after which he undertook a Resident Fellowship with the Information Society Project at Yale Law School, where he retains an affiliation as a Faculty Fellow. He received dual Bachelor of Arts degrees (Broadcasting & Mass Communications Studies and Psychology) from the State University of New York College at Oswego (with honors), and a Juris Doctor (with
honors) from Albany Law School of Union University. Prof. Heverly is currently the Chair of the Internet and Computer Law Section of the American Association of Law Schools. Professor Heverly's research interests include intellectual property, technology and society (especially the Internet, computers, networks, and information law), media law, property, and globalization. He regularly teaches continuing legal education courses on legal ethics and social media & online activity. He has taught Torts, Property Law, Art and Entertainment Law, Cyber/Internet Law, Copyright Law, International and Comparative Intellectual Property Law, and related courses. He has published articles and book chapters in the Berkeley Technology Law Journal, the Georgetown Journal of International Law, and MIT Press, among others, and recently spoke at the Drones and Aerial Robotics Conference (DARC) sponsored by NYU's Engleberg Center on Innovation Law and Policy.
Ethics and Risks of New Technologies in the Legal Profession

Morning Session Materials
Public Service Workshops Program
September 23, 2016

Robert A. Heverly
Associate Professor of Law
Albany Law School
rheve@albanylaw.edu
Phone: 518 445-2379
http://robert.heverly.org/
This page intentionally blank
D. Texas lawyer gets in trouble for asking for continuance for funeral then partying ........................... 25
E. Posting False Negative Review Earns Reprimand .............................................................................. 25
F. Responding to Negative Online Review with Confidential Information Earns Rejection of Mere Reprimand ........................................................................................................................................... 25
G. Posting Fake Dating Ad for College Acquaintance Yields Suspension ............................................. 26
H. Hiring a Secretary via Craigslist Is Fine; Asking for Sex as Part of the Job is not .......................... 26
I. Judges can get in trouble, too ............................................................................................................... 27
J. The Firm Online .................................................................................................................................. 28
K. Electronic Errors Are Bound to Happen ............................................................................................ 31
L. E-mail is not a Phone Call .................................................................................................................. 31
M. Encryption and Electronic Transactions ............................................................................................ 33
N. Being in Two Places at Once ............................................................................................................. 35
O. Being in One Place and not Another .................................................................................................. 35
P. Working Two Places at Once ............................................................................................................. 35
Q. More problems with E-mail ................................................................................................................ 36
R. Trying to Influence Public Perception by Posting Criminal Discovery Video Online ...................... 37
S. Westlaw Access Not Allowed After Leaving Position ........................................................................ 37
T. With Computers You Can Make Stuff Up (but shouldn’t) ................................................................ 37
U. What’s on the Web Can Be Found ...................................................................................................... 38
V. You Can’t Get Rid of What’s on Facebook, But You Can Try (Though Maybe You Shouldn’t) ........ 38
W. Friends, Following, and Linking-in: Connections in a Connected World ......................................... 39
The Internet, mobile telephony, and the apparently constant connectedness of business professionals and their clients and colleagues raise a variety of issues in the modern professional world. Of these, new technologies often raise many issues, often simply because we are unaware of the technology’s true impact on our lives and our practice. These materials will look at how connectedness in many of its forms implicates judicial, procedural, and ethical concerns.

I. Introduction to Law & Technology

The Internet is essentially a series of inter-connected computers. At each end of any particular connection established over the Internet are computers, and in between are all the networking elements that allow the Internet to function. Networking works by providing standardized ways to transmit information from one location to another, and involves a transmission medium (such as fiber optic cable) and routers that know where the information needs to go. The “under the hood” elements are not particularly important for us here, though some of the workings of the network itself are relevant to inquiries regarding things like cloud computing and E-mail usage, and where that is the case we will delve lightly into them.

In the opening days of the Internet there was a scholarly debate between Judge Frank Easterbrook and other scholars (most notably Larry Lessig) as to whether there should be a legal field known as “Cyberspace Law.” While the debate took turns not relevant to us here, one advantage of its having taken place is that it helped develop the analytical tools we need to ask whether the Internet changes anything when it comes to legal relations among people. In some cases, the Internet changes nothing. The doctrinal analysis we undertake is “the same” as it was before the Internet, and the Internet’s involvement in the scenario is at best a red herring, and at worst a fatal distraction. In other cases, the Internet does change something, either by amplifying the effects of actions that existed in the past, by changing how those actions are perceived, or by making new aspects of them salient to our legal analysis.

The Internet is sometimes called “The Big Equalizer;” it allows everyone who wants to publish to publish whatever they would like. A variety of ways to publish are available, and in each case they offer various advantages and disadvantages. Building your own Web site takes time, some design sense, and an ability to understand how other people will use your site. Websites are also often time-consuming to update manually. This has lead to a plethora of online options for people to not only publish entire websites, but also options to publish in more limited ways, or to more limited groups of people. These include blogging platforms such as Wordpress and Blogger (the latter now owned by Google) that allow you to publish rather quickly and without much knowledge of how the Web works. These sites are indexed by the
search engines and all the maintenance is done by the host site, streamlining the online presence problem.

Social networking sites play a different and larger role, but include publishing abilities within their structures. These sites, such as MySpace and Facebook, allow much more than publishing, but publishing – whether to the world or to a group of “friends” that can be upwards of 1,000 or more people – is a key ingredient to what the sites hope to accomplish. Add to these Twitter, a “micro-publishing” site that allows users to post short messages of up to 140 characters and in which people can “follow” and “be followed” by other Twitter users, and you have but a few of the ways in which content can be added by Internet users to the Web.

Each of these methods of online exchange contains pitfalls that must be considered by those who take them up. One woman lost her position in a teaching school because she posted a picture on Facebook of herself, holding a cup of what appeared to be beer. Her school kicked her out of the program and she lost her opportunity to finish the program and become a school teacher (she has rather infamously become known as the “drunk pirate” as that is what she captioned the image). Others have, for example, been “caught” cheating on disability claims, posting how active they have been while collecting disability benefits.

The potential pitfalls of both publishing online and of connecting online are multiplied by their interaction with the Rules of Professional Conduct. The complexity of the ethical analysis increases when we talk about using online resources in the practice of law itself (ie, as a component of practice, such as in seeking information about other parties, connecting with the judiciary, or soliciting business online), as opposed to more straightforwardly engaging in online speech.

A. The Technological Framework

In addition to the “regular” Internet uses with which most of us are familiar – sending E-mail and browsing the Web – recent years have brought us a host of new ways to interact and work over the Internet. These technologies and the ways they are implemented change over time. Learning today about MySpace.com, a web meeting place that was popular in the late 2000s, peaking in popularity from 2005 to 2008, may not be useful directly today, but the same kinds of issues raised by MySpace may arise again in the context of another technology. What is the current “fad” tends to get lots of attention, both in the popular press and in the courts. As the introductory discussion shows, however, the technology focused approach is often the wrong approach. A better approach involves learning about a technology, determining how it works, who uses it, and how it is used, and then making appropriate determinations based on the
elements of the analysis that become more or less important given the technological context in which the issue arose.

To spend significant time making rules for Facebook, or Google, or E-mail, or texts, is inefficient both in terms of resources and in terms of development of the common law. There may be times that one technology needs to be treated differently than another, but it will not be because one is called Facebook and another is called E-mail. It may be because the written content of an E-mail, when functioning properly, is largely under the control of the sender, while what appears on a person’s Facebook page is an amalgamation of the input of others, advertisements, and choices made by Facebook itself.

The steps to addressing any social media question are to: 1) Determine who plays what role in the content or process that is relevant to the case; and, 2) Determine how users actually use the system (that is, what do they do with the technology). With these two questions in hand, a court is well placed to decide whether and to what extent social media should be a focus in the decision or is rather a red herring, distracting the court and the attorneys from issues more directly relevant to the case. As an aid to understanding the basics of the technologies, the following short descriptions of some of the most prominent social media technologies in use today serve as an introduction to these social media technologies themselves.

B. Facebook

One of the most prominent social media networks, Facebook allows its members to post announcements, photographs, videos, links to other sites, and related materials. Facebook members can become “friends” with other Facebook members, at which point the members can interact more closely, for example, by reading what the other has posted or seeing details about the friend’s work, family or hometown. To become a friend, one member sends a friend request to another, and if the second member accepts the request, they are then “friends” for Facebook purposes. Facebook friends may be people the member knows in real life, such as family members, current or past classmates, colleagues, and others, but Facebook does not control “friending” and some people have thousands of friends on Facebook, essentially accepting all friend requests that come their way. Additionally, businesses and prominent or famous individuals may have business pages that members can “like” to receive posts from the liked page. Facebook obtains financial support for the site from targeted advertisements shown to the members, as well as from related commercial agreements. Users have some control over how much of their information is available to non-friends and to non-Facebook members (for example, through search engines).
C. LinkedIn

LinkedIn is often referred to as a professional or business person’s Facebook. LinkedIn encourages people to “connect” (the LinkedIn word for what is a “friend” on Facebook) only with people they know or have been introduced to, and the content on LinkedIn is decidedly more professional and serious. Unlike Facebook, LinkedIn offers a premium membership which provides greater access to other users’ information.

D. Twitter

Twitter is a “micro-blogging” platform. Users use Twitter to post links, short bursts of information, and images. Twitter’s “Tweets” are limited to 140 characters (including spaces). Users can “follow” another person’s Twitter feed, and then see the things that person is tweeting. Direct interaction among members is possible using direct messaging, but the majority of twitter users interact simply by directing messages at each other. Twitter is the main impetus behind “hash tags” – short lines of text following the “hash” symbol (#). A Twitter user can search for a hash tag to see what others are identifying as being related to that topic. Twitter feeds can be private, allowing only those approved by the Twitter user to see the tweets.

E. Google Plus (Google+)

Google+ is Google’s foray into the Facebook/LinkedIn style of social network. Users form “circles” and share information, posts and links. As with Facebook, users have some controls over who can see and access their information.

F. Other Sites and Technologies

There are a variety of other social media and sharing sites on the Internet. Instagram and Flickr are focused primarily on image sharing. Snapchat was designed as a way to send secure images that “self-destruct” shortly after they are viewed, and Delicio.us and Digg allow users to share web content with others. Pinterest allows users to share web content by “pinning” it to pages on the Pinterest site, and sites such as Reddit allow users to share links, jokes, images and more anonymously (Reddit has a culture of prohibiting “doxing” – or identifying users in real life).

In addition to these technologies, all of which allow some interaction among users (thus qualifying as social media), more Internet-based technologies exist, such as blogging platforms that allow for the posting of stories, links or images (and more), E-mail, and even “plain, old”
web pages. All of these may raise the same kinds of questions and concerns raised by social media. When we add in smartphone “apps” (short for applications that run either the Windows operating system, Android, or Apple’s iOS operating system), many of which exist for the social media networks described above, the issues can expand quite quickly. In any case, however, be clear as to which technology is at issue, and in what way, and determination of the who and the how from our questions above becomes easier.

III. Law & the Internet: Particular Legal Concerns

A. Introduction

When we think through whether the Internet matters when we are asked to answer legal questions, one place to start is to ask whether there are “Internet specific” statutes relevant to the question raised. If there are, we know that – at least from a statutory standpoint – the Internet matters. In this section we will address questions that are likely to arise in generalized legal practice, that is, in practices that are not focused on technology, communications or the Internet. Within this area we will look at two examples where there are specific federal statutes on point, and at another area where the Internet has asserted it importance in practice.


One area of Cyberspace Law that any general practitioner might run into involves the potential liability of online hosts (and other service providers) for civil wrongs carried out by service users. If a Facebook user posts a defamatory statement on his or her wall, is Facebook liable for “publishing” the post, at the time it is posted, after Facebook gains knowledge of it, or after Facebook is informed it is defamatory?

Two early cases dealt with a similar issue and reached different results on slightly different facts. In the first, the Southern District of New York held that online service providers were distributors, not speakers, for defamation law purposes, analogizing an online service provider to a newspaper stand rather than a publisher or republisher of a statement.¹ As distributors are only liable for defamation if they have the requisite knowledge – that they knew or should have

known – of the defamation – the court thus held that the defendant was a distributor and not liable for the complained defamation.

In a subsequent case, a New York State court held that an online service provider could be liable as a speaker, specifically as a republisher, if it did more than simply distribute the defamation.\(^2\) In the second case, the online service provider used volunteer moderators to remove or edit posts that were objectionable (selling itself as “family friendly” due in part to this feature). Given the apparent incongruity in granting distributor status to service providers who take no action to counter the edginess of Internet communications, while imposing a more onerous burden on those who made that ostensibly worthwhile effort, Congress enacted (as part of the Communications Decency Act) 47 U.S.C. §230, limiting liability for providers for content provided by others. The statute provides, in part, as follows:

(c) Protection for “Good Samaritan” blocking and screening of offensive material

(1) Treatment of publisher or speaker
No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability
No provider or user of an interactive computer service shall be held liable on account of—
(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

While set out in terms of providing protection for service providers who block or screen offensive material, that language is not operative in the statute, and the courts have dismissed it. That is, the statute instead precludes treating online service providers as publishers in all circumstances where the defamatory content is or was provided by another. This interpretation has significantly expanded the scope of the provision and subjected it to significant criticism. For example, even where a service provider was made aware of defamatory material that was causing current harm and promised to take action to remove the material but failed to do so, §230 immunized the service provider from liability for content provided by another.\(^3\)

Subsequent cases applied the bar against liability to an online service provider that paid for content from a third party (holding the service provider immune from liability for content


\(^3\) Zeran v. America Online, Inc., 129 F. 3d 327 (4th Cir., 1997).
provided by the paid provider), as well as an allegation that an online service provider failed to maintain a safe online environment for its users (the court instead holding that the claim sought to hold the provider liable for the speech two users engage in while using the site). One exception seemed to be found where a provider required a user to provide content that was illegal (in this case a violation of the Fair Housing Act) as a condition of posting on the site. There a court found the provider to be engaged in joint provision of the content, and thus potentially liable. The result, however, was thrown into uncertainty by a later holding of the same court that held that the underlying activity that formed the basis for the earlier holding was in fact not illegal.

The lesson to take away in this area of law is that when “bad things” happen online, often the primary perpetrator is either anonymous/hidden or judgment proof. In these cases, it is tempting to go after the online service provider. But as Zeran and its progeny teach us, even where an online service provider has been given notice of content that in some way injures the legal rights of a client (outside of the intellectual property area, which we will discuss next), the provider will not be liable for the damages caused by the content.

Lawyers sometimes meet word of this near absolute ban on service provider liability with a sense of incredulity: how can it be that an online service provider that has knowledge of damaging content can ignore that content and not be held liable? The answer is one of the standards of the legal lexicon: because the courts have said so. 47 U.S.C. §230 is thus a bar to many types of actions that might be brought outside of the Internet context, and ignoring it means risking dismissal of the case on motion early on in the proceedings. Note that this provision is relevant to any size business that allows third party generated content – which includes user comments and ratings – on its site. As such, it may serve you well when defending businesses with an online presence from civil liability.

---


6 Fair Housing Council of San Fernando Valley v. Roommate.com, LLC, 521 F.3d 1157 (9th Cir. 2008).

7 Fair Housing Council of San Fernando Valley v. Roommate.com, LLC, 666 F.3d 1216 (9th Cir. 2012).
C. The Internet and User Content—Part II: 17 U.S.C. §512

In addition to the bar provided by 47 U.S.C. §230, a second federal statute provides a safe harbor for website owners and operators whose sites contain content provided by third parties (section 230 does not apply to Intellectual Property⁸). While some provisions of this statute are more relevant to those engaged more deeply in Cyberspace Law issues, the safe harbor provides immunity to copyright infringement claims to all online service providers under the defined circumstances. Because the provisions ostensibly protect all kinds of businesses, it is worthwhile to ensure that clients that have an online presence take the minimal steps necessary to gain the protection of the statute. Where a business or site is engaged in the “user generated content” business, further study of 17 U.S.C. §512 is required.

Subdivision (c) of 17 U.S.C. provides as follows:

(c) Information Residing on Systems or Networks at Direction of Users.—

(1) In general. — A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider -

(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

(2) Designated agent. — The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:

(A) the name, address, phone number, and electronic mail address of the agent.

(B) other contact information which the Register of Copyrights may deem appropriate.

The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, and may require payment of a fee by service providers to cover the costs of maintaining the directory.

Unlike 47 U.S.C. §230, 17 U.S.C. §512 does not automatically apply to online service providers. Instead, the provider must follow the process set out both to obtain protection and to keep it. Registering an agent for copyright purposes and responding to notice and takedown requests are essential elements of §512’s structure. While there is more here, and while details of

what constitutes notice remain in flux, the basic requirement of registering and having appropriate policies in place is a simple step that every business with an online presence can take to minimize potential liability from the actions of third parties who can post content to a website.

D. Jurisdiction and the Internet

The final area to touch on that may confront non-technology practitioners is that old law school standby, personal jurisdiction. One of the early trends in Cyberspace Law cases was to treat the Internet as “different” and to fashion tests that focused on elements of online interaction that seemed unique in comparison to offline transactions. In Zippo Manufacturing Co.,⁹ the court fashioned a “sliding scale” by which jurisdictional claims could be measured. According to the Court:

[T]he likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. This sliding scale is consistent with well developed personal jurisdiction principles. At one end of the spectrum are situations where a defendant clearly does business over the Internet. If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the Internet, personal jurisdiction if proper. At the opposite end are situations where a defendant has simply posted information on an Internet Web site which is accessible to users in foreign jurisdictions. A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise personal jurisdiction. The middle ground is occupied by interactive Web sites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site. (citations omitted)

While the sliding scale has some appeal, more recent cases have placed it, if using it all, in the context of the overall test for personal jurisdiction (that is, the well-known International Shoe test requiring minimum contacts, a claim arising out of those contacts, and reasonableness in the exercise of jurisdiction). Zippo can be read as establishing an independent test for jurisdiction, but it can also be read as applying primarily to the minimum contacts element of

the test, and this is how it has been applied in recent cases.\textsuperscript{10} That is, it can inform the “minimum contacts” inquiry, but does not determine it. Thus, a “standard” jurisdiction inquiry should be performed in Internet involved cases, with the caveat that the sliding scale may prove useful in cases with facts tied up in Internet transactions.

\textit{E. Access to Electronic Communications}

Federal law, in a complicated and confusing patchwork quilt of laws, protects both the transmission and storage of electronic communications. Prof. James Grimmelmann describes it as follows:

\begin{quote}
A variety of federal and state statutes also regulate the use and disclosure of information stored in computers or transmitted on networks. This section examines the two principal federal statutes on point: the Stored Communications Act (the SCA, codified at 18 U.S.C. §§ 2701–2712) and the Wiretap Act (codified at 18 U.S.C. §§ 2510–2522). The SCA is also commonly referred to by its other name, Title II of the Electronic Communications Privacy Act, or ECPA. These statutes have two interlocking roles:

- To protect individuals from having their private communications seen by other private parties.
- To regulate the process by which the government acquires private communications during investigations.

Unfortunately for statutory clarity, these two roles are utterly intermingled in the SCA and Wiretap Act. They both take the form of a general prohibition on unauthorized access, together with exceptions for private and governmental access under certain circumstances.

Figuring out what law applies to a given situation is often a matter of extensive back-and-forth cross-referencing. [When considering the statutes], keep in mind the private/governmental distinction and, also, whether the communications are being intercepted while in transit (“prospectively”), or retrieved after the fact (“retrospectively”).\textsuperscript{11}

We must add to this uncertainty restrictions on access to electronic communications under the Fourth Amendment to the Constitution (and perhaps the Fifth, as well). Unfortunately, a full review of these statutes and requirements would require materials (and a lecture) of their own. We must make due instead with the understanding that these concerns are relevant to court orders related to electronic evidence, and we must consider them thoroughly when making such orders. By way of example, one of the best known cases in this area is Romano v. Steelcase,

\begin{footnotes}
\end{footnotes}
In Romano, the Court granted a party’s request to an opposing party’s Facebook pages and accounts (both current and deleted), noting that a Facebook member does not have a privacy interest that would preclude such access given Facebook’s terms of service and warnings, which make clear that information posted to Facebook may not be private even when a user chooses private settings. The federal statutory prohibitions on Internet service providers disclosing information by requiring the party to consent to the disclosure and provide the information.

F. Crypto-Currencies

Cryptographic currencies are “virtual currencies” that owners trade to others for goods and services (and for real-world currencies). Bitcoin is the best known of these, but others exist, as well, such as Dogecoin. They are called crypto-currencies because their existence is based on cryptographic strategies. As explain by Professor Grimmelmann:

NOTE ON BITCOIN

Bitcoin is simpler than it sounds. It is a “cryptocurrency” not because it is mysterious but because it is based on cryptography. To see how, let us consider what jobs a financial record-keeping system needs to do, and then see how Bitcoin does them. The most intuitive way of talking about money is as a tangible thing: dollars are pieces of paper that you hold in your hand. On this view, the numbers in a bank account balance also represent a thing: the number of dollars “in” the account. So a bank, or an online substitute for one, needs to keep track of who has which things.

But another way of thinking about money is in terms of verbs, rather than nouns. What matters are the transactions in which it passes from hand to hand. When you deposit a $50 birthday check from your aunt in your bank account, that’s a transaction in which your aunt gives you $50. You are now capable of engaging in transactions in which you give away up to $50. So you could write a $50 check to your aunt, or a $25 check to your dentist and a $25 check to your cousin. With credit cards and online payment systems like Paypal, the transactions are electronic rather than paper, but the idea is the same: keep track of who pays how much to whom and when.

In this example, the bank maintains a ledger of transactions involving your account.

12 Romano v. Steelcase, 30 Misc. 3d 426 (Sup. Ct. Suffolk County 2010)
Your aunt’s bank maintains a ledger of transactions involving her account. When you deposit her check, the two banks consult with each other, and then very carefully adjust both of their ledgers. Bitcoin is exactly the same, with three differences:

- The Bitcoin ledger, called the blockchain, keeps track of transactions involving everyone’s Bitcoin accounts.
- Instead of being maintained by a centralized authority, the blockchain is maintained collectively, by everyone who uses Bitcoin.
- The blockchain is secured using public-key cryptography.

First, start with the blockchain. Suppose that Alice sends Bob two Bitcoins. (Perhaps he mowed her lawn, or perhaps he gave her some U.S. dollars in exchange.) Abstractive slightly from the technical details, this transaction could be represented as:

```
From: Alice                      To: Bob          Amount: 2.000
BTC
```

Alice makes the transfer to Bob by appending this new transaction to the blockchain. Suppose that just before she does, the blockchain (ordered with the most recent transaction at the top) read:

```
From: Carol                      To: Alice      Amount: 200.000 BTC
From: Sujit                      To: Rajiv      Amount: .500 BTC
From: Dave                       To: Alice      Amount: 7.250 BTC
From: Carol                      To: Alice      Amount: 5.250 BTC
[millions of previous transactions]
```

After Alice adds her transaction to Bob, the blockchain now reads:

```
From: Alice                      To: Bob          Amount: 2.000 BTC
From: Carol                      To: Alice      Amount: 200.000 BTC
From: Sujit                      To: Rajiv      Amount: .500 BTC
From: Dave                       To: Alice      Amount: 7.250 BTC
From: Carol                      To: Alice      Amount: 5.250 BTC
[millions of previous transactions]
```

What keeps Alice honest? It is only possible for Alice to make a transaction giving Bob Bitcoins if there are previous transactions giving Alice enough Bitcoins. Just as a bank will bounce a check drawn against an account without sufficient funds, other Bitcoin users will reject the transaction unless there are previous transactions already in the blockchain supplying the necessary Bitcoins.* But if Alice has the Bitcoins to spend, other Bitcoin users will agree to add the transaction to the

This checking process is substantially easier because each Bitcoin transaction explicitly
identifies the previous transaction or transactions providing the necessary funds. When Bob sees that the blockchain has been extended to include Alice’s payment to him, he knows that the payment has succeeded. Second, the blockchain is publicly maintained. The blockchain is just a large and growing file that lists every Bitcoin transaction ever since the start of time. Instead of a bank storing the file on its servers (with appropriate backups), many different Bitcoin users keep a copy of the blockchain. Every time a new “block” of transactions is added to the chain (hence the name), the user adding the block broadcasts it to other users, who add the new transactions to their own copy of the blockchain. It is this collective process of agreement on which transactions have taken place that most distinguishes Bitcoin from traditional payment systems. Bitcoin relies on a peer-to-peer process of consensus rather than on one authority with the power to say which transactions are valid and which are not. Anyone who wants to take part, or to check up on past Bitcoin transactions, can obtain a copy of the blockchain and examine it. In theory, at least, this makes Bitcoin less vulnerable to arbitrary exercises of power: no single person or government can arbitrarily create new Bitcoins or take them away from their owners. Third, add security into the mix. Bitcoin uses digital signatures to guard against all of the obvious attacks, and a great many subtle ones as well. Every Bitcoin address (the source or destination of a transaction) has its own private-key/public-key pair. The “From: Alice” part of the transaction is a digital signature generated using the private key for Alice’s address. If the signature matches, anyone examining the transaction can confirm that Alice authorized it; if the signature doesn’t match, the transaction will be rejected. Thus, while it is easy to receive Bitcoins, only someone controlling the appropriate private key can spend them. (This also means that if you lose the private key for a Bitcoin address, the Bitcoins are gone forever; no one can spend them.) Now we are ready to answer two questions hanging over the system: Where do Bitcoins come from? and Why do Bitcoin users cooperate in maintaining the blockchain? The answer is that there are rewards for participating. A new block of transactions is added to the blockchain roughly every ten minutes: the user who first adds it receives a reward of 25 Bitcoins.* Which user that is is chosen essentially at random through a digital version of a scratch-off lottery in which there is an immense supply of free tickets and scratching one off takes a little bit of work.
and time. Since whoever scratches off a winning number first wins, Bitcoin users have an incentive to devote their computers’ time to “mining” Bitcoins, as the process is called. Each time someone proves that they have won the lottery by exhibiting the winning number for a block of transactions, everyone adds that block to the blockchain. As of 2014, the number will gradually decrease over time, and be replaced by transaction fees offered by the Alices of the world as an incentive to process their transactions.\(^{13}\) and immediately starts scratching off tickets in the next lottery for the next block. This scheme cleverly harnesses Bitcoin users’ greed to get them to participate in keeping the system working.

Bitcoin is interesting for many regulatory reasons [and] raises some interesting questions about anonymity. On the one hand, Bitcoin transactions are not identified with users’ names, only with inscrutably opaque Bitcoin addresses like 16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM, so it can be hard to tell who is behind Bitcoin transactions. On the other hand, the blockchain is public, so anyone can scrutinize its history. It is easy to follow Bitcoins from one address to another, unlike cash, which can circulate in near-total secrecy.\(^ {14}\)

There are currently no regulatory restrictions on using Bitcoin or other crypto-currencies for buying and selling goods and services. Those who act to trade the currencies for real-world currencies, or who assist in the transfer or storage of Bitcoin, however, are likely to be viewed as financial institutions and as such be subject to rules regarding money laundering and related requirements.\(^ {15}\)

\(^{13}\) To be a little more precise, Bitcoin miners are computing hash values. The winner is the one who finds a 32-bit number with a hash that is sufficiently close to zero. Since the hash function used by Bitcoin (SHA-256) produces outputs that are all but indistinguishable from random, there is no way to speed up the process other than to try one 32-bit number after another. The Bitcoin protocol automatically calibrates the difficulty of the hashing problem – i.e., the number of winning tickets in the lottery, or how close is “sufficiently close” to zero – so that someone will find a matching hash and add a block roughly every ten minutes. There is no way to save up winning numbers from one block to the next, since the details of the hashing depend on the transactions in the block.


G. Trademarks and Domain Names

Domain names, also known as URLs (universal resource locators) or web page names, are the things we type in to a web browser to “go to” a web page. Where the domain name is the same as or confusingly similar to a trademarked name (of a business, product or service), issues may arise as to its continued use. In short, there are a variety of methods of working out rights to domain names that touch on trademark law. Federal law provides that where a domain name has been registered in bad faith in an attempt to take advantage of another’s trademark, the mark is to be transferred to the trademark owner.\(^\text{16}\) In addition, the organization that oversees domain name issues at the international level, known as the Internet Corporation for Assigned Names and Numbers (ICANN), has a mandatory arbitration procedure in place for disputes concerning domain name conflicts. The procedure, entitled “The Uniform Domain Name Dispute Resolution Policy,” or the UDRP.\(^\text{17}\) ICANN requires that all domain registrars – the entities that sell domain names – require agreement to arbitrate as part of the sales process. As such, nearly every Internet website is bound to ICANN’s process for resolving domain name disputes.

The process itself involves the complainant submitting a request for arbitration of the dispute, followed by a response from the domain name owner. An arbitrator (or arbitrators) are appointed, and each side makes its case. If the arbitrator decides in favor of the complainant, the registrar is instructed to transfer the domain name to the complainant, who can then use it, stop its use, or otherwise control it. If the arbitrator finds in favor of the current website owner, then no transfer occurs.

The ICANN procedure does not preclude lawsuits based on trademark law, but such suits – which sound in a “likelihood of confusion” based on the website name, are more time consuming and expensive. A trademark holder is always permitted, however, to bring a lawsuit under relevant law in the state or country in which they operate, even if it is more expensive and time consuming.

H. International Law: The Right to Forget as an Example

The Internet is a global technology and oftentimes the decisions reached concerning Internet issues in one country affect how the Internet functions in another. In many cases, the


\(^\text{17}\) https://www.icann.org/resources/pages/help/dnrd/udrp-en.
rest of the world has fought against U.S. control over the Internet’s tendency to reflect U.S. norms and values, such as free speech. In 2014, the Court of Justice of the European Union ruled that Google had to recognize and respect the right of European citizens to “be forgotten.” Referred to as the “right to be forgotten,” Google was required to accept notices from individuals who wanted their data removed from Google searches. Information that could be removed included information that was inaccurate, inadequate, irrelevant, or excessive, though this right is balanced against rights of free speech and the press. Subsequently a French court has held that Google must remove the offending information worldwide, not just in a way that prevents Europeans from viewing it.

The Google case shows that while the Internet spans jurisdictional borders, it is also subject to the rules of the states in which it exists, and these rules may affect how the Internet works or “looks” for those outside of those borders, as well.

1. Computers, the Internet, and the Courts

Judges are called upon more and more to make decisions about discovery and admissibility of evidence from Internet and other communications sources. Many of these decisions so far have been based on a particular technology, such as E-mail, social networks such as Facebook, twitter, or even text messages via cell phones. The issues, however, are likely to be similar across the various technologies. In addition, even where we talk about a particular technology, the issues will change based on how and what within that technology we are talking about. For example, making the bare claim that “service of process via E-mail is appropriate” misses the point. Some technologies may raise one issue more strongly, while another may raise other issues, but on the whole the framework of analysis should be – and is – likely to remain consistent across technologies. This means that as we proceed, a decision regarding admissibility of E-mail may provide strong arguments as to why (or why not) a “tweet” might be admissible in a later case, but may not be particularly helpful when it comes to discussing a later case involving E-mail. Each inquiry should focus on what is being sought or offered and how it came into existence, but not the general type of technology being considered.

J. Social Media Evidence

1. A General Framework

In relation to evidentiary decisions, authentication and hearsay form the core doctrines for the issues that surround social media evidence in the courts and provide the framework within which individual requests should be considered. In considering how to authenticate or treat social media content for hearsay purposes, it is again best not to focus too closely on the name or type of the social media in question. It is unlikely to matter, for authentication purposes, for example, whether a post offered as the defendant’s was posted on Facebook or on Twitter or, for that matter, was sent by E-mail. It must still be shown to have its origin with the defendant. If it is offered for its content, and that content originated with a declarant, it must meet the requirements of hearsay doctrine. Content offered from automated systems that relates to the operation of those systems lacks a declarant, however, and thus is subject only to authentication, not hearsay, analysis. The key is to pay attention to who took the actions relevant to the information sought, not the name or type of technology they used to do so.

2. Authentication Issues

Authentication requires that evidence be shown to be what it is represented to be. Authentication may relate to the content of the message, or it may relate to the operation of the system that generated the content. If referring, for example, to a delivery report for a Facebook message, it is the operation of the Facebook messaging system that is in question. If referring to information found in a post or message sent via Facebook’s services, then it is the content of the message that is in question. The two types of authentication raise separate questions.

For example, when allowing into evidence a printout of a page from a Russian social networking website that was referred to as the Russian Facebook, the Federal District Court was held on appeal to have erred. This was not because the page was a social media site, or even that it was a Russian site, but rather because the prosecutors in the case failed to fully authenticate the website represented in the printout as belonging to the defendant.¹⁹ The case provides a template for dealing with authentication issues of this type. Beginning with authentication in general:

For instance, we have said that a document can be authenticated by “distinctive characteristics of the document itself, such as its [a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with the circumstances.” Maldonado–Rivera, 922 F.2d at 957

¹⁹ United States v. Vayner, 769 F.3d 125 (2d Cir. 2014).
(alteration in original) (quoting Fed.R.Evid. 901(b)(4) (pre–2011 amendments)); see also Sliker, 751 F.2d at 488 (contents of alleged bank records, in conjunction with their seizure at purported bank office, provided sufficient proof of their connection to allegedly sham bank). Or, where the evidence in question is a recorded call, we have said that “[w]hile a mere assertion of identity by a person talking on the telephone is not in itself sufficient to authenticate that person’s identity, some additional evidence, which need not fall into any set pattern, may provide the necessary foundation.” Dhinsa, 243 F.3d at 658–59 (brackets and internal quotation marks omitted); see also Sliker, 751 F.2d at 499 (voice on tape recording was sufficiently authenticated as defendant’s based on comparison of taped voice with defendant’s trial testimony). And in a case where credit card receipts purportedly signed by the defendant would have tended to support his alibi defense, we ruled that the defendant’s copies had been sufficiently authenticated, despite some question as to when these copies had been signed, where the defendant offered testimony from store managers as to how the receipts were produced, testimony from the defendant’s wife (a joint holder of the credit card) that she had not made the purchases in question, and testimony from a handwriting expert that the defendant’s signature was genuine. United States v. Tin Yat Chin, 371 F.3d 31, 35–38 (2d Cir.2004)

In analyzing the admissibility of the website content, the court continued:

The government did not provide a sufficient basis on which to conclude that the proffered printout was what the government claimed it to be—Zhyltsou’s profile page—and there was thus insufficient evidence to authenticate the VK page and to permit its consideration by the jury.

In the district court, the government initially advanced the argument that it offered the evidence simply as a web page that existed on the Internet at the time of trial, not as evidence of Zhyltsou’s own statements. The prosecution first represented to the district court that it was presenting the VK page only as “what [Special Agent Cline] is observing today on the Internet, just today,” J.A. 26, conceded that “the agent does not know who created it,” and averred that Special Agent Cline would testify only that “he saw [the VK page] and this is what it says,” J.A. 30. Consistent with these representations, Special Agent Cline testified only that the page containing information related to Zhyltsou was presently accessible on the Internet and provided no extrinsic information showing that Zhyltsou was the page’s author or otherwise tying the page to Zhyltsou.

At other times, however, the government repeatedly made a contrary argument to both the trial court and the jury, and insisted that the page belonged to and was authored by Zhyltsou. Nor is this surprising. The VK profile page was helpful to the government’s case only if it belonged to Zhyltsou—if it was his profile page, created by him or someone acting on his behalf—and thus tended to establish that Zhyltsou used the moniker “Azmadeuz” on Skype and was likely also to have used it for the Gmail address from which the forged birth certificate was sent, just as Timku claimed. Moreover, the district court overruled Zhyltsou’s hearsay objection and admitted a printout of the profile page, which stated that “Zhiltsov’s” Skype username was “Azmadeuz,” because it found that the page was created by Zhyltsou, and the statement therefore constituted a party admission. See J.A. 23 (The Court: “This is a statement made by your client. This is his Facebook record.”); J.A. 29–30 (describing the government’s plan to establish that the Gmail address was Zhyltsou’s “by what [the court] regard[ed] to be perfectly legitimate admissible evidence of what it is, the assumption is quite clear that what appears on the Facebook page is information which was provided by” Zhyltsou); J.A. 32 (The Court: “It’s his Facebook page. The information on there, I think it’s fair to assume, is

20 Id. at 130-131.
information which was provided by him.”); see also Fed.R.Evid. 801(d)(2)(A) (defining an opposing party’s statement as non-hearsay).

As noted above, Rule 901 requires “evidence sufficient to support a finding that the item is what the proponent claims it is.” It is uncontested that information about Zhyltsou appeared on the VK page: his name, photograph, and some details about his life consistent with Timku’s testimony about him. But there was no evidence that Zhyltsou himself had created the page or was responsible for its contents. Had the government sought to introduce, for instance, a flyer found on the street that contained Zhyltsou’s Skype address and was purportedly written or authorized by him, the district court surely would have required some evidence that the flyer did, in fact, emanate from Zhyltsou. Otherwise, how could the statements in the flyer be attributed to him? Cf. Dhinsa, 243 F.3d at 658–59 (“[A] mere assertion of identity by a person talking on the telephone is not in itself sufficient to authenticate that person’s identity....”). And contrary to the government’s argument, the mere fact that a page with Zhyltsou’s name and photograph happened to exist on the Internet at the time of Special Agent Cline’s testimony does not permit a reasonable conclusion that this page was created by the defendant or on his behalf.

It is true that the contents or “distinctive characteristics” of a document can sometimes alone provide circumstantial evidence sufficient for authentication. Fed. R. Evid. 901(b)(4). For example, a writing may be authenticated by evidence “that the contents of the writing were not a matter of common knowledge.” Maldonado–Rivera, 922 F.2d at 957 (brackets and internal quotation marks omitted). Here, however, all the information contained on the VK page allegedly tying the page to Zhyltsou was also known by Timku and likely others, some of whom may have had reasons to create a profile page falsely attributed to the defendant. Other than the page itself, moreover, no evidence in the record suggested that Zhyltsou even had a VK profile page, much less that the page in question was that page. Nor was there any evidence that identity verification is necessary to create such a page with VK, which might also have helped render more than speculative the conclusion that the page in question belonged to Zhyltsou.

What occurred in Vayner was an attempt by the prosecution to introduce the social media page and attribute that page to the defendant. The prosecution did this not just by using his photograph and related personal information appearing on the page, but by trying to buttress this information with testimony of someone who knew the defendant and whose story matched with what appeared on the page. The Second Circuit rejected this approach, and most likely rightfully. While authenticating a document by its contents is at times acceptable, it takes more than just a consistency between the content and the person alleged to be responsible for it. Where the allegedly distinctive characteristics are not sufficiently distinctive, however, because for example others have knowledge sufficient to create the content, authentication fails and the evidence should not be admitted.

Alternative questions are raised when evidence results from the operation of a technological process. In these cases, the reliability of the process itself is at issue, and must be established by

---

21 Id. at 131-132.
someone with sufficient knowledge of the system so as to be able to testify as to its operation and dependability.

3. Hearsay

As with authentication, it is easy to quickly become focused on a specific technology when considering hearsay questions. A better path is to consider the how the statement came into being and what it is being offered to show. If it was the result of a technological process that occurred without direct human intervention, there is no declarant, and authentication is the primary barrier to admissibility. Where content is offered as allegedly originating with a declarant, hearsay considerations may come to the forefront. The hearsay considerations, however, are not substantially different from those raised with other kinds of evidence, and the relevant hearsay exceptions apply.

Not getting distracted by the technology will help when applying the hearsay exceptions, however. For example, not all E-mail sent from a work computer will qualify as a business record. Where sent for personal reasons, the business record exception is inapposite. This is true for the same reasons that would hold if an employee sent personal letters from work, even if the employee kept a file with the letters in his work filing cabinet, because it was not a record kept in the ordinary course of business.

4. Anonymity

Anonymous speech is constitutionally protected. The Constitutional protection extends to the Internet. The Internet, and social media in particular, provide significant opportunities for anonymous speech. Under what circumstances should a court order an anonymous – or a pseudonymous – speaker to be identified using the legal process? The Federal District Court for the District of Connecticut answered that question using the following balancing analysis:

1) Whether “the plaintiff has undertaken efforts to notify the anonymous posters that they are the subject of a subpoena and withheld action to afford the fictitiously named defendants a reasonable opportunity to file and serve opposition to the application;”

2) Whether the plaintiff has identified a cause of action arising from the online speech;


3) Whether the anonymous person had an expectation of privacy at the time of posting; and,
4) Whether the plaintiff has made an “adequate showing” as to the cause of action against the poster.\textsuperscript{24}

Using this analysis, a court can try to ensure that the Internet’s promise as a robust forum for discourse and deliberation does not unnecessarily restrict access to the courts for those who have suffered legal wrongs via the Internet.

\textit{K. Service of Legal Process via the Internet}

Due process permits service of process via alternative means so long as the means is “reasonably calculated, under all the circumstances, to apprise interested parties of the pendency of the action and afford them an opportunity to present their objections.”\textsuperscript{25} Various courts have permitted service of process via the Internet, including specific decisions permitting service by E-mail and through Facebook.\textsuperscript{26}

The issues that arise in these cases provide another good example of the point made at the start of these materials: sometimes the Internet matters, sometimes it does not. In determining whether to allow alternative service of process via some Internet based method, courts should generally ask two questions (after the appropriateness of alternative service is generally established by the moving party):

1) Do the defendants have the technological sophistication necessary to receive important documents in the manner requested? And,
2) Is the particular method chosen shown by the moving party to be a reliable one for reaching these particular defendants.

This second point should be further broken into two inquiries:

a) Does the address, identity, location or Internet facility unquestionably belong to the defendant? And,

\textsuperscript{24} \textit{Doe I v. Individuals}, Civil Action No. 3:07 CV 909 (CFD) (D. Ct. 2008).


b) Is it reasonable to believe that there are likely to be technological impediments to receipt of the process given the method chosen?

While courts confronted with this issue to date have often engaged in the inquiry spawned by questions 1 and 2 above, they have often not taken into account part b of the second part of the inquiry. Once the appropriateness of alternative methods of service are established, the courts ask whether the defendant is an Internet user of the type who is able to receive important communications via the Internet method in question. They may then ask whether the particular address or resource used belongs to the defendants, requiring plaintiffs to show that the address is “reliable,” but courts to date have not shown an awareness of the many ways in which E-mail and other online communications can become lost or waylaid. For example, an automated spam filter may prevent service from reaching a defendant, although it will appear as though the message was delivered to the relevant account. A simple misspelling of the address may also result in lost service, and because a significant online spam problem has caused mail servers not to notify the sender that the message was not delivered. In addition, there is no foolproof method to ensure delivery through delivery confirmation via Internet, even this method will not suffice to ensure delivery. In such cases, E-mail or social media service may be appropriate, but additional methods – such as publication – may be necessary to ensure the defendant’s due process rights are protected.

IV. Social Media and Legal Ethics: Lawyers Online

There are a variety of ways to publish online. One is simply to develop a Web page. This was the earliest of the ways in which people published online, but it required (and to a certain degree still requires) skills in web page coding (known as HTML, now in its fifth iteration), and it can be labor and time intensive. In place of developing a Web page or site, a variety of opportunities for easier online publishing exist, including blogging platforms such as Blogger and Typepad. A ready-made blogging platform allows the user to choose a design for their page, choose various elements of the page, and integrate them into the final blog – a blog being little more than a web page that allows for interactive publishing, including comments and links from other blogs that

27 Spam is the Internet name for unsolicited commercial advertisements which often arrive unrequested via E-mail.

28 http://www.blogger.com/

29 http://www.typepad.com/
In addition to blogging, lawyers may publish through social networking platforms such as Facebook, Google+, LinkedIn, and Twitter. These platforms enable publishing in different ways, oftentimes integrated with tools to connect the user to friends, acquaintances, and perhaps even strangers. Twitter, for example, requires posts to be short: no longer than 140 characters. Facebook allows users to “friend” each other and to control the extent to which their information and posts are shared with others, but a large part of the Facebook experience involves a user posting information as a “status update.” This information is then automatically placed into the user’s friend’s wall, where they can scroll their friends’ updates and see what they have been up to. LinkedIn uses a similar newsfeed model, though LinkedIn is more focused on professional information and less on personal updates.

With all of these (and even more) outlets for online expression, it is not surprising that lawyers have been crossing the line when it comes to information posted online.

A. Identifying clients online

Illinois Assistant Public Defender Kristine Peshek was suspended from the practice of law in the spring of 2010 for content she posted on her blog, which was entitled, “The Bardd Before the Bar—Irreverant Adventures in Life, Law, and Indigent Defense.” Her blog included stories of her defense activities, but she included clients in her posts, using either names or jail numbers that would have allowed them to be identified. She also admitted that one of her clients had lied to a court and she had not brought the lie to the Court’s attention. Finally, she referred to one judge as an a**hole, and another as “clueless.” She lost her job and was suspended from the practice of law for 60 days.

30 Legal or “Law Blogs” are sometimes referred to as Blawgs. For a thorough and up to date list, see, Blawg Directory, ABA Journal (with ability to search by category, region, and author type): http://www.abajournal.com/blawgs/

31 http://www.facebook.com/

32 http://plus.google.com/

33 http://www.linkedin.com/

34 http://www.twitter.com/

35 MySpace is another social networking site, but it is not often used by lawyers.
B. Florida lawyer disciplined for calling a judge names on a blog

Sean Conway was upset with Judge Cheryl Aleman for using procedural rules he thought deprived his clients of the right to a speedy trial. After filing complaints with the judicial watchdog agency without any observable results, he posted about his experiences on his blog.\(^{36}\) Included in his posting were the following quotations:

Recently, in an attempt to make defendants waive their rights to a speedy trial, Judge Cheryl Aleman has decided to set trials about 1-2 weeks after arraignment, hoping that defendants will move for a continuance, thereby waiving their right to a natural speedy trial.

Today, Oct. 30th, I along with several other attorneys, had to endure her ugly, condescending attitude . . . Every atty tried their best to bring reason to that c'troom, but, as anyone who has been in there knows, she is clearly unfit for her position and knows not what it means to be a neutral arbiter.

* * *

As my case was on recall for 2 hours, I watched this seemingly mentally ill judge condescend each previous attorney.

* * *

ME: "Judge (not your honor b/c there's nothing honorable about that malcontent) ... there seems to be a mistake in this case."

EVIL, UNFAIR WITCH ("hereinafter "EUW"): "and what is that?"

The Florida Bar found that Conway’s post violated five ethics rules. Included were alleged violations of Florida Rules 4-8.2(a) (“A lawyer shall not knowingly make a false statement of fact concerning the qualifications, conduct or integrity of a judge” – New York’s rule is the same, N.Y. R. Prof’l. Conduct 8.2(a)) and 4-8.4(d) (“A lawyer or law firm shall not . . . engage in conduct that is prejudicial to the administration of justice”). Conway initially defended himself on free speech grounds, but after the Florida Supreme Court rejected his argument, he eventually agreed to a public reprimand and a fine.

---

C. Admission Denied for Online Crime

Other online troubles can arise when people do things online that they may have never tried offline for fear of getting caught. In one case, a recent law school graduate waiting to take the bar exam was arrested for sexual solicitation of an underage girl online. He was unable to take the bar, but after completing a diversion program, the charges were dropped. He then applied to take the bar and was allowed, subsequently passing, but was then denied admission to practice. The Supreme Court of Louisiana stated:

“[I]t is ordered that the petition for admission to the bar of Louisiana filed by petitioner, Philip R. Pilie, be and hereby is denied. It is further ordered that no applications for admission shall be accepted from petitioner in the future.”37

D. Texas lawyer gets in trouble for asking for continuance for funeral then partying

In another case a Texas lawyer asked a judge for a continuance so that she could attend a funeral. She seemed to have forgotten, however, that she and the judge were “Facebook friends.” While she really was attending a funeral, she also posted many times about going to parties, drinking, and generally having a good time. When she returned, she asked the judge for another continuance, which the judge denied.

E. Posting False Negative Review Earns Reprimand

In a case in Minnesota, an attorney was publicly reprimanded (and paid costs) for “falsely posing as a former client of opposing counsel and posting a negative review about opposing counsel on a website.”38

F. Responding to Negative Online Review with Confidential Information Earns Rejection of Mere Reprimand

The Georgia Supreme Court rejected a voluntary reprimand for an attorney who disclosed client confidences online. The client posted negative reviews of the attorney online after


Heverly: Legal Practice and the Internet

dismissing her, and the attorney responded by disclosing details concerning the case. The Georgia Supreme Court noted that “a lawyer maintain confidentiality of information relating to the representation is a fundamental principle in the client-lawyer relationship” and rejected the reprimand as an appropriate sanction.\(^{39}\)

\(\text{G. Posting Fake Dating Ad for College Acquaintance Yields Suspension}\)

A New York attorney who created a fake lesbian dating profile for a woman he knew in college years before was suspended by the Appellate Division, Second Department. According to the Court, “respondent's conduct was highly inappropriate and adversely reflects on the legal profession.”\(^{40}\)

\(\text{H. Hiring a Secretary via Craigslist Is Fine; Asking for Sex as Part of the Job is not}\)

A Chicago attorney was suspended from practice after he ran this Craigslist Ad advertising a vacant secretarial position with his firm:

Loop law firm looking to hire an energetic woman for their open secretary/legal assistant position. Duties will include general secretarial work, some paralegal work and additional duties for two lawyers in the firm. No experience required, training will be provided. Generous annual salary and benefits will be provided, including medical, dental, life, disability, 401(k) etc. If interested, please send current resume and a few pictures along with a description of your physical features, including measurements. We look forward to meeting you.

This ad isn’t what led to the suspension, however. It was the follow-up E-mail that went to those who expressed an interest in the position:

[I]n addition to the legal work, you would be required to have sexual interaction with me and my partner, sometimes together sometimes separate. This part of the job would require sexy dressing and flirtatious interaction with me and my partner, as well as sexual interaction. You will have to be comfortable doing this with us.

\(^{39}\) In re Skinner, 292 Ga. 640, 740 S.E.2d 171 (2013)(note that the court was also clearly unhappy that details of the case, such as the actual items disclosed, were not part of the record in the case).

\(^{40}\) In re O’Hare, App. Div. 2\(^{nd}\) Dept. (July 11, 2013), http://www.nycourts.gov/reporter/3dseries/2013/2013_05320.htm
In addition, Chowhan indicated to applicants that they would have to “perform” during the interview, and initially denied that he had sent the E-mail (claiming he had been hacked).  

I. Judges can get in trouble, too

There are a number of judges who have run into problems with their online interactions in recent years. One is Ninth Circuit Chief Judge Alex Kozinski, known for his decisions in Cyberlaw cases. Judge Kozinski maintained a web page on a private server and on which he shared what he thought was humorous material, but which content was also at times risqué or sexually oriented. Unfortunately for the judge, who thought the web page was private, the webpage was publicly available. An external ethics investigation (conducted by the Judicial Conduct panel for the Third Circuit) called Kozinski’s actions “imprudent” but concluded without any further action following the judge’s acceptance of responsibility and corrective actions following disclosure of the site.

Chief Judge Cebull of the Montana Federal District Court also ran into trouble, but in a different way. Earlier this year he sent out an E-mail that contained a racist joke about President Obama’s mother (and, by implication, the president himself). After Judge Cebull sent the message, one of the recipients forwarded it on to the press, at which point the Judge was subjected to numerous public calls for his resignation. He then asked for an ethics investigation into his own behavior, but before the investigation concluded, the Judge retired from the Bench.

---

41 Lizzie Schiffman, Samir Chowhan, Illinois Attorney, Suspended Over Ad For Secretary Job With ‘Sexual Aspect’ [http://www.huffingtonpost.com/2011/12/02/samir-zia-chowhan-illinois_n_1127022.html]


45 Montana Judge to be investigated over anti-Obama e-mail, USA Today, April 6, 2012, http://www.usatoday.com/news/washington/story/2012-04-06/judge-racist-email-montana/54076036/1

Judge McCree of Michigan was publicly censured for taking a cell phone picture of himself naked from the waist up and sending it to a court officer, and then not taking media reports and inquiries about the matter seriously. He allegedly responded to a reporter’s questions about the photos by saying, “Hot dog, yep, that’s me. I’ve got no shame in my game”. According to the Michigan Supreme Court, Judge McCree “conducted himself in a flippant manner and did not give the interview the seriousness he should have. As a result, he brought shame and obloquy to the judiciary.”47

In Texas, Judge Elizabeth Coker sent texts from the bench to an assistant district attorney who was observing a trial, instructing the ADA to pass the information to the ADA trying the case. Her actions eventually led to both a judicial commission investigation and an attempt to impeach her brought in the Texas House.48

J. The Firm Online

While we will not delve deeply into the specific rules for advertising and publicizing, there are some matters worth mentioning relating to oversight and involvement with law firm marketing. The first issue involves that identifier that is the new phone number: the domain name. A domain name is the “web address” or URL (“universal resource locator”) used to identify websites. Must the web address match the firm name (with all of the limitations that matching would imply49)? The answer comes directly from the rules themselves. RPC 7.5(e) provides:

(e) A lawyer or law firm may utilize a domain name for an internet web site that does not include the name of the lawyer or law firm provided:

(1) all pages of the web site clearly and conspicuously include the actual name of the lawyer or law firm;


49 See, e.g., New York State Bar Association Committee on Professional Ethics, Opinion 869 (May 31, 2011) (“A law firm may not include an area of law in the law firm name. A sole practitioner may use the terms “Firm” or “Law Firm” as part of the law firm name”). Note that this opinion specifically acknowledges that while under Alexander v. Cahill, 598 F.3d 79, 95 (2d Cir.), cert. denied, 131 S. Ct. 820 (2010), the ban on trade names as law firm names (as opposed to trade names as mottos) may be constitutionally suspect, the Committee will continue to apply it unless it is actually ruled unconstitutional.
(2) the lawyer or law firm in no way attempts to engage in the practice of law using the domain name;

(3) the domain name does not imply an ability to obtain results in a matter; and

(4) the domain name does not otherwise violate these Rules.\(^{50}\)

Thus domain names fit within the “motto” rule rather than the name rule for purposes of the Rules, and a firm can use a motto/trade name rather than the firm’s precise practice name as its domain name.

The next issue involves responsibility for what the firm puts on the Web. Rule 7.1 prohibits lawyers from engaging in false advertising and in making false claims in their advertising, and as such forbids a lawyer “in the use or dissemination of any advertisement that: (1) contains statements or claims that are false, deceptive or misleading; or (2) violates a Rule.” In addition, firms are required by Rule 5.3 to properly supervise non-lawyers in their employ. When a non-law employee at a firm in Louisiana “implied” on the firm’s website that a former Louisiana governor was “a member of the firm, a governmental relations specialist, and a partner when in fact the former governor is not now nor has he ever been a licensed Louisiana attorney[,]” the firm’s managing partner was disciplined for failing to oversee the non-law employee.\(^{51}\)

A South Carolina practitioner also went astray of the rules when he misstated his qualifications (year of bar admission, experience in federal court) on his web page, and then continued those misrepresentations on sites such as LinkedIn and lawyers.com.\(^{52}\)

Other things that are likely raise ethical concerns include the kinds of content that is permitted on a law firm website. Biographical data has been specifically approved, including past positions (with other law firms, for example). Favorable quotations from publications are

\(^{50}\) This last provision duplicates the introductory provision to this Rule found in Rule 7.5(a): “A lawyer or law firm may use internet web sites, professional cards, professional announcement cards, office signs, letterheads or similar professional notices or devices, provided the same do not violate any statute or court rule and are in accordance with Rule 7.1[.]”

\(^{51}\) In re Murphy J. Foster, III, Supreme Court of Louisiana, Attorney Disciplinary Proceedings No. 10-B-2118 (Oct. 15, 2010).

also allowed, so long as they are not false, deceptive or misleading, and the required disclosures are present.\footnote{See, N.Y.S. Bar Association, Committee on Professional Ethics, Opinion 877 (September 12, 2011); note that the requirements of Rule 7.1 will apply when the maker of the quotation is paid, and that, in addition, the rules of the Federal Trade Commission on online disclosures will also be likely to apply (these require disclosure of payment for advertising or for a variety of other situations where payment may imply an undisclosed conflict of interest. See, 16 C.F.R. Title 16: Commercial Practices).}

Within the otherwise broader category of allowable content are links posted on a firm website. Recently the N.Y. Bar Association has concluded that, “A lawyer may include links to other businesses on the lawyer’s web site provided neither the link nor the linked material involves misrepresentation or causes confusion.”\footnote{NYS Bar Association, Committee on Professional Ethics, Opinion 888 (November 15, 2011).} Generally, links are allowed to offsite resources not under the control of the lawyer, but the purpose of the link, the nature of the linked site, and the relationship of the lawyer to the owner of the linked site are all relevant to any ethical inquiry. Informational sites are acceptable, but reciprocal links raise additional concerns. Where the reciprocal link constitutes advertising, the link is subject to Rule 7.1’s advertising provisions and a link that is part of a cooperative business arrangement subjects the link to rule 5.8(a).

In addition, use of online discounters such as GroupOn and LivingSocial have been approved in a New York State Bar Association Committee on Professional Ethics,\footnote{NYS Bar Association, Committee on Professional Ethics, Opinion 897 (December 13, 2011).} citing with general approval a South Carolina ethics opinion that reached the same conclusion.\footnote{South Carolina Bar, Ethics Advisory Opinion 11-05 (2011); see also, State Bar of Arizona, Opinion 13-01: Internet Marketing Vouchers or Coupons (2013)(approving Groupon style discounters in theory but noting the practical difficulties of their ethical use).} Such uses are subject to the standard attorney advertising requirements (such as labeling as attorney advertising and not being deceptive), as well as additional concerns regarding when a lawyer can keep the payment without actually rendering services (issues that the attorney should make sure are covered by the advertising agreement, a point not explicitly noted in the NYSBA Ethics Committee opinion). Advertising by text messaging has likewise been approved in the State of Ohio.\footnote{Supreme Court of Ohio, Board of Commissioners on Grievances & Disciplines, Opinion 2013-02: Direct Contact with Clients: Text Messages (2013) (distinguishing text messages from more direct, or “real time” communications with potential clients.)} Note that not all online arrangements are likely to be so easily approved. Michigan has
rejected the idea of lawyers paying a referral fee to for-profit websites where the fee structure is specifically linked to the referrals in question.58

K. Electronic Errors Are Bound to Happen

Misdirected E-mail is a fact of life in the information age. What happens when one lawyer receives a message clearly intended for an opposing party or attorney? In Terraphase Engineering, Inc. v. Arcadis, No. C 10-04647 JSW (N.D. Ca. 2010), the plaintiff’s attorney mistakenly sent confidential information to an inside counsel for the defendants (due to not catching an improperly completed “autocomplete” address on the E-mail prior to sending it). Defendant used the information to form a counterclaim in the litigation, and plaintiff moved for a protective order, seeking to disqualify various lawyers involved in the action from continuing. Judge Jeffrey White granted the motion and issued an order disqualifying a defendant’s inside, associate corporate counsel, along with the law firm currently representing the client, due to their reading of E-mail messages clearly intended for the opposing parties in the litigation. The Judge also removed the defendant’s General Counsel from overseeing the litigation.59

The resulting message is clear: errors happen, but judges are unlikely to allow clients to benefit from reasonable errors made by the attorneys on the other side.

L. E-mail is not a Phone Call

Where two attorneys engaged in inappropriate and abusive E-mail exchanges during the course of litigation, those E-mail messages were not only used in their disciplinary proceeding, but were attached to the complaint filed with the disciplinary board. In this particular situation, the lawyers were allegedly attempting to schedule various aspects of an ongoing litigation matter, but were having what might be rather charitably defined as “difficulties.” Short-tempers turned to snark, and snark turned to insults and exchanges including the following took place (among others). Defendant’s attorney addressed Plaintiff’s attorney as “Sparky” and Plaintiff’s attorney responded by referring to defendant’s attorney as “Corky.”


59 See, Beware the Evolving Ethics of Reviewing E-mails, edd blog online (March 8, 2011); http://eddblogonline.blogspot.com/2011/03/beware-evolving-ethics-of-reviewing-e.html; see also, The Association of the Bar of the City of New York Committee on Professional Ethics, Formal Opinion 2012-1: Obligations Upon Receiving a Document Not Intended for the Recipient (2012)(noting that reading a misdirected message is not violative of ethics rules, but even reading privileged information may be).
Plaintiff’s attorney also wrote the following to Defendant’s attorney: “You are an ass clown and absolutely an ass clown. Shouldn’t you be tending to your retarded son and his 600th surgery or something instead of sending useless E-mails. [sic] In fact, I think I hear the little retards [sic] monosyllabic grunts now; Yep, I can just barely make it out; he is calling for his ass clown. How sweet.” This message followed an earlier one from the Defendant’s attorney that included the following: “If you need to find indications of the ‘retardism’ that you seek, I suggest you look in the mirror, and then look at your wife . . . she has to be a retard to marry such a loser like you” and “Unfortunately, it looks like the better part of you was the sperm cells left on the back seat of the Ford Pinto.”

The lawyers were both disciplined; the Defendant’s lawyer received a public reprimand and was required to take a class in professionalism, while Plaintiff’s attorney was suspended for 10 days and required to take an anger management class.60

In another case, a Texas lawyer referred to his opponent’s attorney as a pansy and threatened him using vulgar language, again during scheduling of a deposition and various discovery disputes. The Texas lawyer lost his position as a partner at the firm and a sanctions motion was brought against him by opposing counsel.61

Finally, a Virginia lawyer was ordered to attend a “non-internet” anger-management course after sending an E-mail to a counsel who had been opposing counsel in an earlier case after that counsel was later indicted on an unrelated matter. The E-mail included suggestions that the attorney would comfort the receiver’s wife while he was in prison, and that he (the indicted attorney) should look forward to being victimized in prison.62

The lesson here is that while exchanges such as these may have taken place between lawyers in the past, they were far more likely to have been part of an in-person or telephone conversation. As we move to more use of electronic communications, lawyers should be aware that E-mail is written, potentially permanent, and easily shared. An E-mail is not a phone call,

60 Note that this can happen in person, as well. See, Complaint in the Matter of David Alan Novoselsky, Before the Hearing Board of the Illinois Attorney Registration and Disciplinary Commission, Commission No. 2011PR00043 (September 2012), where the respondent was charged with calling opposing counsel and “bitch” and a “slut” while in a courtroom and during legal negotiations.


and appropriate levels of decorum and professionalism must be shown by lawyers engaged in using electronic communications technologies.

As an aside, note that if addressed to the substance of an argument, rather than framed as a personal attack, such comments and “name calling” may be acceptable given current norms in U.S. Supreme Court Practice.63

M. Encryption and Electronic Transactions

While some messages may be misdirected or mislaid, others may fall into the hands of hackers or others who “overhear” the electronic communications. Lawyers are required to maintain client confidentiality, but to date ethics committees have not required lawyers to use encryption technology – technology that “locks up” messages and only allows unlocking with a key – while engaging in electronic communications. In 2010, the NYS Bar Association Committee on Professional Ethics issued its opinion that “A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer’s obligations under Rule 1.6.”64 The opinion also imposes a duty on the lawyer to follow current technology to ensure confidentiality is retained in the face of technological change. The opinion is consistent with other state bar opinions, such as those of California65 and Alabama.66

The NYS Bar opinion sets out four elements that are relevant to making the determination of whether confidentiality is reasonably assured:

1. Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;

63 For example, Justice Scalia, in his dissenting opinion in Sykes v. United States, wrote: “That incompatible variation has been neither overlooked nor renounced in today’s tutti-frutti opinion.” Sykes v. United States, slip op., Dissenting Opinion of Justice Scalia, p. 3. If calling majority opinions “tutti-frutti” is acceptable for a sitting Supreme Court Justice, it is hard not to argue that professional norms of civility have shifted away from politeness in recent years.

64 NYS Bar Association, Committee on Professional Ethics, Opinion 842 (September 10, 2010).


2. Investigating the online data storage provider’s security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;

3. Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or

4. Investigating the storage provider’s ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.

The rules thus would seem to require a storage provider that provides confidentiality and that also provides portable data rather than proprietary data storage solutions. Other jurisdictions have reached similar results, though at times with subtle differences in articulation and detail.67

These opinions are consistent with earlier opinions that did not require encryption in E-mail use, but still required the lawyer to follow practices intended to safeguard confidentiality.68 Note that after the ABA Commission on Ethics 20/20 proposed changes to the Model Rules of Professional Conduct intended to further alter the duties placed on lawyers in relation to electronic communications emphasizing that lawyers must be aware of, understand, and make reasonable decisions about the technologies they use.69 The rule was adopted, with new Model Rule 1.1 reading:

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

And an amended comment 8 to Model Rule 1.1 reading:

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.

In addition to being competent when it comes to technology, a lawyer may have to help clients maintain competence, as well. When working with a client who is using employer


68 See, e.g., NYS Bar Ass’n, Committee on Professional Ethics, Opinion 709 (Sept. 16, 1998); see also, Assn’of the Bar of the City of New York Opinion 1998-2 (December 21, 1998).

69 ABA Commission on Ethics 20/20 Initial Draft Proposals – Technology and Confidentiality (May 2, 2011) [see appendix for text of the proposed changes]
provided E-mail, a lawyer may have an obligation (especially if the matter involves the employer) to notify the employee that E-mail communications may not be private and that attorney-client privilege may be waived when using employer provided E-mail.  

N. Being in Two Places at Once  
A lawyer from Ohio established “a relationship” with a law firm in Florida that worked on cases involving consumer debt. As part of the relationship, the Ohio lawyer provided the Florida firm with his Ohio bar registration number and his electronic signature. The Florida firm used these details in cases without the lawyer’s permission. The Ohio lawyer was suspended from practice for six months, but the suspension was stayed so long as he did not engage in further misconduct.

O. Being in One Place and not Another  
We all know that technology can be a distraction in modern life, but sometimes it can also lead to ethical violations. An attorney who was trying to arrange a settlement but who had not been able to reach his client about the matter went to court on the return date to appear. While outside the court room on his cell phone trying to reach his client, the attorney missed the case being called on the docket. The opposing attorney responded to the call and a default judgment was entered against the attorney’s client. While the attorney argued he was trying to sort the matter out while he was out of the courtroom, by failing to check the status of the case with the clerk and to follow-up with the clerk before he left the courtroom he committed misconduct and was suspended from the practice of law for 60 days.

P. Working Two Places at Once  
In another case that would have been nearly impossible to imagine before the Internet arrived on the scene, an attorney working for the State of Kentucky was disciplined when he

---

70 American Bar Association, Standing Committee on Ethics and Professional Responsibility, Formal Opinion 11-459 (August 4, 2011); see also, “Law Firms are Pressed on Security for Data,” NY Times, March 26, 2014 (noting client pressure on law firms to secure computer and networking of data) http://dealbook.nytimes.com/2014/03/26/law-firms-scrutinized-as-hacking-increases/

71 Disciplinary Counsel v. Lorenzon, Slip Opinion No. 2012-Ohio-4713

72 Attorney Grievance Commission of Maryland v. John Wayne Walker-Turner, Misc. Docket, AG No. 16, September Term, 2011 (this was Walker-Turner’s second brush with discipline; he had earlier received a 30 day suspension for unrelated conduct).
used State resources – time and the office’s Westlaw account – to earn money by posting answers to legal questions on JustAnswer.com, an online question and answer forum. The Supreme Court of Kentucky publicly reprimanded the respondent for his actions. 73

Q. More problems with E-mail

In two separate cases, attorneys sent photos via E-mail or posted them on Facebook (thinking they were limited to just friends). In the first case, an attorney handling a wrongful death case sent a picture of the dead body to a friend and included disparaging remarks. As the firm monitored E-mail, the message was seen and his firm reported him to the disciplinary authorities.

In the second case, a public defender in Florida posted a photo of a client’s underwear on Facebook. According to the Miami Herald:

[Defendant’s] family brought him a bag of fresh clothes to wear during trial. When Miami-Dade corrections officers lifted up the pieces for a routine inspection, Recalde’s public defender Anya Cintron Stern snapped a photo of Recalde’s briefs with her cellphone, witnesses said.

While on a break, the 31-year-old lawyer posted the photo on her personal Facebook page with a caption suggesting the client’s family believed the underwear was “proper attire for trial.”

The posting led to a mistrial in the case (and the attorney was fired, as well). 74

In a similar vein, the attorney defending George Zimmerman in the Trayvon Martin shooting case in Florida was pictured eating ice cream on his daughter’s Instagram page with a caption that read, “‘We beat stupidity celebration cones.’ #zimmerman #defense #dadkilledit

The attorney later apologized for the posting.75

73 Matthew Scott Finley Movant v. Kentucky Bar Association, Supreme Court of Kentucky, 2012-SC-000465-KB (October 2, 2012)


R. Trying to Influence Public Perception by Posting Criminal Discovery Video Online

A lawyer in Illinois tried to convince the public that his client had been framed, with police planting drugs on his client. The video, which the attorney received during discovery, was posted to YouTube and then linked from Facebook, where it received more than 2,000 views before a judge ordered it removed. The complaint alleged that the attorney violated rules relating to discovery materials. That the attorney took all of the relevant actions without informing the client, let alone obtaining the client’s permission, was also noted in the complaint.\textsuperscript{76}

S. Westlaw Access Not Allowed After Leaving Position

An attorney had helped his legal employer enter into an agreement with Thomson-Reuters for the use of Westlaw. On leaving his position, the attorney tried to cancel the arrangement, but Westlaw would not allow cancellation of the contract, so the old office maintained payments on the contract. The attorney, who retained his Westlaw ID, began using the account when he took up his new legal position. His use was discovered and an ethical complaint was filed. The Supreme Court of Oregon, in reviewing a claim for reciprocal discipline (the misconduct occurred in Hawaii, and respondent was admitted in both Hawaii and Oregon), publicly reprimanded the respondent for his actions.\textsuperscript{77}

T. With Computers You Can Make Stuff Up (but shouldn’t)

An attorney who was involved in a proceeding related to her children forged, in the words of the Court, “from whole cloth,” an order of a court in New Jersey to show to authorities in Colorado. In discovering the forgery, ethics charges were brought and the respondent was publicly reprimanded for her actions.\textsuperscript{78}

\textsuperscript{76} http://www.abajournal.com/news/article/ethics_complaint_claims_lawyer_tried_to_sway_potential_jurors_by_posting_di/
; https://www.iardc.org/12PR0006CM.html;

\textsuperscript{77} In re The Reciprocal Discipline of EVERETT WALTON, Accused, OSB 12-70; SC S060606, Supreme Court Of The State Of Oregon (October 11, 2012).

U. What’s on the Web Can Be Found

When an attorney who was suspended from the practice of law continued to practice, it didn’t take long before a magistrate found the listing of his suspension on the Supreme Court’s website. A client also found the listing. Both the magistrate and the client notified the disciplinary authorities, and the attorney was suspended from the practice of law for two years (one year stayed if the attorney followed the required course of action outlined by the Court).79

In another case, an attorney who failed to take any action on a case while continually assuring the client that the case was underway – even after it was dismissed – was indefinitely suspended by the Maryland Court of Appeals for his actions. The client found out about the true status of the case when she searched for the case on the Maryland case search website.80

V. You Can’t Get Rid of What’s on Facebook, But You Can Try (Though Maybe You Shouldn’t)

An ethics opinion from the New York County Lawyers Association provides guidance for counseling clients on social media content. The opinion addresses the following:

It is the Committee’s opinion that New York attorneys may advise clients as to (1) what they should/should not post on social media, (2) what existing postings they may or may not remove, and (3) the particular implications of social media posts, subject to the same rules, concerns, and principles that apply to giving a client legal advice in other areas

While the answer to each is yes, it is a very soft, qualified yes, with quite a few caveats. Attorneys may not participate in the creation of false evidence, cannot suppress evidence, and cannot destroy evidence (evidence being material related to litigation). That said, the overall conclusion is that social media is part of the litigation strategy of the modern age, and lawyers can and should deal with it explicitly, though ethically.81

A Virginia lawyer could have been aided by the NYCLA’s qualms, but confronted the issue of Facebook deletions prior to the opinion’s issuance. The lawyer counseled his client to delete

79 Disciplinary Counsel v. Seabrook, 133 Ohio St.3d 97, 2012-Ohio-3933 (2012).


Facebook posts and content while the client was involved in litigation to which the Facebook content was relevant. Considered spoliation of evidence, the court reduced a wrongful death jury award and the lawyer was subsequently suspended from the practice of law for five years.  

W. Friends, Following, and Linking-in: Connections in a Connected World

There are a variety of ways in which connecting to others online may implicate ethical requirements. Ethics opinions are split, for example, as to whether judges can friend lawyers who appear in their courts, with Florida deciding against and New York allowing judges to join social networks and make such contacts where otherwise within the rules. Note that at least one judge in North Carolina has been reprimanded for exchanging ex parte messages on Facebook concerning an ongoing case with an attorney on the case. A judge who initiated a friend request with a litigant was disqualified from ruling on the case in question.

As for attorneys, the questions that arise tend to be concerned more with whether information can be ethically gleaned from public web pages and public areas of social networking sites (NY has concluded it can) and whether a lawyer or a lawyer’s agent/employee can seek to “friend” a witness or other interested party who is unrepresented by a lawyer (friending someone represented by a lawyer would violate rules requiring that a lawyer avoid communicating directly with someone who is represented by a lawyer).


83 Florida Supreme Court, Judicial Ethics Advisory Committee, Opinion Number 2009-20 (Nov. 17, 2009).

84 New York State Judicial Ethics Commission, Opinion 08-176 (Jan. 29, 2009); see also, American Bar Association, Standing Committee on Ethics and Professional Responsibility, Formal Opinion 462, “Judge’s Use of Electronic Social Networking Media (Feb. 21, 2013) (concluding that judges should be allowed to use social media, and that being “friends” does not immediately disqualify a judge in a case involving that attorney friend, but that judges must be cautious and watch for potential violations of judicial ethics).

85 See, Judge Reprimanded for Friending Lawyer and Googling Client, ABA Journal Law News (June 1, 2009); http://www.abajournal.com/news/article/judge_reprimanded_for_friending_lawyer_and_googling_litigant/


87 New York State Bar Association, Committee on Professional Ethics, Opinion 843 (September 10, 2010); note that this opinion applies only to publicly available information. The NYS Bar Association has not weighed in on the discussion regarding friending, below.
On this latter point, the Philadelphia Bar Association has issued an opinion that prohibits the practice of friending someone to gain information about them or matters related to litigation. The Bar Association opinion finds that seeking to friend someone while omitting the critical information as to why that friend request is being sent is deceptive in violation of Rule 4.2.88 The NYC Bar Association, on the other hand, has issued a contrary opinion, and argues that the situation is like one that arises when a person sitting in a bar is approached by a lawyer’s investigator. The investigator has no obligation to immediately disclose he or she is an investigator, but rather may engage the person in conversation hoping to uncover relevant information (so long as the investigator is not deceptive). In the same regard, the opinion opines, so may a person send a “blank” friend request to an unrepresented person as the blank request is not itself deceptive, and the person accepting that friend request and opening up their social networking activities to the investigator is the person taking the risk that the stranger asking to friend them does not have their best interests at heart.89

Another social networking issue to consider is the extent to which lawyers can interact with jurors via social networking or other communications technologies. The New York County Bar Association Committee on Professional Ethics has approved searching publicly available information on prospective jurors both prior to and during a trial.90 Analogizing the situation to that which confronts lawyers who might wish to investigate other parties in litigation, the Committee concluded, “we conclude that passive monitoring of jurors, such as viewing a publicly available blog or Facebook page, may be permissible.” That conclusion does not change for searching for information about jurors during trial, but notes that in this case, as lawyers are prohibited from talking to jurors during the pendency of litigation, the lawyer must take extra precautions to ensure that the juror does not become aware of the attorney’s efforts. 91

In this respect, fully understanding how a particular technology platform works is critical to the situation. Despite repeated appearances of claims to the contrary on Facebook, Facebook

88 Philadelphia Bar Association, Professional Guidance Committee, Opinion 2009-02 (2009); see also, San Diego County Bar Association, SDCBA Legal Ethics Opinion 2011-2, agreeing with the Philadelphia opinion, but based on a different provision, as California has not adopted the relevant ABA Model Rules as part of its ethics framework.

89 Ass’n of the Bar of the City of New York, Committee on Professional Ethics, Formal Opinion 2010-2 (2010). Note that the opinion does not allow for any deception in seeking information in this regard.

90 NYCLA Committee on Professional Ethics, Formal Opinion No. 743 (May 18, 2011).

91 Id., at page 3.
users are not aware when someone has viewed their public profile pages. However, LinkedIn, however, allows you to see not only that “someone” has viewed your LinkedIn profile, but who that person is (if that person was LinkedIn member signed in at the time they viewed the profile). Checking a juror’s public Facebook page would be allowed under the County Bar’s opinion, checking a juror’s LinkedIn profile while logged in to LinkedIn would not. The American Bar Association has agreed in part with this reasoning – noting that lawyers can read juror social media postings and content – but disagreeing that simply because a juror may become aware of the lawyer’s efforts the lawyer has “communicated” with a juror.

Understanding the nature of the sites and the way they are structured – and the way they structure your information and your public facing profile – is also important. LinkedIn, for example, currently provides an option for connections to recognize your skills and to be endorsed for your knowledge. LinkedIn has in the past included categories labeled “skills and expertise” and “specialties.” These raised issues for lawyers as words like “specialty” are often viewed with skepticism by bar ethics committees. In these circumstances, the Philadelphia Bar Association opined that lawyers could list their practice areas under “skills and expertise,” and could even rank their proficiency in those areas, but could not indicate that they were “experts” in any particular areas. The New York State Bar Association Committee on Professional Ethics issued an opinion in the summer of 2013 that lawyers certified as specialists could list those areas under LinkedIn’s “specialist” category, but limited that holding to individual lawyers, not firms, as firms cannot be certified as specialists. Florida took a predictably conservative line,


96 New York State Bar Association, Committee on Professional Ethics , Opinion 972 (July, 2013); note that LinkedIn subsequently changed its categorization system such that individual lawyers can no longer list specialties.
disagreeing with Philadelphia’s conclusions in issuing guidelines for attorneys indicating that Florida attorneys who were not certified specialists should not list their practice areas under the “skills and expertise” category.\textsuperscript{97} Even LinkIn’s new formulation – endorsements – can raise problems where they suggest endorsements and connections endorse you for experience or expertise you don’t actually have.\textsuperscript{98}

As a final, and closing, note, online social networking sites are opening new opportunities that may implicate the rules in new and unique ways. For example, in an opinion from June of last year (2011), the New York State Bar Association, Committee on Professional Ethics, concluded that an attorney can offer a prize as an incentive for others to join the attorney’s social network (with caveats, of course, such as that the lawyer not require the prize seeker to retain the lawyer, and that the lawyer award the prize randomly, among others).\textsuperscript{99} This is the kind of situation that likely would have never arisen before the Internet became a part of everyday legal practice. No one would have had an opportunity to give a prize to others for “connecting” with them. Today, however, those opportunities are prevalent, and benefits of pursuing them – such as having an established network of people with whom to communicate legal practice news and events – are becoming clearer. The ethics committees have so far done a good job keeping up with technological changes and whether/how they affect law practice (the uncertainty of “friending” non-party witnesses aside), and it is important to keep up with developments in this area of professional conduct as technology and the law march forward.

\textsuperscript{97} The Florida Bar Standing Committee on Advertising, Guidelines for Networking Sites (April 16, 2013); The Florida Bar, Advisory Letter (Sept. 11, 2013).

\textsuperscript{98} See, Dennis Kennedy, Is LinkedIn’s Endorsement Feature Ethical for Lawyers? LawNewsNow, ABA Journal (Dec. 1, 2013) [http://www.abajournal.com/magazine/article/linkedin_endorsement_feature_draws_some_questions]

\textsuperscript{99} NYS Bar Association, Committee on Professional Ethics, Opinion 873 (June 9, 2011).
Technology & Security: It’s All About Cyber

Table of Contents

Technology & Security: It’s All About Cyber PowerPoint ........................................ 43

NIST.IR.7298r2 (2013), at 57-58, 94-95, 141, 146 [8 pp] (for reference to define “information security” and other terms) ................................................................................................. 86

2016-01-31 GTDT - Cybersecurity U.S., at 72-77 [6 pp] (read through) ......................... 94

Key Findings, ACC Foundation -State of Cybersecurity [10 pp] (skim) ....................... 104

FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. 2015) [24 pp] (focus on alleged security failures and basis of FTC regulatory authority) ................................. 118

California AG Breach Report (2016), at i-vi (skim) and 1 -26 (skim), at 27-39 (focus on recommendations) [45 pp] .................................................................................. 142

Exercise: Cyber Breach Incident Response

The corporate IT director reports that malware has been discovered on your company’s computer systems, and it is likely that sensitive personal information, as well as business plans and intellectual property of the company, have been exposed. U.S. and state data security breach notification laws have been triggered and, once the required notices go out, media inquiries and letters from the Federal Trade Commission and State Attorneys General arrive, seeking information about the incident and the company’s cybersecurity practices. A letter comes from a prominent legislator asking questions about the incident. Corporate partners inquire about contractual data security and privacy obligations, and the potential impact of the incident on their systems, data, and business. It is time for a regular SEC filing, which requires evaluating whether to report the incident as a material risk. Shareholder representatives and plaintiffs’ lawyers are organizing themselves to pursue actions related to the incident and its effect on the company, its operations and revenues, and individuals’ privacy. And the Board wants to know what steps the Office of General Counsel has taken to assess and mitigate the legal risks.
Technology & Security: It’s All About Cyber

Antony K. Haynes

September 23, 2016
Attacks

**FINANCE**
In 2015, an unknown group infiltrated hundreds of banks in multiple countries, swiping somewhere in the neighborhood of $1 billion.

**GOVERNMENT**
U.S. Indicts 7 Iranian Hackers For Cyber Attacks On Banks, New York Dam

The indictment described the suspects as "experienced computer hackers" believed to have been working on behalf of the Iranian government.

**HEALTH**
US health insurer Anthem hit by massive cyberattack: 80 million customers' private data exposed

Hackers have stolen personal information relating to current and former customers and staff of number two US health insurer Anthem, after breaching an IT systems containing data on up to 80 million people.
Goals

1. Gain knowledge and understanding of key cybersecurity and data privacy issues facing corporate counsel.

2. Begin a conversation and information sharing around best practices for cybersecurity and data privacy.
Corporate Cybersecurity Standards
Corporate Cybersecurity Standards

• Threat Agents
• Top 10 Issues
• Checklists
• “Reasonable Security”
• Wyndham Worldwide
Top 10 Issues

• Complexity, multi-disciplinary and dynamic nature
• Rapidly evolving cyber threats and threat agents

**Attack Vectors**
- Malware
- Phishing
- DDoS
- APT
- ZDE

**Threat Agents**
- Insiders
- Hacktivists
- Cybercriminals
- Nation Sates
Top 10 Issues

**Cybersecurity**: The ability to protect or defend the use of cyberspace from an attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

**Cyberspace**: A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

Source: Committee on National Security Systems Instruction (CNSSI)-4009 (National Information Assurance (IA) Glossary
Top 10 Issues

Information Security: Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

2) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

3) availability, which means ensuring timely and reliable access to and use of information.

Source: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-66 (Information Security); 44 U.S.C., Sec 3541
Cyber Threat Agents

Hacktivist – Insider – Cyber Criminal – Nation State
Nation States

Motivation

• This hacker is directly employed by an arm of a national government and is typically very well-funded compared to small hacktivist groups and individual cyber criminals.

• These hackers are motivated by economic, political, and military advantages. This means that there is potentially much greater damage if they are successful in accessing the data they seek.

• Nation states are interested in data about critical infrastructure, along with trade secrets, business information and emerging technologies (espionage).

• This can lead to a loss of competitive advantage for the countries or organizations they target, as well as a disruption to critical infrastructure (sabotage), which could wreak havoc on the general population.

Source: http://cybersec.buzz/cyber-threat-actors-motivation/
Cyber Criminals

Motivation

- Cyber-criminals seek the immediate satisfaction of a financial payout. They typically target personal and financial information, hoping to exploit or sell the data for their own financial gain.

Effects

- The organization targeted, can suffer direct financial loss or legal issues, in the form of lawsuits and regulatory penalties. Above all, a breach caused by a cyber-criminal can cause a loss of confidence and reputational damage, which can be difficult to regain, especially if sensitive customer data has been compromised. One of the most worrying aspects about cyber-criminals is their increasing level of sophistication and organization.

Data Targeted

- **ATM and point-of-sale (PoS) skimming**: Stealing bank and PIN information when cards are used at ATMs, credit/debit card terminals and other card readers.
- **Random Access Memory (RAM) scraping**: Stealing credit/debit card information when the card information is stored in the server’s memory system.
- **Code injection**: Introducing malicious code into a computer program to redirect the system’s actions.
- **Keylogging**: Using a program to record computer keystrokes in order to gain confidential information.
- **Phishing**: Creating fraudulent, socially engineered electronic content (websites, emails, etc.) that is from a seemingly legitimate source, enticing victims to provide confidential information.

Source: http://cybersec.buzz/cyber-threat-actors-motivation/
Hacktivists

Motivation

• Activist hackers who are looking to influence political or social groups (subversion) by pressuring businesses, governments and other entities to change their practices.

• How? By attacking organizations and stealing trade secrets or sensitive business information, including data relevant to key leaders, employees, and customers.

• Hacktivists take advantage of the data to disrupt normal business activities and put the focus and media attention on their own agenda. The target’s reputation is likely to be damaged as a result of this type of attack, which often has a long-lasting effect that extends beyond the initial loss. The most well-known hacktivist group today is a collective known around the globe as Anonymous.

Common Attack Vectors

• Distributed Denial of Service (DDoS) attack:

• Website defacement: Changing the appearance of a website via unauthorized access such as through a cross-site scripting vulnerability.

• Information disclosure: Publicizing information about the targeted institution that was not previously publicly known or releasable.

• Doxing: The publication of personally identifiable information (PII) about a specific person for malicious purposes.

Source: http://cybersec.buzz/cyber-threat-actors-motivation/
Malicious Insiders

• Insiders are an often forgotten source of attacks, though they are arguably the most dangerous as they represent trusted employees and partners.

• Motivated by personal gain, professional revenge, and monetary reward, malicious insiders usually have easy access to the data they are looking to expose or monetize. This typically includes customer data, company financial and salary information, along with employee data, corporate secrets, and notable research that has yet to be released.

• Malicious insiders seek to disrupt business operations and damage the organization’s brand and reputation. In some cases, they may be collaborating with cyber-criminals for personal financial gain.

Source: http://cybersec.buzz/cyber-threat-actors-motivation/
Top 10 Issues – 1. Increased Regulation & Compliance Requirements

FTC

• Most common actions due to insufficient cybersecurity practices and failure to disclose breaches involving consumer information
• 3rd Circuit in Wyndham Worldwide
• $100M settlement in 2015 with LifeLock Inc.
• → Get FTC’s Start with Security: A Guide for Business (lists 10 lessons)

• FCC

• $10M fine in 2014 against TerraCom, YourTel - stored PII in clear on internet
• $25M fine in 2015 against AT&T - employees sold 280,000 customer SSANs
Top 10 Issues – 1. Increased Regulation & Compliance Requirements

SEC’s Division of Investment Management

- RT Jones (investment advisor) fined $75k for “failure to adopt policies reasonably designed to protect consumer records and information”
- → SEC’s IM Guidance Update for Cybersecurity

DOJ’s Cybersecurity Unit

- → Best Practices for Victim Response and Reporting of Cyber Incidents

California State AG

- → 2016 California Data Breach Report
- Recommendations: (1) Implement 20 CIS Critical Security Controls (2) Expand use of multi-factor authentication (3) Use strong encryption to protect PII in portable devices and (4) Encourage consumers’ use of credit file fraud alerts
- Failure to implement [applicable] Controls... constitutes a lack of reasonable security
Top 10 Issues – 1. Increased Regulation & Compliance Requirements

• Recommended Actions
  • Identify industry’s regulator’s guidelines and relevant data security and privacy laws and regulations applicable to your organization
  • Determine regulatory compliance obligations for cybersecurity
  • Streamline existing regulatory compliance processes
  • Train incident response team compliant with breach notification laws
Top 10 Issues – 2. Increased Litigation Exposure

- Cost = ~ $145 per stolen/lost record
- Target
  - $39M settlement with MasterCard banks’ class action lawsuit
  - $10M settlement with customer class action lawsuit at MTD
- Neiman Marcus
  - 7th Circuit ruled customers had standing for class action
  - Mere theft of PII constitutes imminent risk of suffering a concrete injury
- Spokeo Inc. v. Robins
  - USSC remanded standing issue to 9th Circuit (FCRA)
  - A realistic threat of actual injury is necessary but “intangible injuries can nevertheless be concrete”

• Standard of care
  • Regulators expect boards actively manage cyber risk at enterprise level
  • Industry regulations (e.g. HIPPA, GLBA) and standards (e.g. PCI DISS, NIST Framework)
  • FTC’s *Start with Security: A Guide for Business* (listing 10 lessons)
  • SEC OCIE 2015 Cybersecurity Examination Initiative
  • California AG 2016 Data Breach Report

• Recommended Actions
  • Approach cybersecurity as an enterprise risk management issue (not just IT)
  • Understand legal implication of cyber risks as they relate to company’s circumstances
  • Have adequate access to cybersecurity expertise and provide regular and adequate time on board meeting agendas for cyber risk discussions
  • Set expectation for management to established enterprise risk management framework with adequate staffing and budget
  • Cyber risk discussion includes identification of risks to avoid/ accept/ mitigate/ transfer and specific plans associated with each approach

• Questions boards should ask
  • Governance
  • Critical asset review
  • Threat assessment
  • Incident response preparedness
  • Employee training – Employee error is the most common reason for a breach
  • Third-party management
  • Insurance
  • Risk disclosure
Top 10 Issues – 4. Counseling the C-Suite

• Goal: Provide legal advice at both a strategic and day-to-day operational level to various members of the C-Suite

• Issues

• Stakeholder Interactions

• Recommended Actions:
  • Appoint counsel to be responsible for legal issues related to cyber security and the company’s security program
  • Bring novel issues of policy and legal risk to senior leadership and board
Top 10 Issues – 5. Cyber Insurance

• Duty of Care:
  • Boards actively engaged in monitoring have low personal liability risk—
  • “acted in a deliberate and knowledgeable way, identifying and exploring alternatives”

• Issues – Type of Coverage:
  • First Party coverage (crisis management and identity theft response, cyber extortion, data asset protection)
  • Third Party coverage (network security liability, privacy liability)
  • Specific Policies (underwriting, claims, exclusions, coverage, requirements)

• Recommended Actions:
  • Review efficacy of cyber-risk insurance for your organization’s purposes. Pay particular attention to exclusions and conditions imposed.
Top 10 Issues – 6. Commercial Transactions

• Transactions Implicated:
  • M&A
  • Vendor/Supplier contracts
  • Customer/Client contracts

• Recommended Actions:
  • Update due diligence checklist to include cybersecurity issues
  • Review key contractual provisions used in transactions
  • Review vendor oversight program to include cybersecurity risk assessments
Top 10 Issues – 7. Information Sharing with Law Enforcement

• Governments Compel Decryption
  • China’s counterterrorism law can compel decryption of communications
  • FBI’s request that Apple install iPhone “back door”

• Recommended Actions
  • Confirm company’s information sharing partnerships with industry and government benefit the company and do not put it at undue risk
  • Provide regular legal oversight and training of relevant personnel
  • Appoint counsel for issues arising out of law enforcement interactions
  • Develop law enforcement contacts and relationships prior to needing them
Top 10 Issues – 8. Incident Preparation & Response

- **Recommended Actions**
  - Appoint counsel to help lead the incident response team and process (should be familiar with cybersecurity concepts, fact patterns and terms)
  - Retain key internal and external resources (forensics, counsel, PR)
  - Conduct regular exercises, including senior leaders, to prepare for incidents
  - Prepare for key legal issues in advance, e.g. attorney-client privilege, communications with senior management, criteria for incident disclosure
Top 10 Issues – 9. International Data Transfers

• Trans-Atlantic data transfers face a period of continued uncertainty
  • ECJ in *Schrems* (Oct. 2015) invalidated data transfer safe harbor

• EU-US Privacy Shield proposed in February 2016
  • FTC enforces “strong obligations on companies handling Europeans’ personal data”
  • US agrees to prohibit mass surveillance of EU personal data, subject to “clear limitations, safeguards and oversight mechanisms”
  • EU citizens may seek redress in FTC, free ADR, or in intelligence agency ombudsperson
  • In June, the EC proposed further data sharing limitations on companies ability to transfer data to third parties and on ombudsperson independence.

• Recommended Actions:
  • Anticipate impact of EU-US privacy shield on business operations
Top 10 Issues – 10. Internet of Things

• Limited regulation (currently)
  • FTC’s Trendnet enforcement action in 2013 only significant case

• Recommended Actions:
  • Review company’s use or production of mobile data collection for cybersecurity issues
  • Consider evolving standards on data collection, unexpected uses of consumer data and/or heightened security risks
Cybersecurity Self-Assessment

### Organizational Prevention and Preparedness

- Organization conducts a cybersecurity audit of the entire organization at least annually
- A member of the legal department is on the company’s data breach response team
- Organization has cybersecurity insurance
- Organization has mandatory training on cybersecurity for all employees
- Organization tests employee preparedness/knowledge of cybersecurity practices/data polices at least annually
- Organization retained outside counsel to assist you should a breach occur
- Company collaborates proactively with law enforcement or other governmental agencies to address cybersecurity risks
- Organization retains a forensic company to assist should a breach occur

### Organizational Policies

- Password policy
- Social media policy
- Document retention policy
- Website privacy policy
- Employee manual acceptance policy
- Internet privacy policy
- Identity and access management
- BYOD policy
- Data map

### Organizational Staffing

- Chief Information Officer (CIO)
- Privacy/Security Manager
- Chief Information Security Officer (CISO)
- Chief Risk Officer (CRO)
- Chief Privacy Officer (CPO)
- Chief Security Officer (CSO)

### Organizational Preparedness Evaluation

- Conduct cybersecurity audit of entire organization at least annually
- Use a standard (e.g., SSAE, NIST, ISO) to prepare for, manage, and reduce cybersecurity risk
- Track mandatory training requirement and attendance for all employees
- Test employees’ knowledge of mandatory training
- Conduct mock security event
- Conduct tabletop exercises
- Review disciplinary actions for violations

Source: ACC Foundation, Key Findings from the ACC Foundation the State of Cybersecurity Report (2016), at 8
Questions for the Board to Ask Management

SITUATIONAL AWARENESS
1. Were we told of cyberattacks that already occurred and how severe they were?
2. What are the company’s cybersecurity risks, and how is the company managing these risks?¹
3. How will we know if we have been hacked or breached, and what makes us certain will we find out?
4. Who are our likely adversaries?²
5. In management’s opinion, what is the biggest vulnerability in our IT systems?
6. If an adversary wanted to deal the most damage to our company, how would they go about it?
7. Has the company assessed the inside threat?³
8. Have we had a penetration test or external assessment? What were the key findings, and how are we addressing them? What is our maturity level?
9. Does our external auditor indicate we have deficiencies in IT? If so, where?

CORPORATE STRATEGY AND OPERATIONS
1. What are leading practices for cybersecurity, and where do our practices differ?
2. Do we have an appropriately differentiated strategy for general cybersecurity and for protecting our mission-critical assets?
3. Do we have an enterprise-wide, independently budgeted cyber-risk management team? Is the budget adequate?
4. Do we have a systematic framework, such as the NIST Framework, in place to address cybersecurity to assure
5. Where do management and our IT team disagree on cybersecurity?
6. Do the company’s outsourced providers and contractors have cyber controls and policies in place and clearly monitored? Do those policies align with the company’s expectations?
7. Does the company have cyber insurance? If so, is it adequate?
8. Is there an ongoing, company-wide awareness and training program established around cybersecurity?
9. What is our strategy to address cloud, BYOD and supply chain threats?⁴
10. How are we addressing the security vulnerabilities of an increasingly mobile workforce?

INCIDENT RESPONSE
1. How will management respond to a cyberattack? Is there a validated corporate incident response plan? Under what circumstances will law enforcement and other relevant government entities be notified?²
2. For significant breaches, is our communication adequate as information is obtained regarding the nature and type of breach, the data impacted, and ramifications to the company and the response plan?³
3. Are we adequately exercising our cyber-preparedness and response plan?
4. What constitutes a material cybersecurity breach? How will those events be disclosed to investors?

FTC Section 5 Enforcement

• Reasonable Security Standard
  • FTC Allegations of insufficient cybersecurity practices and failure to disclose breaches involving consumer information.
16 CFR 314.3
Standards for safeguarding consumer information

• **Information security program.**
  • comprehensive information security program that is written
  • contains administrative, technical, and physical safeguards appropriate to:
    • your size and complexity,
    • the nature and scope of your activities, and
    • the sensitivity of any customer information at issue.
Standards for safeguarding consumer information

• **Information security program.**
  
  • Such safeguards ... shall be reasonably designed to ...
    
    • (1) Insure the security and confidentiality of customer information;
    
    • (2) Protect against any anticipated threats or hazards to the security or integrity of such information; and
    
    • (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

• Such safeguards ... shall include the elements set forth in § 314.4
Elements of comprehensive information security program

• (a) Designate an employee or employees to coordinate your information security program

• (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.

• (c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
16 CFR 314.4
Elements of comprehensive information security program

• (d) Oversee service providers, by:
  • (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
  • (2) Requiring your service providers by contract to implement and maintain such safeguards.

• (e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.
FTC v. Wyndham Worldwide
Wyndham’s Hotel Group Brands
Franchise vs Management Contract

• A franchisee is the buyer of a brand name and remains an independent businessman from the franchiser (who owns the brand)

• In a management agreement, the franchiser provides the same services as a franchise agreement, such as brand, reservation system etc., but on top of this, there is an agency agreement, meaning the brand operates the hotel, making all the day-to-day decisions on behalf of the owner.

• In a franchise agreement fees are collected on a room revenue basis, and in the management agreement, fees are collected on a total revenue basis and on the bottom-line
Wyndham Attacks

• 2008 – 2010 – Wyndham attacked three times
  • Hackers stole PII for over 619,000 customers
• April 2010 – FTC begins investigation under Section 5
  • Wyndham spends over $5 million complying
• June 2012 – FTC initiates legal proceedings
• April 2014 – District court denies Wyndham’s motion to dismiss
• August 2015 – 3rd Circuit Affirms trial court
• December 2015 – Consent Decree
What is the legal standard?

• FTC contends the Court can evaluate the reasonableness of Hotels and Resorts’ data security program in view of the following guidance:

  • (1) industry guidance sources that Hotels and Resorts itself seems to measure its own data-security practices against; and

  • (2) the FTC’s business guidance brochure and consent orders from previous FTC enforcement actions.
Wyndham’s Alleged Cybersecurity Failures

• No firewalls
• Stored payment card info in clear readable text
• Did not require franchisees to have adequate information security policies and procedures
• Allowed franchisees to connect servers with outdated O/S’s
• Used “micros” as username and password for Micros Systems software
• No password policy or requirement for complex passwords
Wyndham’s Alleged Cyber Failures Continued

• Inadequate inventory of connected devices
• No intrusion detection system
• No access segmentation or access restriction or IP filtering
FTC’s Deception Claim

• Hotels and Resorts’ website represents, in part, that
  • “[w]e safeguard our Customers’ personally identifiable information by using industry standard practices” and make
  • “commercially reasonable efforts” to collect personally identifiable information “consistent with all applicable laws and regulations” and, among other things, that
  • “[w]e take commercially reasonable efforts to create and maintain ‘fire walls’ and other appropriate safeguards to ensure that to the extent we control the Information, the Information is used only as authorized by us and consistent with this Policy.”
Intrusion Detection System

- Network based intrusion detection attempts to identify unauthorized, illicit, and anomalous behavior based solely on network traffic.
- A network IDS, using either a network tap, span port, or hub collects packets that traverse a given network.
- Using the captured data, the IDS system processes and flags any suspicious traffic.
- Unlike an intrusion prevention system, an intrusion detection system does not actively block network traffic. The role of a network IDS is passive, only gathering, identifying, logging and alerting. Examples of Network IDS:
Demilitarized Zone (DMZ)

- Outer firewall b/t the Internet and the Web Server processing the requests originating on the company Web site.
- Inner firewall b/t the Web Server and the appl. Server to which it is forwarding requests. Data resides behind this.
Conclusion from FTV v Wyndham

• There is a baseline of minimum cybersecurity practices
• Look to industry guidelines and agency consent decrees
• A robust cybersecurity and risk mitigation program require periodic review and iteration to stay up to date with the latest
  • security software and
  • regulatory reports and tools for companies to map policies and practices
Glossary of Key Information Security Terms

Richard Kissel, Editor

http://dx.doi.org/10.6028/NIST.IR.7298r2
Is categorized as either secret key or public key. Secret key cryptography is based on the use of a single cryptographic key shared between two parties. The same key is used to encrypt and decrypt data. This key is kept secret by the two parties. Public key cryptography is a form of cryptography which makes use of two keys: a public key and a private key. The two keys are related but have the property that, given the public key, it is computationally infeasible to derive the private key [FIPS 140-1]. In a public key cryptosystem, each party has its own public/private key pair. The public key can be known by anyone; the private key is kept secret.

SOURCE: FIPS 191

Art or science concerning the principles, means, and methods for rendering plain information unintelligible and for restoring encrypted information to intelligible form.

SOURCE: CNSSI-4009

Cryptology – The science that deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence.

SOURCE: SP 800-60

The mathematical science that deals with cryptanalysis and cryptography.

SOURCE: CNSSI-4009

CVE – See Common Vulnerabilities and Exposures.

Cyber Attack – An attack, via cyberspace, targeting an enterprise’s use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.

SOURCE: CNSSI-4009

Cyber Incident – Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein. See Incident.

SOURCE: CNSSI-4009
Cyber Infrastructure – Includes electronic information and communications systems and services and the information contained in these systems and services. Information and communications systems and services are composed of all hardware and software that process, store, and communicate information, or any combination of all of these elements. Processing includes the creation, access, modification, and destruction of information. Storage includes paper, magnetic, electronic, and all other media types. Communications include sharing and distribution of information. For example: computer systems; control systems (e.g., supervisory control and data acquisition–SCADA); networks, such as the Internet; and cyber services (e.g., managed security services) are part of cyber infrastructure.

SOURCE: NISTIR 7628

Cybersecurity – The ability to protect or defend the use of cyberspace from cyber attacks.

SOURCE: CNSSI-4009

Cyberspace – A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

SOURCE: CNSSI-4009

Cyclical Redundancy Check – (CRC) A method to ensure data has not been altered after being sent through a communication channel.

SOURCE: SP 800-72

Error checking mechanism that verifies data integrity by computing a polynomial algorithm based checksum.

SOURCE: CNSSI-4009

Data – A subset of information in an electronic format that allows it to be retrieved or transmitted.

SOURCE: CNSSI-4009

Data Aggregation – Compilation of individual data systems and data that could result in the totality of the information being classified, or classified at a higher level, or of beneficial use to an adversary.

SOURCE: CNSSI-4009
Information Flow Control – Procedure to ensure that information transfers within an information system are not made in violation of the security policy.

SOURCE: CNSSI-4009

Information Management – The planning, budgeting, manipulating, and controlling of information throughout its life cycle.

SOURCE: CNSSI-4009

Information Operations (IO) – The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making process, information, and information systems while protecting our own.

SOURCE: CNSSI-4009

Information Owner – Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. See Information Steward.

SOURCE: FIPS 200; SP 800-37; SP 800-53; SP 800-60; SP 800-18

Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal.

SOURCE: CNSSI-4009

Information Resources – Information and related resources, such as personnel, equipment, funds, and information technology.

SOURCE: FIPS 200; FIPS 199; SP 800-53; SP 800-18; SP 800-60; 44 U.S.C., Sec. 3502; CNSSI-4009

Information Resources Management (IRM) – The planning, budgeting, organizing, directing, training, controlling, and management activities associated with the burden, collection, creation, use, and dissemination of information by agencies.

SOURCE: CNSSI-4009

Information Security – The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

SOURCE: SP 800-37; SP 800-53; SP 800-53A; SP 800-18; SP 800-60; CNSSI-4009; FIPS 200; FIPS 199; 44 U.S.C., Sec. 3542
Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

1) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

2) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

3) availability, which means ensuring timely and reliable access to and use of information.

**SOURCE:** SP 800-66; 44 U.S.C., Sec 3541

Information Security Architect – Individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization’s core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes.

**SOURCE:** SP 800-37

Information Security Architecture – An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise’s security processes, information security systems, personnel and organizational sub-units, showing their alignment with the enterprise’s mission and strategic plans.

**SOURCE:** SP 800-39

Information Security Continuous Monitoring (ISCM) – Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

[Note: The terms “continuous” and “ongoing” in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.]

**SOURCE:** SP 800-137

Information Security Continuous Monitoring (ISCM) Process – A process to:

- Define an ISCM strategy;
- Establish an ISCM program;
- Implement an ISCM program;
- Analyze data and Report findings;
- Respond to findings; and
- Review and Update the ISCM strategy and program.

**SOURCE:** SP 800-137
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal Identity Verification</strong></td>
<td>An individual who can act on behalf of an agency to authorize the issuance of a credential to an applicant.</td>
<td>CNSSI-4009</td>
</tr>
<tr>
<td><strong>Authorizing Official</strong></td>
<td>An individual who can act on behalf of an agency to authorize the issuance of a credential to an applicant.</td>
<td>CNSSI-4009</td>
</tr>
<tr>
<td><strong>Personal Identity Verification Card</strong></td>
<td>Physical artifact (e.g., identity card, “smart” card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation, etc.) such that a claimed identity of the cardholder may be verified against the stored credentials by another person (human-readable and verifiable) or an automated process (computer-readable and verifiable).</td>
<td>FIPS 201; CNSSI-4009</td>
</tr>
<tr>
<td><strong>(PIV Card)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Personal Identity Verification Issuer</strong></td>
<td>An authorized identity card creator that procures FIPS-approved blank identity cards, initializes them with appropriate software and data elements for the requested identity verification and access control application, personalizes the cards with the identity credentials of the authorized subjects, and delivers the personalized card to the authorized subjects along with appropriate instructions for protection and use.</td>
<td>FIPS 201</td>
</tr>
<tr>
<td><strong>Registrar</strong></td>
<td>An entity that establishes and vouches for the identity of an applicant to a PIV Issuer. The PIV RA authenticates the applicant’s identity by checking identity source documents and identity proofing, and that ensures a proper background check has been completed, before the credential is issued.</td>
<td>FIPS 201</td>
</tr>
<tr>
<td><strong>Sponsor</strong></td>
<td>An individual who can act on behalf of a department or agency to request a PIV Card for an applicant.</td>
<td>FIPS 201</td>
</tr>
<tr>
<td><strong>Personally Identifiable Information</strong></td>
<td>Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.</td>
<td>CNSSI-4009</td>
</tr>
<tr>
<td><strong>(PII)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.</strong></td>
<td>SP 800-122</td>
<td></td>
</tr>
<tr>
<td><strong>SOURCE: CNSSI-4009</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SOURCE: FIPS 201</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SOURCE: FIPS 201</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SOURCE: FIPS 201</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Privacy – Restricting access to subscriber or Relying Party information in accordance with federal law and agency policy.

SOURCE: SP 800-32

Privacy Impact Assessment (PIA) – An analysis of how information is handled: 1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; 2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and 3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

SOURCE: SP 800-53; SP 800-18; SP 800-122; CNSSI-4009; OMB Memorandum 03-22

Privacy System – Commercial encryption system that affords telecommunications limited protection to deter a casual listener, but cannot withstand a technically competent cryptanalytic attack.

SOURCE: CNSSI-4009

Private Key – The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.

SOURCE: SP 800-63

A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public. In an asymmetric (public) cryptosystem, the private key is associated with a public key. Depending on the algorithm, the private key may be used, for example, to:
- 1) Compute the corresponding public key,
- 2) Compute a digital signature that may be verified by the corresponding public key,
- 3) Decrypt keys that were encrypted by the corresponding public key, or
- 4) Compute a shared secret during a key-agreement transaction.

SOURCE: SP 800-57 Part 1

A cryptographic key used with a public key cryptographic algorithm, which is uniquely associated with an entity, and not made public; it is used to generate a digital signature; this key is mathematically linked with a corresponding public key.

SOURCE: FIPS 196

A cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public.

SOURCE: FIPS 140-2
Cybersecurity 2016

Contributing editors
Benjamin A Powell and Jason C Chipman
Wilmer Cutler Pickering Hale and Dorr LLP

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer-client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. Although the information provided is accurate as of January 2016, be advised that this is a developing area.

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112
## Global Overview

Benjamin A Powell, Jason C Chipman and Marik A String
Wilmer Cutler Pickering Hale and Dorr LLP

<table>
<thead>
<tr>
<th>Country</th>
<th>Page</th>
<th>Authors/Authors and Firms</th>
</tr>
</thead>
</table>
| Austria     | 6    | Árpád Geréd
Maybach Görg Lenneis & Partner |
| England & Wales | 11   | Michael Drury
BCL Burton Copeland |
| France      | 18   | Merav Griguer and Dominique de Combles de Nayves
Dunaud Clarenc Combles & Associés |
| Germany     | 22   | Svenja Arndt
ARNDT Rechtsanwaltsgesellschaft mbH |
| India       | 28   | Salman Waris
TechLegis, Advocates & Solicitors |
| Japan       | 33   | Masaya Hirano and Kazuyasu Shiraishi
TMI Associates |
| Korea       | 38   | Jin Hwan Kim, Brian Tae-Hyun Chung, Jennifer S Keh and Sung Min Kim
Kim & Chang |
| Malta       | 43   | Olga Finkel and Robert Zammit
WH Partners |
| Mexico      | 48   | Federico de Noriega Olea and Rodrigo Méndez Solís
Hogan Lovells BSTL, SC |
| Norway      | 53   | Christopher Sparre-Enger Clausen
Advokatfirmaet Thommessen AS |
| Sweden      | 58   | Jim Runsten and Ida Hägström
Synch Advokat AB |
| Switzerland | 63   | Michael Isler and Jürg Schneider
Walder Wyss Ltd |
| United Arab Emirates | 68 | Stuart Paterson, Benjamin Hopps and Nihar Lovell
Herbert Smith Freehills LLP |
| United States | 72 | Benjamin A Powell, Jason C Chipman and Leah Schloss
Wilmer Cutler Pickering Hale and Dorr LLP |
United States

Benjamin A Powell, Jason C Chipman and Leah Schloss
Wilmer Cutler Pickering Hale and Dorr LLP

Legal framework

1. Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

The United States generally addresses cybersecurity through sector-specific statutes, regulations and private industry requirements. At the federal level, numerous agencies impose cybersecurity standards through a variety of regulatory and enforcement mechanisms. For example, the Federal Information Security Management Act of 2002 (and implementing guidance) establishes cybersecurity standards for federal government agencies and their contractors. Similarly, the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) (and implementing regulations and agency guidance) require entities in the financial services and health sectors, respectively, to employ technical, administrative and physical safeguards to protect customer information from unauthorised access or use. Several states have also enacted state parallels to the GLBA and HIPAA requirements. The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide programme that provides a standardised approach to security assessments, authorisation and continuous monitoring for companies providing cloud services to federal civilian agencies.

In 2015, the Department of Defense (DoD) enacted a potentially significant interim rule (meaning that the rule is in effect but may be further refined when finalised) applicable to companies that do business with the US defence community. The new rule is a DoD regulation that establishes prescriptive cybersecurity requirements as part of the Defense Federal Acquisition Regulations Systems (DFARS), which mandates the use of cybersecurity-related contract clauses in all DoD contracts. These clauses are mandatory ‘flowdown’ terms to subcontractors at all tiers. The rule, which includes requirements with respect to security controls and cyber incident reporting, has been highly criticised by industry as being overly burdensome and in need of revision. The rule is currently in effect, but it was open to a public comment period, and may be changed through the standard regulatory process. In fact, DoD has already announced its intent to issue a new interim rule.

For companies handling consumer data, the Federal Trade Commission (FTC), the main federal consumer protection agency responsible for enforcing the prohibition on ‘unfair and deceptive acts or practices,’ frequently enforces minimum security requirements with respect to entities collecting, maintaining or storing personal information. In June 2013, the FTC issued ‘Start with Security’ guidance, which identifies the FTC’s lessons learned from 50+ data security enforcement actions brought by the FTC since 2001. This guidance advises companies to incorporate a series of 10 lessons learned, ranging from authentication controls to network segmentations.

For publicly-traded companies, the Sarbanes-Oxley Act of 2002 (SOX) and implementing regulations require publicly-traded companies to maintain a system of internal controls over financial reporting. Regulatory guidance has stated that ‘[m]anagement’s evaluation of the risk of misstatement [of financial reports] should include consideration of the vulnerability of the entity to fraudulent activity [...] and whether any such exposure could result in a material misstatement of the financial statements’. To meet these requirements, companies are audited to determine the extent to which they maintain a series of IT ‘general controls’ (ITGC) on systems designated as related to financial reporting.

Some subject-matter specific cybersecurity standards focus narrowly on a single constituency or a single government agency. For example, the Veterans Affairs Information Security Enhancement Act, passed in 2006 as part of the Veterans Benefits, Health Care, and Information Technology Act, requires the Department of Veterans Affairs (VA) to implement agency-wide information security procedures to protect sensitive personal information held by the VA and VA information systems. There are also numerous pending legislative proposals to regulate the security of certain sectors, including the automotive sector, data brokers and certain energy companies.

A handful of states have also adopted general security requirements that apply to companies conducting business in their state, collecting personal information about residents or citizens of their states, or both. A primary example is the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth. These regulations require companies collecting personal information about Massachusetts residents to develop written information security programmes containing administrative, technical and physical safeguards. Other states have enacted narrower requirements such as security requirements for particularly sensitive information (e.g. payment card data, mental health information, etc) and secure disposal requirements for electronic or paper media containing personal information.

In the criminal context, the Computer Fraud and Abuse Act (CFAA) outlawed intrusions into or interference with the security of a government computer network or other computers connected to the internet. In addition, several federal surveillance laws prohibit unauthorised eavesdropping on electronic communications, which can limit a variety of cybersecurity activities. For example, the Electronic Communications and Privacy Act (ECPA) prohibits unauthorised electronic eavesdropping. The Wiretap Act prevents the intentional interception, use or disclosure of wire, oral or electronic communication, unless an exception applies. The Stored Communications Act (SCA) precludes intentionally accessing without authorisation, a facility through which an electronic communication service is provided and thereby obtaining, altering or preventing authorised access to a wire or electronic communication while it is in electronic storage.

Beyond regulatory standards, many organisations are subject to voluntary standards or are required by contract to comply with cybersecurity requirements. Of particular note, the payment card industry in the United States establishes its own cybersecurity standards (the Payment Card Industry Data Security Standards (PCI-DSS)) that apply to merchants or vendors that process payment card data. The federal government has also focused substantially in recent years on the establishment of voluntary cybersecurity requirements, particularly for critical infrastructure entities, which are generally entities that provide vital services to a large part of the population. In 2013, the President issued Executive Order 13636, ‘Improving Critical Infrastructure Cybersecurity,’ to establish a process for the government to create voluntary cybersecurity standards applicable to critical infrastructure entities. Pursuant to this Executive Order, the National Institute of Standards and Technology (NIST) issued a voluntary ‘Cybersecurity Framework’, which provides a risk-based approach to cybersecurity, and references various national and international standards.
2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

In several respects, the financial services industry and the health-care sector are the most regulated sectors with regard to cybersecurity. Federal banking agencies promulgated several data security guidelines in 2000, including the ‘Interagency Guidelines Establishing Information Security Standards’. This guidance states that certain covered ‘financial institutions’ are required to implement comprehensive written information security programmes including administrative, technical and physical safeguards ‘appropriate to the size and complexity’ of the financial institutions and ‘the nature and scope of its activities’. The financial regulators, through the Federal Financial Institutions Examination Council (FFIEC), have also issued a series of booklets as part of the IT Examination Handbook, covering requirements ranging from information security to outsourcing technology services to management and governance. The Securities and Exchange Commission (SEC) has also issued guidance to public companies (as well as to the financial services institutions it regulates), and has articulated steps the SEC will take in the future to ensure cybersecurity preparedness in the securities sector. In the health-care sector, under HIPAA, the Department of Health and Human Services (HHS) has adopted security standards to protect individually identifiable health information.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

The United States has not adopted any international cybersecurity standards into law. However, NIST has created a ‘Cybersecurity Framework’, pursuant to Executive Order 13636, establishing voluntary standards applicable to critical infrastructure companies that incorporate many of these international benchmarks as examples of best practice to help US companies manage and reduce cybersecurity risks.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation’s protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

All directors and officers (D&O) owe their companies the fiduciary duties of care, loyalty and good faith. Given the broad-based impact of cybersecurity threats and data breaches on business viability and reputation, D&Os can no longer expect their company’s IT department to successfully manage these concerns in isolation. Instead, successful boards lead their organisations in addressing and incorporating cybersecurity concerns into all facets of business decision-making and processes.

Regulators, particularly in the financial services sector, have made clear that they expect board and management involvement in data security. For example, the financial sector Interagency Guidelines Establishing Information Security Standards provide that the board of directors or an appropriate committee of the board shall approve the entity’s written information security programme and oversee the development, implementation and maintenance of the programme, including assigning specific responsibility for its implementation and reviewing reports from management. Similarly, the FFIEC issued an updated version of the Management Booklet of its IT Examination Handbook in November 2015, which emphasises the importance of board oversight and management implementation of effective IT programmes, including IT security.

US corporate directors are, generally, not required by law to have specific expertise in cybersecurity areas. D&Os are generally responsible for proactively monitoring, managing and educating themselves on risks to the company, including cybersecurity risks and trends. Boards that fail to account for cybersecurity risks to a business may leave their companies vulnerable to a variety of civil litigation claims for failure to adequately maintain cyber and data protections, and prevent unauthorised access to consumer personal and financial information. In light of the growing emphasis on managing cybersecurity concerns, an increasing number of companies in the United States hire outside experts to report to the board on cybersecurity issues on a regular basis. In addition, boards are increasingly examining board committees to ensure that there is appropriate board oversight of the company’s data security and privacy procedures.

5 How does your jurisdiction define cybersecurity and cybercrime?

The United States lacks consistent and clear definitions for cybersecurity and cybercrime. In general, cybercrime is defined by the CFAA as accessing a protected computer without authorisation or exceeding authorised access to such protected computer. A ‘protected computer’ includes computers used in interstate communication, such as computers connected to the internet. ‘Cybersecurity’ is generally not defined in law, although DoD and the General Services Administration published recommendations in 2014 calling for common cybersecurity definitions for federal acquisitions in order to increase efficiency and effectiveness in the public and private sector.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

Industries vary with respect to the protective measures required to be taken to data breaches and data breaches. Both health-care and certain financial services entities have minimum requirements they are required to meet. However, these requirements are generally broad and do not include specific technical standards. For example, although HHS regulations identify a specific level of encryption that companies should use, companies are not required to use it. Instead, encrypting data provides a safe harbour for companies otherwise facing notice obligations in the event of a data security breach. Under the new DoD-mandated contract clauses, DoD contractors and subcontractors holding certain (broadly defined) categories of information (covered defence information) are required to comply with security requirements prescribed in NIST Special Publication 800-171, ‘Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,’ while DoD contractors and subcontractors providing IT services or cloud services are required to comply with other security requirements specified in the contract or in DoD cloud security guidance. Contractors providing cloud services to civilian government agencies under FedRAMP are also required to comply with certain cloud security requirements.

Merchants, payment processors and other parties dealing in payment cards, such as credit cards, are required to comply with various technical requirements under PCI-DSS, which are implemented via contract between parties and are not enacted into law. These standards include 12 categories of requirements that companies must meet with respect to the security of payment card information. Companies failing to comply risk fines from the payment card brands.

Apart from these mandatory standards, NIST’s Cybersecurity Framework created in response to Executive Order 13636 catalogues best practices for identifying, protecting, detecting, responding to and recovering from cybersecurity incidents by creating adaptable benchmarks and recommendations. While these standards are explicitly not mandatory, some have suggested that widespread adoption of this Framework by companies may result in the Framework representing a new ‘standard of care’ for US businesses generally.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Both the Digital Millennium Copyright Act and the CFAA prohibit certain cyberthreats to US intellectual property rights, including threats arising from cyber intrusions.

In addition, the federal government has issued two strategies under President Obama to address cyberthreats to US trade secrets and intellectual property rights. The ‘Strategy on Mitigating Theft of US Trade Secrets’ aims to protect US trade secrets abroad, promote voluntary best practices, enhance domestic law enforcement and improve legislation. The ‘Joint Strategic Plan on Intellectual Enforcement’ focuses on improving transparency in intellectual property policy and rulemaking, ensuring inter-agency coordination and securing US rights abroad.

Several pieces of pending legislation seek to protect US intellectual property rights and trade secrets from foreign governments and allegedly government-sponsored entities involved in hacking US computers and networks.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Some federal agencies in the United States have promulgated standards associated with protecting critical infrastructure entities from cyber intrusions. Of particular note, the Federal Energy Regulatory Commission (FERC) has established ‘Critical Infrastructure Protection Reliability Standards’ to address potential vulnerabilities in the bulk-electric system.
These standards require certain electricity grid ‘bulk-power’ system asset owners and operators to document, report and provide compliance evidence on a variety of security controls to the North American Electric Reliability Corporation (NERC) and FERC. They also require the characterisation of all cyber systems that influence the bulk-electric system as low, medium or high impact. In addition, these standards call for responsible entities to identify, assess and correct deficiencies in their cyber policies. Additionally, the Transportation Security Administration (TSA) has statutory authority to promulgate regulations related to pipeline physical security and cybersecurity, though it has not yet exercised this authority to issue cybersecurity requirements. And, as discussed above, the financial, health care and government contracting sectors are subject to regulatory or contractual requirements to implement administrative, technical and physical safeguards to prevent or mitigate a cyberattack.

The President of the United States has also issued Executive Order 13636, ‘Improving Critical Infrastructure Cybersecurity’, that calls for the enhancement of security measures to protect critical infrastructure. This Executive Order does not establish mandatory standards but, instead, requires the creation of minimum voluntary standards for the protection of critical infrastructure entities. In so doing, it attempts to balance efficiency, safety, privacy, business confidentiality and civil liberties in the cybersecurity realm. Pursuant to this Executive Order, NIST issued a voluntary ‘Cybersecurity Framework’, which provides a risk-based framework and identifies best practices for identifying, protecting, detecting, responding to and recovering from cybersecurity incidents. The Cybersecurity Act of 2015, which was enacted in December 2015, includes several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies, and marks the end of a multi-year effort to find a compromise between industry demands for liability protection for cybersecurity information-sharing and privacy concerns regarding government access to such information.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

In the United States, ECPA, which includes the SCA, restricts sharing of, and government access to, certain private electronic communications. ECPA includes three titles. Title I outlaws unlawful interceptions of wire, oral and electronic communications. Title II is the SCA, which restricts the disclosure of electronic communications held in electronic storage by third-party electronic communication and remote computing service providers. Title III regulates the use of pen registers or trap and trace devices, which are devices that can acquire metadata, such as phone numbers. Many states have similar laws against government and private wiretapping, some of which are even more stringent than the federal laws, including some states with two-party consent requirements for wiretapping.

The GLBA Privacy Requirements mandate that financial institutions give consumers privacy notices that explain the institution’s information-sharing practices. Consumers also have the right to opt-out and limit some of the information shared. Financial institutions must protect the information collected about individuals, except for information collected in business or commercial activities. Other statutes, such as the Right to Financial Privacy Act, restrict the sharing of certain financial information with the government, subject to several exceptions.

In the health-care sector, the HIPAA Privacy Rule protects all individually identifiable health information stored or transmitted by a covered entity or its business associate in any media. In particular, the HIPAA Privacy Rule regulates how covered entities use and disclose protected health information. It also creates limitations on the release of health records to third-parties, creates accountability through civil and criminal penalties and enables patients to determine how their information is used and whether any disclosures have been made.

The Cybersecurity Act of 2015, which was enacted in December 2015, includes several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies, and marks the end of a multi-year effort to find a compromise between industry demands for liability protection for cybersecurity information-sharing and privacy concerns regarding government access to such information.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

In general, a wide variety of criminal laws touch cybersecurity one way or another. For example, federal criminal statutes address the following activities, among others:
- computer hacking;
- identity theft;
- economic espionage;
- trade secret theft;
- breaking into computer systems and accessing, modifying or deleting data;
- stealing confidential information;
- defacing internet websites; and
- flooding websites with high volumes of irrelevant internet traffic to make websites unavailable to actual customers.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

There is no overarching framework for regulation of cloud computing information security. However, companies in several economic sectors, particularly the health, financial and government contracting sectors, are subject to guidance or regulations applicable to cloud security. In general, requirements for cloud security focus on the same basic issue: cloud computing is a species of outsourcing and a company moving data to the cloud remits responsibility for the secure handling of that data.

For example, HIPAA regulations require entities covered by HIPAA to execute a business associate agreement with their service providers (including cloud providers) if their service providers are being provided access to personal health records. These agreements subject the service provider to many of the same privacy and security restrictions as the initial covered entity. Similarly, the GLBA regulations and FFIEC guidance require financial services companies to exercise diligence and oversight over their third-party information technology providers, which include cloud providers.

In addition, FedRAMP is a government-wide programme that incorporates cloud computing into federal government civilian agencies’ IT capabilities through the authorisation and use of certified cloud computer providers. It also provides a standardised approach to securing cloud products and services. DoD has issued its own cloud security requirements, as well as special mandatory contractual clauses for DoD cloud service providers.

12 How do your jurisdiction’s cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Foreign organisations that do business in the United States are generally subject to state and federal laws to the same extent as US businesses operating in the same jurisdictions and collecting information about US individuals.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The NIST Cybersecurity Framework, issued in response to direction from Executive Order 13636, Improving Critical Infrastructure Cybersecurity, provides voluntary cybersecurity standards for protecting private sector computer networks owned or operated by critical infrastructure entities. NIST issued the first version of the Cybersecurity Framework in February 2014.

The Framework is divided into three parts: Framework Core, Implementation Tiers and Framework Profile. The Framework Core is designed to identify key cybersecurity activities common across all critical infrastructure networks. These are activities that companies should address when creating programs to protect critical computer systems and that identify best practices for communicating risks throughout an organisation. Specifically, the Framework Core consists of five functions designed to provide company decision-makers with a strategic view of cybersecurity risk management: identify, protect, detect, respond and recover.

For each function, the Framework identifies existing technical standards from NIST and other standards bodies to serve as ‘informative references’ in support of the technical implementation of the functions.
The Implementation Tiers provide context on how an organisation views cybersecurity risk and the processes in place to manage that risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigour and sophistication in cybersecurity risk management practices based on the business needs of the organisation.

The Framework Profile is intended to help organisations 'establish a roadmap' for prioritisation of organisational efforts to reduce cybersecurity risks. Organisations are encouraged to focus on identifying and eliminating gaps between the 'Current Profile,' which identifies cybersecurity outcomes currently being achieved, and the 'Target Profile,' which indicates the outcomes needed to achieve cybersecurity risk management goals.

14. How does the government incentivise organisations to improve their cybersecurity?

There have been numerous legislative proposals to develop incentives for organisations to improve their cybersecurity, including tying adoption of standards to incentives such as grants and streamlined regulation, or using tax credits, but, so far, these initiatives have not been passed or implemented.

The Cybersecurity Act of 2015, which was enacted in December 2015, includes several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies, and marks the end of a multi-year effort to find a compromise between industry demands for liability protection for cybersecurity, information-sharing and privacy concerns regarding government access to such information. Among other things, the Act provides liability protection for private sector entities to:
- monitor their own information systems, the information systems of another entity (with authorisation), and information on those information systems;
- operate ‘defensive measures’ applied to an entity’s own information systems or the information systems of another entity (with authorisation); and
- share and receive cyberthreat indicators or defensive measures from other entities, with no duty to warn or act based on information received.

15. Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

There are several cybersecurity standards applicable to specific industries. Of note are:
- the NIST Cybersecurity Framework, which establishes a voluntary standard for promoting cybersecurity. It can be accessed at www.nist.gov/cyberframework/;
- for financial institutions, the FFIEC has issued an Information Security Handbook that outlines audit guidelines for reviewing financial institutions’ security practices, effectively providing best practices to protect against security breaches. It can be accessed at http://it handbook.ffiec.gov /cybersecurity-framework/
- the PCI-DSS establish standards applicable to merchants or vendors that process payment card data. The current version of these standards (version 3.1, adopted in April 2015) can be found at www.pcisecuritystandards.org/documents/PCI_DSS_v3.1.pdf; and
- a recently enacted set of standards applicable to certain defence contractors was established in late 2015 through amendments to the DFARS, which mandates the use of cybersecurity-related contract clauses for all DoD contracts. This new rule, which includes requirements with respect to security controls and cyber incident reporting, has been highly criticised by industry as being overly burdensome and in need of revision. The rule is currently in effect, but it was open to a public comment period, and may be changed through the standard regulatory process.

16. Are there generally recommended best practices and procedures for responding to breaches?

Guidance from NIST and other independent organisations generally recommends several key actions immediately after learning of a data security breach. Communication is of particular importance, both among company leadership and with key constituencies. Effective breach response often includes an incident response team made up of forensic experts and key personnel who can address legal, public relations, investor relations and SEC, insurance, IT, audit and customer concerns. Most breaches require a coordinated effort to gather the facts through forensic analysis. At the same time, company leaders may need to develop a strategy to respond to the incident. Outside experts often serve important roles in this regard. External counsel can help guide the response to a breach and can structure a forensic investigation in a manner that preserves legal privileges. Outside forensic experts may be necessary to bring special skills to the response and to ensure that company personnel have appropriate resources to address the situation.

17. Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

The Cybersecurity Act of 2015, which was enacted in December 2015, includes several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies, and marks the end of a multi-year effort to find a compromise between industry demands for liability protection for cybersecurity information-sharing and privacy concerns regarding government access to such information.

The Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance programme is a voluntary cybersecurity information-sharing programme between DoD and eligible DIB companies. Companies in the programme receive certain threat information in return for sharing information regarding network intrusions that could compromise critical DoD programmes and missions. The rule establishing this programme was recently modified to conform with the newly issued DFARS rule (though, as with the DFARS rule, these changes were subject to comment and may be revised through the normal regulatory process).

Several industries have developed information sharing and analysis centres (ISACs) designed to share intelligence on cyber incidents, thereby raising awareness of vulnerabilities and associated responses present throughout the industries. The National Council of ISACs recognises the following centres: aviation, defence industrial base, emergency services, electric sector, financial services, information technology, maritime security, multi-state, communications, national health, nuclear, oil and gas, public transit, real estate, research and education, supply chain, surface transportation and water. In the wake of the recent increase in retail breaches, a new retail ISAC has also been established. US law firms and the automotive industry have also recently announced the establishment of industry ISACs.

Organisations may also choose to voluntarily share information with federal and state law enforcement and the Department of Homeland Security (DHS) to aid in the investigation and prosecution of criminal cybersecurity attacks.

18. How do the government and private sector cooperate to develop cybersecurity standards and procedures?

DHS, the Federal Bureau of Investigation (FBI), and DoD all have established information-sharing programs aimed at encouraging the private sector to share information about cyber threats, such as indicators of compromise. Likewise, the NIST Framework is intended to be a voluntary, industry-led standard that applies to all critical infrastructure sectors. In developing the framework, NIST issued a draft framework, engaged stakeholders at cybersecurity framework workshops and solicited feedback and suggestions for the final framework. NIST continues to update and improve the framework as industry provides feedback on implementation. Additionally, the Cybersecurity Act of 2015, which was enacted in December 2015, includes several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies, and marks the end of a multi-year effort to find a compromise between industry demands for liability protection for cybersecurity information-sharing and privacy concerns regarding government access to such information.

19. Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

Insurance for cybersecurity breaches is available in the United States, and is becoming far more common for companies to have, particularly in the wake of judicial opinions finding that general insurance policies do not cover cybersecurity breaches. DHS has worked with public and private sector stakeholders to examine the current cybersecurity insurance market and develop solutions to advance its capacity to incentivise better cyber risk management.
Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

Enforcement of cybersecurity rules and standards falls to a variety of federal and state agencies. Various state attorneys general have initiated investigations of major data breaches and in some cases a group of US state attorneys generals have joined together to initiate multi-state investigations of data breaches. At the federal level, the US Secret Service (Electronic Crimes Task Forces and Cyber Intelligence Section), FBI and DHS play leading roles in identifying and investigating cyber breaches. The SEC also requires disclosure of material cyber risk and incidents, and has initiated several investigations relating to cyber incidents and information security. The FTC has also investigated companies for failing to protect consumers’ personal information and take reasonable cybersecurity steps. The FTC has reached over 50 settlements of enforcement actions related to the alleged failure of companies to take reasonable data security measures. HHS also has authority to investigate data breaches involving medical patient information. The US Congress has also initiated its own investigations into prominent data breaches.

21 Describe the authorities’ powers to monitor compliance, conduct investigations and prosecute infringements.

US federal and state authorities have wide-ranging authorities to monitor compliance, conduct investigations and prosecute infringements under numerous state and federal statutes. This includes the authority to demand documents and testimony, pursuant to legal process and other information relating to cybersecurity incidents.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

The most common enforcement actions are based on allegations of insufficient cybersecurity practices and failure to disclose breaches involving consumer information. The FTC has an active enforcement programme examining companies that allegedly did not take ‘reasonable’ steps to protect consumer information. The FTC frequently seeks long-term consent agreements with companies that impose cybersecurity obligations. Such obligations may run for decades and require companies at their own expense to take certain security steps and have outside independent audits of the companies’ compliance with the consent agreement. Individual state attorneys general have also initiated investigations and obtained settlements relating to the loss of consumer data. The SEC has sent a variety of letters to corporations requesting information on past cyber incidents. The private sector has responded through the creation of best practices, and NIST released a cybersecurity framework for private industry in early 2014.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The most common penalties for failing to comply with cybersecurity-related regulations are related to the entry into consent orders with the federal or state government, class action lawsuits, civil penalties and payment card industry compliance fees (designed to ensure that credit card information is securely maintained). Other potential penalties include cease and desist orders; criminal penalties; limitations on activities, functions, and operations; registration revocations; and termination of insurance.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Penalties that may be imposed for failure to comply with the rules on reporting threats and breaches include civil enforcement penalties and monetary judgments through litigation.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Depending on the facts of a specific situation, parties may seek private redress under a variety of causes of action, including approximately 34 separate tort claims, 15 contract claims, and other claims based on state and federal statutes. In particular, numerous state data breach notice laws contain individual rights of action, and consumers have brought class actions in response to data breaches involving sensitive personal information.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

There are currently no policies or procedures that all organisations must have in place to protect against cyberthreats. However, there are numerous federal and state laws, regulations and mandatory standards that pertain to securing privately owned IT systems and data in the United States’ critical infrastructure sectors, resulting in a patchwork of regulatory requirements organisations must follow.

For instance, organisations performing contracts requiring a security clearance from the US government generally are covered by the National Industrial Security Program and are obligated to follow the National Industrial Security Program Operating Manual (NISPOM). The NISPOM includes a wide range of information system security requirements, including identification and authentication management, passwords and scanning for malicious code. Other defence contractors and subcontractors at all tiers are also required to comply with various security requirements under the new DoD rule.

Covered entities under HIPAA must implement technical policies that allow only authorised persons to access electronic protected health information and have measures that guard against unauthorised access to electronic protected health information when it is transmitted over an electronic network.

Under the GLBA, financial institutions are required to identify and control risks to customer information and customer information systems and to properly dispose of customer information. Appropriate measures to the institutions must take include access controls on customer information systems and monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.

The main example of a state law requiring companies to develop policies and procedures to protect data and systems from cyberthreat is the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, which requires companies collecting personal information of Massachusetts residents to develop written information security programmes containing administrative, technical and physical safeguards that protect personal information.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Currently there are no broad rules requiring all organisations to keep records of cyberthreats or attacks. Organisations within certain critical infrastructure sectors may be subject to sector-specific rules. For example, the new DoD rule requires companies to report cyber incidents affecting ‘covered defence information’ to DoD, and to maintain forensic evidence (including forensic images and packet captures) for 90 days in the event DoD decides to conduct a further review and requests that evidence. Additionally, companies subject to the PCI-DSS are required to maintain certain log and other forensic data for a period of time to facilitate forensic review and audit.

Because cybersecurity breaches may require disclosure and result in litigation or regulatory enforcement, organisations should be aware that they may be required to provide forensic evidence and information about any such attacks. Organisations should maintain records accordingly (consistent with standard preservation practices).

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Numerous federal and state regulations require organisations to report cybersecurity breaches to regulatory authorities.

Public companies may be required to disclose, through public filings with the SEC, material breaches that affect the company’s products, services, relationships with customers or suppliers, competitive conditions or financial controls.

Defence contractors with ‘covered defence information’ on their systems that experience a cybersecurity breach must report the breach to DoD.

Organisations covered by HIPAA are required to notify the Secretary of HHS following a breach of unsecured protected health information.

Most states also have enacted state data breach notice legislation, many of which require organisations to notify state attorneys general and other state regulatory agencies of security breaches involving sensitive
personally identifiable information that affect individuals in the state. Many of these states also require additional notice to individuals and, at times, the media, consumer credit reporting agencies, or both, of certain breaches that result in the loss of personally identifying information.

29 What is the timeline for reporting to the authorities?

Public companies may disclose material breaches to the SEC through a Form 8-K, the ‘current report’ companies must file with the SEC to announce major events that shareholders should know about. Depending on timing, these breaches may instead be reported in typical quarterly or annual securities filings.

For breaches that affect covered defence information, reports must be sent to DoD via http://dibnet.dod.mil/ within 72 hours of discovery of any cyber incident and must include specific, detailed data about the nature of the intrusion and any government projects possibly implicated. For breaches related to unsecured protected health information that affect 500 or more individuals, HIPAA-covered organisations are required to notify the Secretary of HHS without unreasonable delay, and in any case no later than 60 days after a breach. For breaches that affect fewer than 500 individuals, the Secretary may be notified of such breaches on an annual basis.

For notification to states regarding breaches affecting individuals in that state, most state laws require notification be made without undue delay and in the most expedient time possible, though some states include specific time frames.

Companies may also report breaches to law enforcement agencies, which the FTC has stated will be regarded favourably when considering whether to bring an enforcement action against a company.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Most states require organisations to report security breaches involving personally identifiable information to individuals whose information was affected. Each state has its own rules, but typical requirements include that the notification be made in writing in the most expedient time possible. At the federal level, HIPAA and the GLBA require covered entities to report breaches of sensitive health or financial information, respectively. Many state data breach laws include an exception for entities complying with these federal obligations.

Update and trends

Legislators and regulators in the United States remain keenly focused on improving cybersecurity of critical infrastructure systems that are largely perceived as too vulnerable to cyberthreats. Although pressure will continue to grow to establish more uniform and clear cybersecurity standards, a consensus on how to craft such standards is likely to remain elusive. Some political leaders are advocating for regulatory mandates, and others are looking for industry-driven solutions to cybersecurity challenges. In the absence of any broad consensus for how to establish better cybersecurity standards, Federal agencies in the United States are likely to continue efforts to craft more aggressive cybersecurity regulatory requirements applicable to particular economic sectors, such as recent DoD efforts in the United States to impose far-reaching cybersecurity standards on companies operating in the defence sector. Legislative action in the near term will almost certainly steer clear of establishing mandatory cybersecurity requirements, and will instead focus on creating incentives for private sector entities to share cyberthreat data more freely with one another and with the government.
LEARN ABOUT the best practices, organizational roles, and experiences of in-house counsel in more than 800 organizations.

FIND OUT HOW top in-house lawyers mitigate the threat of breaches and safeguard their data.

DISCOVER INSIGHT from over 1,000 in-house lawyers in 30 countries.
The ACC Foundation wishes to acknowledge with gratitude the contributions of Ballard Spahr LLP for its underwriting support of the *State of Cybersecurity Report*.

---

**Ballard Spahr LLP**

The ACC Foundation also wishes to recognize the following members of cybersecurity project advisory group for their contributions to the development of the *State of Cybersecurity Report*:

Phil N. Yanella, Ballard Spahr LLP
Kim Phan, Ballard Spahr LLP
Edward J. Willey III, Dallas, TX
Kerry L. Childe, Richfield, MN
Neal Dittersdorf, Intersections Inc.
Jandria S. Alexander, The Aerospace Corporation
Companies process more information about their customers than ever before. And the consequences if that information is lost or inadvertently disclosed can be catastrophic. Our cross-disciplinary team of attorneys helps clients around the world mitigate risk, respond in the event of a crisis, and recover.

- Information Risk Management
- Asset Inventories
- Employee Training
- Transactions/Vendor Management
- Privacy and Consumer Marketing Compliance
- Data Incident Response Plans
- Network Intrusion/Data Breach Response
- Litigation
- Investigations
- Plan Assessment
TABLE OF CONTENTS

| Introduction | 3 |
| Key Findings | 5 |
| Project Overview & Interpreting the Data | 9 |
| Executive Summary (full report only) | 11 |
| Industry Trends (full report only) | 30 |
| Overall Results (full report only) | 38 |

- Top concerns related to cybersecurity | 39 |
- Experienced a data breach | 41 |
- Year of breach | 43 |
- How did you find out about the breach? | 45 |
- Comments from experienced in-house counsel: | 47 |
- What you wish you’d known before breach? | 49 |
- In-house counsel responsibilities regarding cybersecurity | 51 |
- Types of data security specialists employed by company | 53 |
- Location of cybersecurity central operations in company | 55 |
- Frequency company conducts cybersecurity audits | 57 |
- Entity conducted most recent cybersecurity audit | 59 |
- Audit of legal service providers for cybersecurity risk | 61 |
- Cybersecurity standards used in company | 63 |
- Cybersecurity policies in company | 65 |
- Legal department’s role on data breach response team | 67 |
- Cyber insurance | 69 |
- Amount of cybersecurity insurance coverage | 71 |
- Confidence in cybersecurity insurance coverage | 73 |
- Determining the amount of coverage needed | 75 |
- Expectations for changes in cyber insurance coverage over next year | 77 |
- Employee training | 79 |
- Evaluating preparedness at employee level | 81 |
- Retention of forensic company | 83 |
- Retention of outside counsel | 85 |
- Frequency legal department briefs board of directors on cybersecurity | 87 |
- Preference regarding cybersecurity role and responsibilities | 89 |
- Expectations of legal department’s cybersecurity role over the next year | 91 |
- Confidence third-parties are protecting company from cybersecurity risk | 93 |
- Confidence outside law firms are appropriately managing data security | 95 |
- Third party notification requirements (cybersecurity risks/breaches) | 97 |
- Termination of contractual relationship due to cybersecurity risks | 99 |
- Termination of pending merger/acquisition due to cybersecurity risks | 101 |
- Cybersecurity budget allocation trends | 103 |
- Law department spend changes related to cybersecurity | 105 |
- Allocation of increase in law department spend on cybersecurity | 107 |
- Law department budget dedicated to cybersecurity | 109 |
- First executive officer to be notified when breach discovered | 111 |
- From whom do you expect to be notified of a data breach? | 113 |
- Company primary point of contact during a breach | 115 |
- Company collaborates with law enforcement/other government agencies to address cybersecurity risks? | 117 |
- How was the system breached? | 119 |
- Type of information compromised during a breach | 121 |
- Role of encryption on breach incidence | 123 |
- Public notice | 125 |
- Regulatory/governmental notification | 127 |
- Comments from experienced in-house counsel: | 129 |
- Challenges faced in preserving lawyer-client privilege after a data breach and how to navigate them | 131 |
- Number affected by the breach | 133 |
- Length of time to resolve breach | 135 |
- Comments from experienced in-house counsel: | 137 |
- Resource most helpful in managing breach response | 139 |
- Degree of change made to company policies post-breach | 141 |
- Comments from experienced in-house counsel: | 143 |
- Lessons learned and changes made following breach | 145 |
- Insurance coverage of breach damages | 147 |
- Best practices: Comments from experienced in-house counsel on best practices to manage cybersecurity risk and/or a breach | 149 |
- Demographic Profile | 151 |
- Glossary of Key Terms | 153 |
The State of Cybersecurity Report is a special study published by the Association of Corporate Counsel (ACC) Foundation. The ACC Foundation — a 501(c)(3) nonprofit organization — supports the efforts of the Association of Corporate Counsel, serving the needs of the more than 40,000 corporate lawyers employed by over 10,000 organizations in 85 countries. Through the dissemination of cutting-edge research and surveys, the ACC Foundation developed an unprecedented study of the state of cybersecurity in the corporate sector. Considering the increasingly active role general counsel play in cybersecurity strategy, risk assessment, and prevention, this report provides insight from more than 1,000 corporate lawyers. The largest study of its kind, the report aims to serve as a resource for corporations, lawyers, board of directors, and members of the public affected by one of the greatest challenges organizations face today — cybersecurity.

In an environment where data breaches are largely an inevitability, assiduous preparation is key. Threats to an organization’s information security are as varied as they are dangerous. Preventing, preparing, and responding to data breaches in real time is a chief concern for today’s general counsel (GC) and chief legal officers (CLOs), who are increasingly called on to guide their organizations and aid with thwarting such attacks. Knowing common practices, what works, and what your peers are doing is key in benchmarking and planning to protect your company from risk. Straddling business, IT, and legal, today’s GC/CLOs are uniquely positioned to engage the multiple stakeholders that a robust data protection regime requires. Execution of incident response plans, protection of privilege, and compliance and notification requirements arising from a breach — these are just some of the unique functions that legal is charged with to manage when data is compromised or lost. And with one in four CLOs/GC reporting a breach in the last two years, the damage and repercussions of major cybersecurity incidents will heighten the legal department’s role in strategic planning and risk management as well as in responding to cybersecurity-related incidents.

Consumer exposure and privacy concerns have begun to weigh on government agencies and regulators as well. European regulators struck down the longstanding international Safe Harbor agreement, which had enabled American companies working in the European Union to transfer data painlessly. Various data protection bills are working their way through the US Congress, including the Cybersecurity Information Sharing Act recently passed by the Senate. And at a time of tension between the world’s largest economies over cybersecurity in general, the United States and China held a cybersecurity summit in September 2015, pledging to ease off the burgeoning Internet arms race. Dealing with the dual threats of breach preparedness and compliance with cybersecurity laws is not trivial—it’s no wonder that data security is one of the leading issues that keep in-house counsel up at night.

The 2015 ACC Global Census of more than 5,000 in-house counsel in 73 countries found that in-house counsel considered cybersecurity one of the greatest challenges in complying with laws inside their jurisdiction, just behind privacy concerns, which ranked number one among all concerns.\(^2\) In short, data security is top of mind for in-house counsel. And rightly so — data theft is a growing risk. No single metric can capture the immense cost of data breaches, but by any measure they represent a large and growing threat to virtually any company doing business today. The Center for Strategic and International Studies estimates that “the likely annual cost to the global economy from cybercrime is more than US $400 billion.”\(^3\)

Additionally, the average cost incurred per stolen record increased in 2015. The Ponemon Institute in its Cost of Data Breach Study: Global Analysis found that the average consolidated total cost of a data breach has risen 23 percent since 2013, clocking in at US $3.8 million.\(^4\) And the average cost for each stolen record has risen as well. Costs per stolen record have risen due to mounting financial consequences of losing customers due to security incidents — likely due to high-profile news reports and consumers’ increasing concern over the vulnerability of their data. Expenditures related to class-action lawsuits, compliance, damages, crisis management, and the necessity of forensic activities related to malicious data breaches have contributed to this rise in cost per compromised record as well.

No form of data is safe. Cybercriminals have come to value data that might otherwise seem difficult to monetize, such as personally identifiable information (PII), as it can be sold to third parties who specialize in exploiting such records. Data thieves have come to value data useful for long-term, insidious identity theft schemes over the “smash and grab” credit-card plots of yesteryear. Once compromised, it can take individuals years to recover and secure their information — or even to notice that it has been stolen in the first place. As such, safeguarding PII is a vital practice in maintaining the trust of the general public and regulators.

As more and more business data storage moves into cloud data storage servers, hackers have an ever-expanding trove of enterprise data to plunder. The theft of intellectual property has especially pernicious effects for industries that depend on intellectual property (IP) protection. It disproportionately affects market leaders that invest in research and development, and it discourages innovation. Corporations must now contend with increasingly sophisticated and well-resourced actors—targeting organizations rich in IP for strategic purposes or for competitors seeking to close the gap in proprietary manufacturing processes.

In keeping with the ACC Foundation’s goal of generating the most comprehensive reports of its kind, and capturing as large a segment of the in-house counsel population as possible, we have surveyed mainly GC and CLOs\(^5\) — hailing from 887 organizations in 30 countries — to chronicle information about cyber-related events that are not normally available to the public. The State of Cybersecurity Report therefore captures the thoughts of an unprecedented record number of in-house counsel. This survey also reveals best practices for preparation, crisis management, and breach response. Read on to find out what worked and what didn’t, why breaches happen, how to prepare, and how to react.

---

\(^2\)Net Losses: Estimating the Global Cost of Cybercrime, June 2014. Center for Strategic and International Studies
\(^4\)GC and CLOs constituted 77 percent of the total set of respondents for a total of 776 GC/CLOs
KEY FINDINGS
Employee error is the number-one cited cause of breaches

Employee error is the most common reason for a breach. And while nearly half of all in-house counsel say that mandatory training exists, few have a policy of testing knowledge or tracking attendance at these trainings. Lawyers in Canada are least likely to say their company has mandatory employee training (29 percent) compared with those in the US, which has the highest percentage reporting so (48 percent). Overall, 17 percent of in-house counsel say the data accessed during a breach was encrypted.

Thirty-six percent of all respondents reported employee error as the cause of a system breach when an audit was conducted by an outside auditor compared with 26 percent of respondents when an audit was conducted by internal staff.

Reputation: the top concern worldwide when it comes to cybersecurity

Top concerns cited by in-house counsel include damage to reputation, loss of proprietary information, and economic damage. In Europe, the Middle East and Africa (EMEA), and Asia Pacific regions, government and regulatory action made the top three most cited primary concerns.

Data breaches are a reality for many

Nearly one in three in-house counsel have experienced a data breach at their company. Nineteen percent say their current company has experienced a data breach, while 10 percent say their former employer did. Nearly half (47 percent) have recent experience, reporting the breach took place in 2014 or 2015. Forty-five percent of in-house counsel in companies with 5,000 or more employees say they either work or have worked at a company that experienced such a breach.

Company and legal department budgets are growing when it comes to cybersecurity

Despite an overall trend toward insourcing, cybersecurity spend seems to be the exception for most law departments. Fifty-six percent of GC and CLOs say their company is allocating more money to cybersecurity than one year ago, and 23 percent say their legal department spend has increased as a result of company focus on cybersecurity. Among GC/CLOs who report an increase in departmental spend, 53 percent say this is mainly outside spend, and 24 percent report spend as equally split between inside and outside. Notably, just 8 percent of GC/CLOs have a portion of their departmental budget explicitly dedicated to cybersecurity-related issues despite the growing role of the legal department.

The expanding role of legal in the cyber arena

Fifty percent of all GC and CLOs want to increase their role and responsibilities when it comes to cybersecurity. Though oversight of cyber-risk continues to sit firmly in the IT department, the legal role is also expanding, with 57 percent of GC and CLOs expecting their department’s role to increase in the coming year.

Cybersecurity insurance is becoming more common, and amount of coverage is rising

Half of all GC and CLOs surveyed say their company has cybersecurity insurance, and for companies that have this insurance, 68 percent have coverage valued at US $1 million or more. One in four say they expect their company to increase coverage in the coming year, while 58 percent expect it to remain the same. Barely 1 percent expect a decrease in cybersecurity coverage amounts. Among those who have experienced a breach, just 19 percent say the insurance policy fully covered the related damages.

Managing outside risk plays a significant role in preparing and preventing

With only 61 percent of GC/CLOs confirming that third parties are required to notify them should a breach occur, it appears outside support and risk are high for many companies. Just one in four report that their company has retained a forensic company, and one in three have retained outside counsel to help should a cybersecurity event occur. This leaves companies searching for outside support in many instances where data has been compromised. And just 7 percent of all in-house counsel surveyed are very confident that their third-party vendors and affiliates are protecting the company from cybersecurity risks. Twenty-two percent are very confident their outside service providers are managing the security of client data.
Industry trends

The healthcare industry continues to see the highest percentage of in-house counsel reporting they have experienced a data breach. Over half in the healthcare and social assistance industry say they have experienced a breach at their current or former employer compared with 31 percent of corporate counsel on average across all industries. In-house lawyers in the healthcare industry (75 percent) are most likely to report that their company has cybersecurity insurance. In-house counsel in the healthcare industry are also most likely to say their vendors and third-party agents are required to notify them of a breach (88 percent). Corporate lawyers in the retail industry have the highest percentage reporting that they proactively collaborate with law enforcement or other government agencies to address cybersecurity risks (45 percent).

Waiting to change until after the breach can be costly

We are clearly observing a dramatic increase in budget allocation toward cybersecurity issues across companies and legal departments. A major reason may be due to the lack of prevention strategies implemented. Among those who have experienced a data breach, 74 percent say that their company is making at least some changes to their security policies as a result of the breach, and 58 percent report making moderate to significant changes.

Benchmarking the state of cybersecurity

Key variables in prevention, preparedness, and response cross organizational boundaries and functional areas. However, several items related to the legal department, both directly and indirectly, are excellent benchmarks for evaluating preparedness. The checklist in this section provides a summary of these items. Inside the report, benchmarks from more than 800 organizations can be found along with this checklist for comparison purposes. These items are commonly recommended as foundational best practices for the prevention or preparation of a data breach. While few have all of the items listed, it is useful to examine your practices in comparison and take steps to plan for data security.

Sample cybersecurity checklist with benchmarks.

See full report for complete benchmarking checklist.

Organizational Policies

- Password policy
- Social media policy
- Document retention policy

“I wish we had done a better job at educating employees on cybersecurity issues, how to recognize and what to do and to become more informed on various ways that data breaches occur and proactive ways that could eliminate or reduce exposure.”
### Cybersecurity Checklist

#### Self-Assessment Tool

<table>
<thead>
<tr>
<th><strong>Organizational Prevention and Preparedness</strong></th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization conducts a cybersecurity audit of the entire organization at least annually</td>
<td></td>
</tr>
<tr>
<td>A member of the legal department is on the company's data breach response team</td>
<td></td>
</tr>
<tr>
<td>Organization has cybersecurity insurance</td>
<td></td>
</tr>
<tr>
<td>Organization has mandatory training on cybersecurity for all employees</td>
<td></td>
</tr>
<tr>
<td>Organization tests employee preparedness/knowledge of cybersafety practices/data policies at least annually</td>
<td></td>
</tr>
<tr>
<td>Organization retained outside counsel to assist you should a breach occur</td>
<td></td>
</tr>
<tr>
<td>Company collaborates proactively with law enforcement or other governmental agencies to address cybersecurity risks</td>
<td></td>
</tr>
<tr>
<td>Organization retains a forensic company to assist should a breach occur</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Organizational Policies</strong></th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password policy</td>
<td></td>
</tr>
<tr>
<td>Social media policy</td>
<td></td>
</tr>
<tr>
<td>Document retention policy</td>
<td></td>
</tr>
<tr>
<td>Website privacy policy</td>
<td></td>
</tr>
<tr>
<td>Employee manual acceptance policy</td>
<td></td>
</tr>
<tr>
<td>Internet privacy policy</td>
<td></td>
</tr>
<tr>
<td>Identity and access management</td>
<td></td>
</tr>
<tr>
<td>BYOD policy</td>
<td></td>
</tr>
<tr>
<td>Data map</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Organizational Staffing</strong></th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Information Officer (CIO)</td>
<td></td>
</tr>
<tr>
<td>Privacy/Security Manager</td>
<td></td>
</tr>
<tr>
<td>Chief Information Security Officer (CISO)</td>
<td></td>
</tr>
<tr>
<td>Chief Risk Officer (CRO)</td>
<td></td>
</tr>
<tr>
<td>Chief Privacy Officer (CPO)</td>
<td></td>
</tr>
<tr>
<td>Chief Security Officer (CSO)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Organizational Preparedness Evaluation</strong></th>
<th>✓</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conduct cybersecurity audit of entire organization at least annually</td>
<td></td>
</tr>
<tr>
<td>Use a standard (e.g., SSAE, NIST, ISO) to prepare for, manage, and reduce cybersecurity risk</td>
<td></td>
</tr>
<tr>
<td>Track mandatory training requirement and attendance for all employees</td>
<td></td>
</tr>
<tr>
<td>Test employees' knowledge of mandatory training</td>
<td></td>
</tr>
<tr>
<td>Conduct mock security event</td>
<td></td>
</tr>
<tr>
<td>Conduct tabletop exercises</td>
<td></td>
</tr>
<tr>
<td>Review disciplinary actions for violations</td>
<td></td>
</tr>
</tbody>
</table>
PROJECT OVERVIEW & INTERPRETING THE DATA
Project Overview

This survey opened on August 31, 2015, and closed October 10, 2015. An email invitation to participate in the survey was delivered to 15,176 chief legal officers, general counsel, and assistant general counsel. Those holding the title of group general counsel and head of legal are included in the GC/CLO sample. The population includes members of ACC and nonmembers. A total of 1,015 responses were received; 760 were from ACC members, and 255 were from nonmembers. This represents an overall response rate of 7 percent. Seventy-seven percent identified as GC/CLO, and 14 percent are assistant general counsel. The remainder hold other titles not included in the GC/CLO group. Those not in the GC/CLO or AGC role may have been invited to complete the survey by their GC, CLO, or AGC on behalf of their organization. Participants represent 887 unique organizations as determined by their email address and/or pre-identified employer.

Interpreting the Data

The full report contains an introduction, key findings, executive report, and overall results. Although many pertinent topics are covered in the key findings, other thought-provoking findings are exhibited in the overall survey results. Overall results touch upon all survey questions, and responses from all respondents are stratified by a number of relevant segments such as region/country; industry; company revenue; number of employees in the company; department size; GC/CLOs and those with other titles; ever worked where a cybersecurity breach has occurred; and company domestic only or global. By analyzing responses in this way, we are able to decrease the influence of overrepresentation across audience segments. Cross-tabulations were conducted in order to assess the influence of these segments of the survey population, and t-tests were used when appropriate to determine whether differences between groups or between time points were statistically significant at the .05 a level.
for further consideration of Sprauve’s and Smith’s claims consistent with this opinion.

FEDERAL TRADE COMMISSION

v.

WYNDHAM WORLDWIDE CORPORATION, a Delaware Corporation Wyndham Hotel Group, LLC, a Delaware limited liability company; Wyndham Hotels and Resorts, LLC, a Delaware limited liability company; Wyndham Hotel Management Incorporated, a Delaware Corporation Wyndham Hotels and Resorts, LLC, Appellant.

No. 14–3514.

United States Court of Appeals,
Third Circuit.


Holdings: The Court of Appeals, Ambro, Circuit Judge, held that:

(1) company’s alleged failure to maintain reasonable and appropriate data security, if proven, could constitute an unfair method of competition in commerce;

(2) subsequent Congressional acts did not cause Federal Trade Commission Act provision prohibiting unfair practices to exclude cybersecurity issues; and

(3) company had fair notice of meaning of provision of Act prohibiting unfair practices.

Affirmed.

1. Federal Courts


2. Antitrust and Trade Regulation


3. Antitrust and Trade Regulation

It is not a necessary condition that a practice be unscrupulous or unethical in order for that practice to constitute an unfair method of competition in commerce in violation of the Federal Trade Commission Act. Federal Trade Commission Act, §§ 5(a), 5(n), 15 U.S.C.A. §§ 45(a), 45(n).

4. Antitrust and Trade Regulation

5. Antitrust and Trade Regulation

$\Rightarrow 138$

Although unfairness claims under the Federal Trade Commission Act usually involve actual and completed harms, they may also be brought on the basis of likely rather than actual injury, and the Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs. Federal Trade Commission Act, §§ 5(a), 5(n), 15 U.S.C.A. §§ 45(a), 45(n).

6. Negligence $\Rightarrow 213, 381$

That a company’s conduct was not the most proximate cause of an injury generally does not immunize the company from liability for foreseeable harms. Restatement (Second) of Torts § 449.

7. Antitrust and Trade Regulation

$\Rightarrow 238$

Hospitality company’s alleged failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information, if proven, which allegedly resulted in computer hackers, on three occasions, being able to access the company’s network and access data of hundreds of thousands of consumers, could fall within the plain meaning of “unfair,” such that the alleged failure could constitute an unfair method of competition in commerce in violation of the Federal Trade Commission Act. Federal Trade Commission Act, § 5(a), 15 U.S.C.A. § 45(a).

8. Statutes $\Rightarrow 1247(4), 1251$

Subsequent legislative history is particularly dangerous ground on which to rest an interpretation of a prior statute when it concerns a proposal that does not become law.

9. Antitrust and Trade Regulation

$\Rightarrow 304$

Congress did not exclude cybersecurity from the Federal Trade Commission’s (FTC) authority to regulate unfair methods of competition in commerce by passing legislation, subsequent to amendment of Federal Trade Commission Act which added prohibition on unfair methods, including amendment to Fair Credit Reporting Act directing the FTC and other agencies to develop regulations for the proper disposal of consumer data, the Gramm-Leach-Bliley Act, requiring the FTC to establish standards for financial institutions to protect consumers’ personal information, and the Children’s Online Privacy Protection Act, ordering the FTC to promulgate regulations requiring children’s websites to provide notice of information collected on children; Congress had reason to pass the subsequent legislation even if the FTC already had regulatory authority over some cybersecurity issues. Federal Trade Commission Act, § 5(a), 15 U.S.C.A. § 45(a); Consumer Credit Protection Act, § 602, as amended, 15 U.S.C.A. § 1681w; Gramm–Leach–Bliley Act, § 501(b), 15 U.S.C.A. § 6801(b); 15 U.S.C.A. § 6502(b).

10. Constitutional Law $\Rightarrow 4426, 4505$

A conviction or punishment violates the Due Process Clause of the Constitution if the statute or regulation under which it is obtained fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement. U.S.C.A. Const. Amend. 5.

11. Constitutional Law $\Rightarrow 3905, 4426$

The requirement that, to comply with the Due Process Clause, a statute or regulation must provide a person of ordinary intelligence fair notice of what is prohibited, extends to civil cases, particularly where a penalty is imposed, though lesser degrees of specificity are allowed in civil cases because the consequences are smaller than in the criminal context. U.S.C.A. Const. Amend. 5.
12. Constitutional Law ⇐4426

For civil statutes that regulate economic activities, a party lacks fair notice of what is prohibited under the statute, such that a punishment for violation of the statute violates the Due Process Clause, when the relevant standard is so vague as to be no rule or standard at all. U.S.C.A. Const. Amend. 5.

13. Constitutional Law ⇐4026

The Due Process Clause prevents judicial deference from validating the application of a regulation, by a federal administrative agency, that fails to give fair warning of the conduct it prohibits or requires. U.S.C.A. Const. Amend. 5.

14. Administrative Law and Procedure ⇐413, 433

Statutes ⇐1104

In resolving ambiguity in statutes or regulations, courts generally adopt the best or most reasonable interpretation.

15. Administrative Law and Procedure ⇐413, 432

Because a federal administrative agency is often free to adopt any reasonable construction of a statute or regulation that it administers, it may impose higher legal obligations than required by the best interpretation of an ambiguous statute or regulation.

16. Statutes ⇐1104

Courts generally resolve statutory ambiguity by applying traditional methods of construction.

17. Administrative Law and Procedure ⇐413, 432

In resolving ambiguity in a statute or regulation that a federal administrative agency administers, an agency may rely on technical expertise and political values.

18. Antitrust and Trade Regulation ⇐238

Constitutional Law ⇐4261

Hospitality company was entitled to notice of meaning of provision of Federal Trade Commission Act prohibiting unfair methods of competition commerce, and was not entitled to know with ascertainable certainty the Federal Trade Commission’s (FTC) interpretation of what cybersecurity practices were required by the provision, for purposes of determining whether company had fair notice of provision’s meaning, under due Process Clause, in FTC’s action against company, alleging violation of the provision based on alleged failure to maintain reasonable and appropriate data security for consumers’ sensitive personal information. U.S.C.A. Const. Amend. 5; Federal Trade Commission Act, § 5(a), 15 U.S.C.A. § 45(a).

19. Antitrust and Trade Regulation ⇐238

Constitutional Law ⇐4261

Hospitality company had fair notice of meaning of provision of the Federal Trade Commission Act prohibiting unfair methods of competition in commerce such that the Federal Trade Commission’s (FTC) action against company, alleging unfair practices based on allegations that company failed to maintain reasonable and appropriate data security for consumers’ sensitive personal information, did not violate the Due Process Clause for failure to provide notice of what statute prohibited; subsection of provision setting forth standard of proof used to determine whether an act is unfair in violation of the Act asked whether “the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition,” company was alleged to have used no cybersecurity measures to protect
consumers' personal information, as a result of the failure, company was hacked three times, resulting in losses for consumers, FTC had issued guidebook for protecting consumers' personal information in which it recommended cybersecurity measures, and, prior to hacking incidents, FTC had filed complaints and entered into consent decrees in administrative cases raising unfairness claims based on inadequate corporate cybersecurity. U.S.C.A. Const. Amend. 5; Federal Trade Commission Act, §§ 5(a), 5(n), 15 U.S.C.A. §§ 45(a), 45(n).

20. Constitutional Law

Statutes regulating economic activity receive a less strict test for determining whether the statute is unduly vague in violation of due process; such a statute's subject matter is often more narrow, and businesses, which face economic demands to plan behavior carefully, can be expected to consult relevant legislation in advance of action. U.S.C.A. Const. Amend. 5.


Scott M. Michelman, Esquire, Jehan A. Patterson, Esquire, Public Citizen Litigation Group, Washington, DC, Counsel for Amicus Appellees, Public Citizen Inc.; Consumer Action; Center for Digital Democracy.

for Democracy & Technology, Electronic Frontier Foundation.

Before: AMBRO, SCIRICA, and ROTH, Circuit Judges.

OPINION OF THE COURT

AMBRO, Circuit Judge.

The Federal Trade Commission Act prohibits “unfair or deceptive acts or practices in or affecting commerce.” 15 U.S.C. § 45(a). In 2005 the Federal Trade Commission began bringing administrative actions under this provision against companies with allegedly deficient cybersecurity that failed to protect consumer data against hackers. The vast majority of these cases have ended in settlement.

On three occasions in 2008 and 2009 hackers successfully accessed Wyndham Worldwide Corporation’s computer systems. In total, they stole personal and financial information for hundreds of thousands of consumers leading to over $10.6 million dollars in fraudulent charges. The FTC filed suit in federal District Court, alleging that Wyndham’s conduct was an unfair practice and that its privacy policy was deceptive. The District Court denied Wyndham’s motion to dismiss, and we granted interlocutory appeal on two issues: whether the FTC has authority to regulate cybersecurity under the unfairness prong of § 45(a); and, if so, whether Wyndham had fair notice its specific cybersecurity practices could fall short of that provision. We affirm the District Court.

I. Background

A. Wyndham’s Cybersecurity

Wyndham Worldwide is a hospitality company that franchises and manages hotels and sells timeshares through three subsidiaries. Wyndham licensed its brand name to approximately 90 independently owned hotels. Each Wyndham-branded hotel has a property management system that processes consumer information that includes names, home addresses, email addresses, telephone numbers, payment card account numbers, expiration dates, and security codes. Wyndham “manage[s]” these systems and requires the hotels to “purchase and configure” them to its own specifications. Compl. ¶ 15, 17. It also operates a computer network in Phoenix, Arizona, that connects its data center with the property management systems of each of the Wyndham-branded hotels.

The FTC alleges that, at least since April 2008, Wyndham engaged in unfair cybersecurity practices that, “taken together, unreasonably and unnecessarily exposed consumers’ personal data to unauthorized access and theft.” Id. at ¶ 24. This claim is fleshed out as follows.

1. The company allowed Wyndham-branded hotels to store payment card information in clear readable text.

2. Wyndham allowed the use of easily guessed passwords to access the property management systems. For example, to gain “remote access to at least one hotel’s system,” which was developed by Micros Systems, Inc., the user ID and password were both “micros.” Id. at ¶ 24(f).

1. On appeal, Wyndham also argues that the FTC fails the pleading requirements of an unfairness claim. As Wyndham did not request and we did not grant interlocutory appeal on this issue, we decline to address it.

2. In addition to Wyndham Worldwide, the defendant entities are Wyndham Hotel Group, LLC, Wyndham Hotels and Resorts, LLC, and Wyndham Hotel Management, Inc. For convenience, we refer to all defendants jointly as Wyndham.
3. Wyndham failed to use "readily available security measures"—such as firewalls—to "limit access between [the] hotels' property management systems, . . . corporate network, and the Internet." *Id.* at ¶ 24(a).

4. Wyndham allowed hotel property management systems to connect to its network without taking appropriate cybersecurity precautions. It did not ensure that the hotels implemented "adequate information security policies and procedures." *Id.* at ¶ 24(c). Also, it knowingly allowed at least one hotel to connect to the Wyndham network with an out-of-date operating system that had not received a security update in over three years. It allowed hotel servers to connect to Wyndham’s network even though "default user IDs and passwords were enabled . . ., which were easily available to hackers through simple Internet searches." *Id.* And, because it failed to maintain an "adequate[] inventory [of] computers connected to [Wyndham’s] network [to] manage the devices," it was unable to identify the source of at least one of the cybersecurity attacks. *Id.* at ¶ 24(g).

5. Wyndham failed to "adequately restrict" the access of third-party vendors to its network and the servers of Wyndham-branded hotels. *Id.* at ¶ 24(j). For example, it did not "restrict[] connections to specified IP addresses or grant[] temporary, limited access, as necessary." *Id.*

6. It failed to employ "reasonable measures to detect and prevent unauthorized access" to its computer network or to "conduct security investigations." *Id.* at ¶ 24(h).

7. It did not follow "proper incident response procedures." *Id.* at ¶ 24(i). The hackers used similar methods in each attack, and yet Wyndham failed to monitor its network for malware used in the previous intrusions.

Although not before us on appeal, the complaint also raises a deception claim, alleging that since 2008 Wyndham has published a privacy policy on its website that overstates the company's cybersecurity.

We safeguard our Customers’ personally identifiable information by using industry standard practices. Although “guaranteed security” does not exist either on or off the Internet, we make commercially reasonable efforts to make our collection of such [i]nformation consistent with all applicable laws and regulations. Currently, our Web sites utilize a variety of different security measures designed to protect personally identifiable information from unauthorized access by users both inside and outside of our company, including the use of 128–bit encryption based on a Class 3 Digital Certificate issued by Verisign Inc. This allows for utilization of Secure Sockets Layer, which is a method for encrypting data. This protects confidential information—such as credit card numbers, online forms, and financial data—from loss, misuse, interception and hacking. We take commercially reasonable efforts to create and maintain “fire walls” and other appropriate safeguards . . . .

*Id.* at ¶ 21. The FTC alleges that, contrary to this policy, Wyndham did not use encryption, firewalls, and other commercially reasonable methods for protecting consumer data.

**B. The Three Cybersecurity Attacks**

As noted, on three occasions in 2008 and 2009 hackers accessed Wyndham's network and the property management systems of Wyndham-branded hotels. In April 2008, hackers first broke into the local network of a hotel in Phoenix, Arizona, which was connected to Wyndham’s network and the Internet. They then
used the brute-force method—repeatedly guessing users’ login IDs and passwords—to access an administrator account on Wyndham’s network. This enabled them to obtain consumer data on computers throughout the network. In total, the hackers obtained unencrypted information for over 500,000 accounts, which they sent to a domain in Russia.

In March 2009, hackers attacked again, this time by accessing Wyndham’s network through an administrative account. The FTC claims that Wyndham was unaware of the attack for two months until consumers filed complaints about fraudulent charges. Wyndham then discovered “memory-scraping malware” used in the previous attack on more than thirty hotels’ computer systems. Id. at ¶ 34. The FTC asserts that, due to Wyndham’s “failure to monitor [the network] for the malware used in the previous attack, hackers had unauthorized access to [its] network for approximately two months.” Id. In this second attack, the hackers obtained unencrypted payment card information for approximately 50,000 consumers from the property management systems of 39 hotels.

Hackers in late 2009 breached Wyndham’s cybersecurity a third time by accessing an administrator account on one of its networks. Because Wyndham “had still not adequately limited access between . . . the Wyndham-branded hotels’ property management systems, [Wyndham’s network], and the Internet,” the hackers had access to the property management servers of multiple hotels. Id. at ¶ 37. Wyndham only learned of the intrusion in January 2010 when a credit card company received complaints from cardholders. In this third attack, hackers obtained payment card information for approximately 69,000 customers from the property management systems of 28 hotels.

The FTC alleges that, in total, the hackers obtained payment card information from over 619,000 consumers, which (as noted) resulted in at least $10.6 million in fraud loss. It further states that consumers suffered financial injury through “unreimbursed fraudulent charges, increased costs, and lost access to funds or credit,” Id. at ¶ 40, and that they “expended time and money resolving fraudulent charges and mitigating subsequent harm.” Id.

C. Procedural History

The FTC filed suit in the U.S. District Court for the District of Arizona in June 2012 claiming that Wyndham engaged in “unfair” and “deceptive” practices in violation of § 45(a). At Wyndham’s request, the Court transferred the case to the U.S. District Court for the District of New Jersey. Wyndham then filed a Rule 12(b)(6) motion to dismiss both the unfair practice and deceptive practice claims. The District Court denied the motion but certified its decision on the unfairness claim for interlocutory appeal. We granted Wyndham’s application for appeal.

II. Jurisdiction and Standards of Review

The District Court has subject-matter jurisdiction under 28 U.S.C. §§ 1331, 1337(a), and 1345. We have jurisdiction under 28 U.S.C. § 1292(b).

We have plenary review of a district court’s ruling on a motion to dismiss for failure to state a claim under Rule 12(b)(6). Farber v. City of Paterson, 440 F.3d 131, 134 (3d Cir.2006). In this review, “we accept all factual allegations as true, construe the complaint in the light most favorable to the plaintiff, and determine whether, under any reasonable reading of the complaint, the plaintiff may be entitled to relief.” Pinker v. Roche Hold-
ings Ltd., 292 F.3d 361, 374 n. 7 (3d Cir. 2002).

III. FTC’s Regulatory Authority Under § 45(a)

A. Legal Background

[2] The Federal Trade Commission Act of 1914 prohibited "unfair methods of competition in commerce." Pub.L. No. 63–203, § 5, 38 Stat. 717, 719 (codified as amended at 15 U.S.C. § 45(a)). Congress "explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' . . . by enumerating the particular practices to which it was intended to apply." FTC v. Sperry & Hutchinson Co., 405 U.S. 233, 239–40, 92 S.Ct. 898, 31 L.Ed.2d 170 (1972) (citing S.Rep. No. 63–597, at 13 (1914)); see also S.Rep. No. 63–597, at 13 ("The committee gave careful consideration to the question as to whether it would attempt to define the many and variable unfair practices which prevail in commerce. . . . It concluded that . . . there were too many unfair practices to define, and after writing 20 of them into the law it would be quite possible to invent others." (emphasis added)). The takeaway is that Congress designed the term as a "flexible concept with evolving content," FTC v. Bunte Bros., 312 U.S. 349, 353, 61 S.Ct. 580, 85 L.Ed. 881 (1941), and "intentionally left [its] development . . . to the Commission," Atl. Ref. Co. v. FTC, 381 U.S. 357, 367, 85 S.Ct. 1498, 14 L.Ed.2d 443 (1965).

For the next few decades, the FTC interpreted the unfair-practices prong primarily through agency adjudication. But in 1964 it issued a "Statement of Basis and Purpose" for unfair or deceptive advertising and labeling of cigarettes, 29 Fed.Reg. 8324, 8355 (July 2, 1964), which explained that the following three factors governed unfairness determinations:

(1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; [and] (3) whether it causes substantial injury to consumers (or competitors or other businessmen).

Id. Almost a decade later, the Supreme Court implicitly approved these factors, apparently acknowledging their applicability to contexts other than cigarette advertising and labeling. Sperry, 405 U.S. at 244 n. 5, 92 S.Ct. 898. The Court also held that, under the policy statement, the FTC could deem a practice unfair based on the third prong—substantial consumer injury—without finding that at least one of the other two prongs was also satisfied. Id.

During the 1970s, the FTC embarked on a controversial campaign to regulate children’s advertising through the unfair-practices prong of § 45(a). At the request of Congress, the FTC issued a second policy statement in 1980 that clarified the three factors. FTC Unfairness Policy Statement, Letter from the FTC to Hon. Wendell Ford and Hon. John Danforth, Senate Comm. on Commerce, Sci., and Transp. (Dec. 17, 1980), appended to Int’l Harvester Co., 104 F.T.C. 949, 1070 (1984) [herein-
after 1980 Policy Statement]. It explained that public policy considerations are relevant in determining whether a particular practice causes substantial consumer injury. *Id.* at 1074–76. Next, it “abandoned” the “theory of immoral or unscrupulous conduct . . . altogether” as an “independent” basis for an unfairness claim. *Int’l Harvester Co.,* 104 F.T.C. at 1061 n. 43; 1980 Policy Statement, *supra* at 1076 (“The Commission has . . . never relied on [this factor] as an independent basis for a finding of unfairness, and it will act in the future only on the basis of the [other] two.”). And finally, the Commission explained that “[u]njustified consumer injury is the primary focus of the FTC Act” and that such an injury “[b]y itself . . . can be sufficient to warrant a finding of unfairness.” 1980 Policy Statement, *supra* at 1073. This “does not mean that every consumer injury is legally ‘unfair.’” *Id.* Indeed, [t]o justify a finding of unfairness the injury must satisfy three tests. [1] It must be substantial; [2] it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and [3] it must be an injury that consumers themselves could not reasonably have avoided. *Id.*


The Commission shall have no authority under this section . . . to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

FTC Act Amendments of 1994, Pub.L. No. 103–312, § 9, 108 Stat. 1691, 1695. Like the 1980 Policy Statement, § 45(n) requires substantial injury that is not reasonably avoidable by consumers and that is not outweighed by the benefits to consumers or competition. It also acknowledges the potential significance of public policy and does not expressly require that an unfair practice be immoral, unethical, unscrupulous, or oppressive.

B. Plain Meaning of Unfairness

Wyndham argues (for the first time on appeal) that the three requirements of 15 U.S.C. § 45(n) are necessary but insufficient conditions for an unfair practice and that the plain meaning of the word “unfair” imposes independent requirements that are not met here. Arguably, § 45(n) may not identify all of the requirements for a finding of unfairness. (While the provision forbids the FTC from declaring an act unfair “unless” the act satisfies the three specified requirements, it does not answer whether these are the only requirements for a finding of unfairness.) Even if so, some of Wyndham’s proposed requirements are unpersuasive, and the rest are satisfied by the allegations in the FTC’s complaint.

[3] First, citing *FTC v. R.F. Keppel & Brother, Inc.*, 291 U.S. 304, 54 S.Ct. 423, 78 L.Ed. 814 (1934), Wyndham argues that conduct is only unfair when it injures consumers “through unscrupulous or unethical behavior.” Wyndham Br. at 20–21. But *Keppel* nowhere says that unfair conduct must be unscrupulous or unethical. Moreover, in *Sperry* the Supreme Court rejected the view that the FTC’s 1964 policy
statement required unfair conduct to be "unscrupulous" or "unethical." 405 U.S. at 244 n. 5, 92 S.Ct. 898. Wyndham points to no subsequent FTC policy statements, adjudications, judicial opinions, or statutes that would suggest any change since Sperry.

Next, citing one dictionary, Wyndham argues that a practice is only "unfair" if it is "not equitable" or is "marked by injustice, partiality, or deception." Wyndham Br. at 18–19 (citing Webster's Ninth New Collegiate Dictionary (1988)). Whether these are requirements of an unfairness claim makes little difference here. A company does not act equitably when it publishes a privacy policy to attract customers who are concerned about data privacy, fails to make good on that promise by investing inadequate resources in cybersecurity, exposes its unsuspecting customers to substantial financial injury, and retains the profits of their business.

[4] We recognize this analysis of unfairness encompasses some facts relevant to the FTC's deceptive practices claim. But facts relevant to unfairness and deception claims frequently overlap. See, e.g., Am. Fin. Servs. Ass'n v. FTC, 767 F.2d 957, 980 n. 27 (D.C.Cir.1985) ("The FTC has determined that . . . making unsubstantiated advertising claims may be both an unfair and a deceptive practice."); Orkin Exterminating Co. v. FTC, 849 F.2d 1354, 1367 (11th Cir.1988) ("[A] practice may be both deceptive and unfair. . . ."). We cannot completely disentangle the two theories here. The FTC argued in the District Court that consumers could not reasonably avoid injury by booking with another hotel chain because Wyndham had

3. Id. ("[Petitioner] argues that . . . [the 1964 statement] commits the FTC to the view that misconduct in respect of the third of these criteria is not subject to constraint as 'unfair' absent a concomitant showing of misconduct according to the first or second of these criteria. But all the FTC said in the [1964] statement . . . was that '[t]he wide variety of decisions interpreting the elusive concept of unfairness at least makes clear that a method of selling violates Section 5 if it is exploitive or inequitable and if, in addition to being morally objectionable, it is seriously detrimental to consumers or others.'" (emphasis and some alterations in original, citation omitted)).

4. The FTC has on occasion described deception as a subset of unfairness. See Int'l Harvester Co., 104 F.T.C. at 1060 ("The Commission's unfairness jurisdiction provides a more general basis for action against acts or practices which cause significant consumer injury. This part of our jurisdiction is broader than that involving deception, and the standards for its exercise are correspondingly more stringent. . . . [U]nfairness is the set of general principles of which deception is a particularly well-established and streamlined subset."); Figgie Int'l, 107 F.T.C. 313, 373 n. 5 (1986) ("[U]nfair practices are not always deceptive but deceptive practices are always unfair."); Orkin Exterminating Co., 108 F.T.C. 263, 363 n. 78 (1986). So have several FTC staff members. See, e.g., J. Howard Beales, Director of the Bureau of Consumer Protection, FTC, Marketing and Public Policy Conference, The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection (May 30, 2003) ("Although, in the past, they have sometimes been viewed as mutually exclusive legal theories, Commission precedent incorporated in the statutory codification makes clear that deception is properly viewed as a subset of unfairness."); Neil W. Averitt, The Meaning of "Unfair Acts or Practices" in Section 5 of the Federal Trade Commission Act, 70 Geo. L.J. 225, 265–66 (1981) ("Although deception is generally regarded as a separate aspect of section 5, in its underlying rationale it is really just one specific form of unfair consumer practice. . . . [For example, the] Commission has held that it is deceptive for a merchant to make an advertising claim for which he lacks a reasonable basis, regardless of whether the claim is eventually proven true or false. . . . Precisely because unsubstantiated ads are deceptive in this manner, . . . they also affect the exercise of consumer sovereignty and thus constitute an unfair act or practice.").
published a misleading privacy policy that overstated its cybersecurity. Plaintiff’s Response in Opposition to the Motion to Dismiss by Defendant at 5, FTC v. Wyndham Worldwide Corp., 10 F.Supp.3d 602 (D.N.J.2014) (“Consumers could not take steps to avoid Wyndham’s unreasonable data security [before providing their personal information] because Wyndham falsely told consumers that it followed ‘industry standard practices.’”); see JA 203 (“On the reasonably avoidable part, . . . consumers certainly would not have known that Wyndham had unreasonable data security practices in this case. . . . We also allege that in [Wyndham’s] privacy policy they deceive consumers by saying we do have reasonable security data practices. That is one way consumers couldn’t possibly have avoided providing a credit card to a company.”). Wyndham did not challenge this argument in the District Court nor does it do so now. If Wyndham’s conduct satisfies the reasonably avoidable requirement at least partially because of its privacy policy—an inference we find plausible at this stage of the litigation—then the policy is directly relevant to whether Wyndham’s conduct was unfair.\footnote{5}

Continuing on, Wyndham asserts that a business “does not treat its customers in an ‘unfair’ manner when the business itself is victimized by criminals.” Wyndham Br. at 21 (emphasis in original). It offers no reasoning or authority for this principle, and we can think of none ourselves. Although unfairness claims “usually involve actual and completed harms,” \textit{Int’l Harvester}, 104 F.T.C. at 1061, “they may also be brought on the basis of likely rather than actual injury,” id. at 1061 n. 45. And the FTC Act expressly contemplates the possibility that conduct can be unfair before actual injury occurs. 15 U.S.C. § 45(n) (“[An unfair act or practice] causes or is likely to cause substantial injury” (emphasis added)). More importantly, that a company’s conduct was not the most proximate cause of an injury generally does not immunize liability from foreseeable harms. \textit{See} Restatement (Second) of Torts § 449 (1965) (“If the likelihood that a third person may act in a particular manner is the hazard or one of the hazards which makes the actor negligent, such an act[,] whether innocent, negligent, intentionally tortious, or criminal[,] does not prevent the actor from being liable for harm caused thereby.”); \textit{Westfarm Assocs. v. Wash. Suburban Sanitary Comm’n}, 66 F.3d 669, 688 (4th Cir.1995) (“Proximate cause may be found even where the conduct of the third party is . . . criminal, so long as the conduct was facilitated by the first party and reasonably foreseeable, and some ultimate harm was reasonably foreseeable.”). For good reason, Wyndham does not argue that the cybersecurity intrusions were unforeseeable. That would be particularly implausible as to the second and third attacks.

Finally, Wyndham posits a \textit{reductio ad absurdum}, arguing that if the FTC’s unfairness authority extends to Wyndham’s conduct, then the FTC also has the authority to “regulate the locks on hotel room doors, . . . to require every store in the land to post an armed guard at the door,” Wyndham Br. at 23, and to sue supermarkets that are “sloppy about sweeping up banana peels,” Wyndham Reply Br. at 6.\footnote{6}

\footnote{5} No doubt there is an argument that consumers could not reasonably avoid injury even absent the misleading privacy policy. \textit{See}, e.g., James P. Nehf, \textit{Shopping for Privacy Online: Consumer Decision–Making Strategies and the Emerging Market for Information Privacy}, 2005 U. Ill. J.L. Tech. & Pol’y. 1 (arguing that consumers may care about data privacy, but be unable to consider it when making credit card purchases). We have no occasion to reach this question, as the parties have not raised it.
The argument is alarmist to say the least. And it invites the tart retort that, were Wyndham a supermarket, leaving so many banana peels all over the place that 619,000 customers fall hardly suggests it should be immune from liability under § 45(a).

[7] We are therefore not persuaded by Wyndham’s arguments that the alleged conduct falls outside the plain meaning of “unfair.”

C. Subsequent Congressional Action


6. Wyndham also points to a variety of cybersecurity bills that Congress has considered and not passed. “[S]ubsequent legislative history . . . is particularly dangerous ground on which to rest an interpretation of a prior statute when it concerns . . . a proposal that does not become law.” Pension Benefit Guar. Corp. v. LTV Corp., 496 U.S. 633, 650, 110 S.Ct. 2668, 110 L.Ed.2d 579 (1990).

[9] We are not persuaded. The inference to congressional intent based on post-enactment legislative activity in Brown & Williamson was far stronger. There, the Food and Drug Administration had repeatedly disclaimed regulatory authority over tobacco products for decades. Id. at 144, 120 S.Ct. 1291. During that period, Congress enacted six statutes regulating tobacco. Id. at 143–44, 120 S.Ct. 1291. The FDA later shifted its position, claiming authority over tobacco products. The Supreme Court held that Congress excluded tobacco-related products from the FDA’s authority in enacting the statutes. As tobacco products would necessarily be banned if subject to the FDA’s regulatory authority, any interpretation to the contrary would contradict congressional intent to regulate rather than ban tobacco products outright. Id. 137–39, 120 S.Ct. 1291; Massachusetts v. EPA, 549 U.S. 497, 530–31, 127 S.Ct. 1438, 167 L.Ed.2d 248 (2007). Wyndham does not argue that recent privacy laws contradict reading corporate cybersecurity into § 45(a). Instead, it merely asserts that Congress had no reason to enact them if the FTC could already regul-
late cybersecurity through that provision. Wyndham Br. at 25–26.

We disagree that Congress lacked reason to pass the recent legislation if the FTC already had regulatory authority over some cybersecurity issues. The Fair Credit Reporting Act requires (rather than authorizes) the FTC to issue regulations, 15 U.S.C. § 1681w (“The Federal Trade Commission . . . shall issue final regulations requiring . . . ” (emphasis added)); id. § 1681m(e)(1)(B) (“The [FTC and other agencies] shall jointly . . . prescribe regulations requiring each financial institution . . . ” (emphasis added)), and expands the scope of the FTC’s authority, id. § 1681s(a)(1) (“A violation of any requirement or prohibition imposed under this subchapter shall constitute an unfair or deceptive act or practice in commerce . . . and shall be subject to enforcement by the [FTC] . . . irrespective of whether that person is engaged in commerce or meets any other jurisdictional tests under the [FTC] Act.”). The Gramm–Leach–Bliley Act similarly requires the FTC to promulgate regulations, id. § 6801(b) (“[The FTC] shall establish appropriate standards for the financial institutions subject to [its] jurisdiction . . . .”), and relieves some of the burdensome § 45(n) requirements for declaring acts unfair, id. § 6801(b) (“[The FTC] shall establish appropriate standards . . . to protect against unauthorized access to or use of . . . records . . . which could result in substantial harm or inconvenience to any customer.” (emphasis added)).

And the Children’s Online Privacy Protection Act required the FTC to issue regulations and empowered it to do so under the procedures of the Administrative Procedure Act, id. § 6502(b) (citing 5 U.S.C. § 553), rather than the more burdensome Magnuson–Moss procedures under which the FTC must usually issue regulations, 15 U.S.C. § 57a. Thus none of the recent privacy legislation was “inexplicable” if the FTC already had some authority to regulate corporate cybersecurity through § 45(a).

Next, Wyndham claims that the FTC’s interpretation of § 45(a) is “inconsistent with its repeated efforts to obtain from Congress the very authority it purports to wield here.” Wyndham Br. at 28. Yet again we disagree. In two of the statements cited by Wyndham, the FTC clearly said that some cybersecurity practices are “unfair” under the statute. See Consumer Data Protection: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce, 2011 WL 2358081, at *6 (June 15, 2011) (statement of Edith Ramirez, Comm’r, FTC) (“[T]he Commission enforces the FTC Act’s proscription against unfair . . . acts . . . in cases where a business[’s] . . . failure to employ reasonable security measures causes or is likely to cause substantial consumer injury.”); Data Theft Issues: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce, 2011 WL 1971214, at *7 (May 4, 2011) (statement of David C. Vladeck, Director, FTC Bureau of Consumer Protection) (same).

In the two other cited statements, given in 1998 and 2000, the FTC only acknowledged that it cannot require companies to adopt “fair information practice policies.” See FTC, Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress 34 (2000) [hereinafter Privacy Online]; Privacy in Cyberspace: Hearing Before the Subcomm. on Telecommuns., Trade & Consumer Prot. of the H. Comm. on Commerce, 1998 WL 546441 (July 21, 1998) (statement of Robert Pitofsky, Chairman, FTC). These policies would protect consumers from far more than the kind of “substantial injury” typically covered by § 45(a). In addition
to imposing some cybersecurity requirements, they would require companies to give notice about what data they collect from consumers, to permit those consumers to decide how the data is used, and to permit them to review and correct inaccuracies. Privacy Online, supra at 36–37.

As the FTC explained in the District Court, the primary concern driving the adoption of these policies in the late 1990s was that "companies ... were capable of collecting enormous amounts of information about consumers, and people were suddenly realizing this." JA 106 (emphasis added). The FTC thus could not require companies to adopt broad fair information practice policies because they were "just collecting the information, and consumers [were not] injured." Id.; see also Order Denying Respondent LabMD's Motion to Dismiss, No. 9357, slip op. at 7 (Jan. 16, 2014) [hereinafter LabMD Order or LabMD] ("[T]he sentences from the 1998 and 2000 reports ... simply recognize that the Commission's existing authority may not be sufficient to effectively protect consumers with regard to all data privacy issues of potential concern (such as aspects of children's online privacy)...." (emphasis in original)). Our conclusion is this: that the FTC later brought unfairness actions against companies whose inadequate cybersecurity resulted in consumer harm is not inconsistent with the agency's earlier position.

IV. Fair Notice

[10] A conviction or punishment violates the Due Process Clause of our Constitution if the statute or regulation under which it is obtained "fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement." FCC v. Fox Television Stations, Inc., — U.S. —, 132 S.Ct. 2307, 2317, 183 L.Ed.2d 234 (2012) (internal quotation marks omitted). Wyndham claims that, notwithstanding whether its conduct was unfair under § 45(a), the FTC failed to give fair notice of the specific cybersecurity standards the company was required to follow.7

A. Legal Standard

The level of required notice for a person to be subject to liability varies by circumstance. In Bouie v. City of Columbia, the Supreme Court held that a "judicial construction of a criminal statute" violates due process if it is "unexpected and indefensible by reference to the law which had been expressed prior to the conduct in issue." 378 U.S. 347, 354, 84 S.Ct. 1697, 12 L.Ed.2d 894 (1964) (internal quotation marks omitted); see also Rogers v. Tennessee, 532 U.S. 451, 457, 121 S.Ct. 1693, 149 L.Ed.2d 697 (2001); In re Surrick, 338 F.3d 224, 233–34 (3d Cir.2003). The precise meaning of "unexpected and indefensible" is not entirely clear, United States v. Lata, 415 F.3d 107, 111 (1st Cir.2005), but we and our sister circuits frequently use language implying that a conviction violates due process if the defendant could not reasonably foresee that a court might adopt the new interpretation of the statute.
ute.8

[11, 12] The fair notice doctrine extends to civil cases, particularly where a penalty is imposed. See Fox Television Stations, Inc., 132 S.Ct. at 2317–20; Boutilier v. INS, 387 U.S. 118, 123, 87 S.Ct. 1563, 18 L.Ed.2d 661 (1967). “Lesser degrees of specificity” are allowed in civil cases because the consequences are smaller than in the criminal context. San Filippo v. Bongiovanni, 961 F.2d 1125, 1135 (3d Cir.1992). The standards are especially lax for civil statutes that regulate economic activities. For those statutes, a party lacks fair notice when the relevant standard is “so vague as to be no rule or standard at all.” CMR D.N. Corp. v. City of Phila., 703 F.3d 612, 631–32 (3d Cir.2013) (internal quotation marks omitted).9

A different set of considerations is implicated when agencies are involved in statutory or regulatory interpretation. Broadly speaking, agencies interpret in at least three contexts. One is where an agency administers a statute without any special authority to create new rights or obligations. When disputes arise under this kind of agency interpretation, the courts give respect to the agency’s view to the extent it is persuasive, but they retain the primary responsibility for construing the statute.10 As such, the standard of notice afforded to litigants about the meaning of the statute is not dissimilar to the standard of notice for civil statutes generally

8. See Ortiz v. N.Y.S. Parole, 586 F.3d 149, 159 (2d Cir.2009) (holding that the “unexpected and indefensible” standard “requires only that the law … not hull the potential defendant into a false sense of security, giving him no reason even to suspect that his conduct might be within its scope.” (emphases added)); In re Surrick, 338 F.3d at 234 (“[W]e reject [the] contention that … nothing in the history of [the relevant provision] had stated or even foreshadowed that reckless conduct could violate it. Indeed, in view of the foregoing, the [state court’s] decision … was neither ‘unexpected’ nor ‘indefensible’ by reference to the law which had been expressed prior to the conduct in issue.” (emphases added)); Warner v. Zent, 997 F.2d 116, 125 (6th Cir.1993) (“The underlying principle is that no man shall be held criminally responsible for conduct which he could not reasonably understand to be proscribed.”) (emphasis added) (quoting United States v. Harris, 347 U.S. 612, 617, 74 S.Ct. 808, 98 L.Ed. 989 (1954)); id. at 127 (“It was by no means unforeseeable … that the [court] would construe the statute as it did.”) (emphasis added); see also Lata, 415 F.3d at 112 (“[S]omeone in [the defendant’s] position could not reasonably be surprised by the sentence he eventually received. … We reserve for the future the case … in which a sentence is imposed … that is higher than any that might realistically have been imagined at the time of the crime. …” (emphasis added)).


10. See Skidmore v. Swift & Co., 323 U.S. 134, 140, 65 S.Ct. 161, 89 L.Ed. 124 (1944) (“[The agency interpretation is] not controlling upon the courts by reason of [its] authority [but is] a body of experience and informed judgment to which courts … may properly resort for guidance.”); Christensen v. Harris Cnty., 529 U.S. 576, 587, 120 S.Ct. 1655, 146 L.Ed.2d 621 (2000) (“[Agency interpretations are] entitled to respect under [Skidmore,] but only to the extent that [they] have the power to persuade.”) (internal quotation marks omitted)); see also Peter L. Strauss, “Deference is Too Confusing—Let’s Call Them “Chevron Space” and “Skidmore Weight”, 112 Colum. L.Rev. 1143, 1147 (2012) (“Skidmore … is grounded in a construct of the agency as responsible expert, arguably possessing special knowledge of the statutory meaning a court should consider in reaching its own judgment.”) (emphasis added)).
because the court, not the agency, is the ultimate arbiter of the statute’s meaning.

The second context is where an agency exercises its authority to fill gaps in a statutory scheme. There the agency is primarily responsible for interpreting the statute because the courts must defer to any reasonable construction it adopts. See Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837, 104 S.Ct. 2778, 81 L.Ed.2d 694 (1984). Courts appear to apply a more stringent standard of notice to civil regulations than civil statutes: parties are entitled to have “ascertainable certainty” of what conduct is legally required by the regulation. See Chem. Waste Mgmt., Inc. v. EPA, 976 F.2d 2, 29 (D.C.Cir.1992) (per curiam) (denying petitioners’ challenge that a recently promulgated EPA regulation fails fair notice principles); Nat’l Oilseed Processors Ass’n v. OSHA, 769 F.3d 1173, 1183–84 (D.C.Cir. 2014) (denying petitioners’ challenge that a recently promulgated OSHA regulation fails fair notice principles).

[13] The third context is where an agency interprets the meaning of its own regulation. Here also courts typically must defer to the agency’s reasonable interpretation.11 We and several of our sister circuits have stated that private parties are entitled to know with “ascertainable certainty” an agency’s interpretation of its regulation. See AJP Const., Inc., 357 F.3d at 75 (internal quotation marks omitted).

[14, 15] A higher standard of fair notice applies in the second and third contexts than in the typical civil statutory interpretation case because agencies en-

11. See Auer v. Robbins, 519 U.S. 452, 461, 117 S.Ct. 905, 137 L.Ed.2d 79 (1997) (“Because the salary-basis test is a creature of the Secretary’s own regulations, his interpretation of it is … controlling unless plainly erroneous or inconsistent with the regulation.”) (internal quotation marks omitted); Decker v. Nw. Envtl. Def. Ctr., — U.S. —, 133 S.Ct. 1326, 1337, 185 L.Ed.2d 447 (2013) (“When an agency interprets its own regulation, the Court, as a general rule, defers to it unless that interpretation is plainly erroneous or inconsistent with the regulation.”) (internal quotation marks omitted); Martin v. Occupational Safety & Health Rev. Comm’n, 499 U.S. 144, 150–51, 111 S.Ct. 1171, 113 L.Ed.2d 117 (1991) (“In situations in which the meaning of [regulatory] language is not free from doubt, the reviewing court should give effect to the agency’s interpretation so long as it is reasonable.”) (alterations in original, internal quotations omitted); Columbia Gas Transp., LLC v. 1.01 Acres, More or Less in Penn Twp., 768 F.3d 300, 313 (3d Cir.2014) (“[A]s an agency interpretation of its own regulation, it is deserving of deference.”) (citing Decker).

gage in interpretation differently than courts. See Frank H. Easterbook, Judicial Discretion in Statutory Interpretation, 57 Okla. L.Rev. 1, 3 (2004) (“A judge who announces deference is approving a shift in interpretive method, not just a shift in the identity of the decider, as if a suit were being transferred to a court in a different venue.”). In resolving ambiguity in statutes or regulations, courts generally adopt the best or most reasonable interpretation. But, as the agency is often free to adopt any reasonable construction, it may impose higher legal obligations than required by the best interpretation. 13

Furthermore, courts generally resolve statutory ambiguity by applying traditional methods of construction. Private parties can reliably predict the court’s interpretation by applying the same methods. In contrast, an agency may also rely on technical expertise and political values. 14 It is harder to predict how an agency will construe a statute or regulation at some unspecified point in the future, particularly when that interpretation will depend on the “political views of the President in office at [that] time.” Strauss, supra at 1147.

Wyndham argues it was entitled to “ascertainable certainty” of the FTC’s interpretation of what specific cybersecurity practices are required by § 45(a). Yet it has contended repeatedly—no less than seven separate occasions in this case—that there is no FTC rule or adjudication about cybersecurity that merits deference here. The necessary implication, one that Wyndham itself has explicitly drawn on two occasions noted below, is that federal courts are to interpret § 45(a) in the first

13. See Nat’l Cable & Telecomms. Ass’n v. Brand X Internet Servs., 545 U.S. 967, 980, 125 S.Ct. 2688, 162 L.Ed.2d 820 (2005) (“If a statute is ambiguous, and if the implementing agency’s construction is reasonable, Chevron requires a federal court to accept the agency’s construction of the statute, even if the agency’s reading differs from what the court believes is the best statutory interpretation.”); Decker, 133 S.Ct. at 1337 (“It is well established that an agency’s interpretation need not be the only possible reading of a regulation—or even the best one—to prevail. When an agency interprets its own regulation, the Court, as a general rule, defers to it unless that interpretation is plainly erroneous or inconsistent with the regulation.” (internal quotation marks omitted)); Auer, 519 U.S. at 462–63, 117 S.Ct. 905 (“[The rule that Fair Labor Standards Act] exemptions are to be narrowly construed against . . . employers . . . is a rule governing judicial interpretation of statutes and regulations, not a limitation on the Secretary’s power to resolve ambiguities in his own regulations. A rule requiring the Secretary to construe his own regulations narrowly would make little sense, since he is free to write the regulations as broadly as he wishes, subject only to the limits imposed by the statute.” (internal quotation marks omitted)).

14. See Garfias–Rodriguez v. Holder, 702 F.3d 504, 518 (9th Cir.2012) (rejecting the applicability of the judicial retroactivity test to a new Board of Immigration Appeals’ interpretation because the “decision fill[ed] a statutory gap and [was] an exercise [of the agency’s] policymaking function”); Easterbrook, supra at 3 (“Judges in their own work forswear the methods that agencies employ” to interpret statutes, which include relying on “political pressure, the President’s view of happy outcomes, cost-benefit studies . . . and the other tools of policy wonks . . .”).

15. See also Brand X Internet Servs., 545 U.S. at 981, 125 S.Ct. 2688 (“[T]he agency . . . must consider varying interpretations and the wisdom of its policy on a continuing basis . . . in response to . . . a change in administrations.” (internal quotation marks omitted, first omission in original)); Motor Vehicle Mfrs. Ass’n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 59, 103 S.Ct. 2856, 77 L.Ed.2d 443 (1983) (Rehnquist, J., dissenting in part) (“A change in administration brought about by the people casting their votes is a perfectly reasonable basis for an executive agency’s reappraisal of the costs and benefits of its . . . regulations.”).
instance to decide whether Wyndham’s conduct was unfair.

Wyndham’s argument has focused on the FTC’s motion to dismiss order in LabMD, an administrative case in which the agency is pursuing an unfairness claim based on allegedly inadequate cybersecurity. LabMD Order, supra. Wyndham first argued in the District Court that the LabMD Order does not merit Chevron deference because “self-serving, litigation-driven decisions . . . are entitled to no deference at all” and because the opinion adopted an impermissible construction of the statute. Wyndham’s January 29, 2014 Letter at 1–2, FTC v. Wyndham Worldwide Corp., 10 F.Supp.3d 602 (D.N.J.2014).

Second, Wyndham switched gears in its opening brief on appeal to us, arguing that LabMD does not merit Chevron deference because courts owe no deference to an agency’s interpretation of the “boundaries of Congress’ statutory delegation of authority to the agency.” Wyndham Br. at 19–20.

Third, in its reply brief it argued again that LabMD does not merit Chevron deference because it adopted an impermissible construction of the statute. Wyndham Reply Br. at 14.

Fourth, Wyndham switched gears once more in a Rule 28(j) letter, arguing that LabMD does not merit Chevron deference because the decision was nonfinal. Wyndham’s February 6, 2015 Letter (citing LabMD, Inc. v. FTC, 776 F.3d 1275 (11th Cir.2015)).

Fifth, at oral argument we asked Wyndham whether the FTC had decided that cybersecurity practices are unfair. Counsel answered: “No. I don’t think consent decrees count, I don’t think the 2007 brochure counts, and I don’t think Chevron deference applies. So are . . . they asking this federal court in the first instance . . . ?] I think the answer to that question is yes . . . .” Oral Arg. Tr. at 19.

Sixth, due to our continuing confusion about the parties’ positions on a number of issues in the case, we asked for supplemental briefing on certain questions, including whether the FTC had declared that cybersecurity practices can be unfair. In response, Wyndham asserted that “the FTC has not declared unreasonable cybersecurity practices ‘unfair.’” Wyndham’s Supp. Memo. at 3. Wyndham explained further: “It follows from [our] answer to [that] question that the FTC is asking the federal courts to determine in the first instance that unreasonable cybersecurity practices qualify as ‘unfair’ trade practices under the FTC Act.” Id. at 4.

Seventh, and most recently, Wyndham submitted a Rule 28(j) letter arguing that LabMD does not merit Chevron deference because it decided a question of “deep economic and political significance.” Wyndham’s June 30, 2015 Letter (quoting King v. Burwell, — U.S. ——, 135 S.Ct. 2480, 192 L.Ed.2d 483 (2015)).

Wyndham’s position is unmistakable: the FTC has not yet declared that cybersecurity practices can be unfair; there is no relevant FTC rule, adjudication or document that merits deference; and the FTC is asking the federal courts to interpret § 45(a) in the first instance to decide whether it prohibits the alleged conduct here. The implication of this position is similarly clear: if the federal courts are to decide whether Wyndham’s conduct was unfair in the first instance under the statute without deferring to any FTC interpretation, then this case involves ordinary judicial interpretation of a civil statute, and the ascertainable certainty standard does not apply. The relevant question is not whether Wyndham had fair notice of the FTC’s interpretation of the statute, but
whether Wyndham had fair notice of what the statute itself requires.

Indeed, at oral argument we asked Wyndham whether the cases cited in its brief that apply the "ascertainable certainty" standard—all of which involve a court reviewing an agency adjudication or at least a court being asked to defer to an agency interpretation—apply where the court is to decide the meaning of the statute in the first instance. Wyndham's counsel responded, "I think it would, your Honor. I think if you go to Ford Motor [Co. v. FTC, 673 F.2d 1008 (9th Cir.1981)], I think that's what was happening there." Oral Arg. Tr. at 61. But Ford Motor is readily distinguishable. Unlike Wyndham, the petitioners there did not bring a fair notice claim under the Due Process Clause. Instead, they argued that, per NLRB v. Bell Aerospace Co., 416 U.S. 267, 94 S.Ct. 1757, 40 L.Ed.2d 134 (1974), the FTC abused its discretion by proceeding through agency adjudication rather than rulemaking. More importantly, the Ninth Circuit was reviewing an agency adjudication; it was not interpreting the meaning of the FTC Act in the first instance.

In addition, our understanding of Wyndham's position is consistent with the District Court's opinion, which concluded that the FTC has stated a claim under § 45(a) based on the Court's interpretation of the statute and without any reference to LabMD or any other agency adjudication or regulation. See FTC v. Wyndham Worldwide Corp., 10 F.Supp.3d 602, 621–26 (D.N.J.2014).

16. See Fox Television Stations, Inc., — U.S. —, 132 S.Ct. 2307, 183 L.Ed.2d 234 (vacating an FCC adjudication for lack of fair notice of an agency interpretation); PMD Produce Brokerage Corp. v. USDA, 234 F.3d 48 (D.C.Cir.2000) (vacating the dismissal of an administrative appeal issued by a Judicial Officer in the Department of Agriculture because the agency's Rules of Practice failed to give fair notice of the deadline for filing an appeal); Gen. Elec. Co., 53 F.3d 1324 (vacating an EPA adjudication for lack of fair notice of the agency's interpretation of a regulation); FTC v. Colgate-Palmolive Co., 380 U.S. 374, 85 S.Ct. 1035, 13 L.Ed.2d 904 (1965) (reviewing an FTC adjudication that found liability).

17. See In re Metro–East Mfg. Co., 655 F.2d 805, 810–12 (7th Cir.1981) (declining to defer to an agency's interpretation of its own regulation because the defendant could not have known with ascertainable certainty the agency's interpretation).

18. We asked, "All of your cases on fair notice pertain to an agency's interpretation of its own regulation or the statute that governs that agency. Does this fair notice doctrine apply where it is a court announcing an interpretation of a statute in the first instance?" Oral Arg. Tr. at 60 (emphases added).

19. To the extent Wyndham could have raised this argument, we do not read its briefs to do so. Indeed, its opening brief appears to repudiate the theory. Wyndham Br. at 38–39 ("The district court below framed the fair notice issue here as whether 'the FTC must formally promulgate regulations before bringing its unfairness claim.' With all respect, that characterization of Wyndham's position is a straw man. Wyndham has never disputed the general principle that administrative agencies have discretion to regulate through either rulemaking or adjudication. See, e.g., [Bell Aerospace Co., 416 U.S. at 290–95, 94 S.Ct. 1757]. Rather, Wyndham's point is only that, however an agency chooses to proceed, it must provide regulated entities with constitutionally requisite fair notice." (internal citations omitted)). Moreover, the Supreme Court has explained that where "it is doubtful [that] any generalized standard could be framed which would have more than marginal utility[, the agency] has reason to . . . develop[ ] its standards in a case-by-case manner." Bell Aerospace Co., 416 U.S. at 294, 94 S.Ct. 1757. An agency's "judgment that adjudication best serves this purpose is entitled to great weight." Id. Wyndham's opening brief acknowledges that the FTC has given this rationale for proceeding by adjudication, Wyndham Br. at 37–38, but, the company offers no ground to challenge it.
We thus conclude that Wyndham was not entitled to know with ascertainable certainty the FTC’s interpretation of what cybersecurity practices are required by § 45(a). Instead, the relevant question in this appeal is whether Wyndham had fair notice that its conduct could fall within the meaning of the statute. If later proceedings in this case develop such that the proper resolution is to defer to an agency interpretation that gives rise to Wyndham’s liability, we leave to that time a fuller exploration of the level of notice required. For now, however, it is enough to say that we accept Wyndham’s forceful contention that we are interpreting the FTC Act (as the District Court did). As a necessary consequence, Wyndham is only entitled to notice of the meaning of the statute and not to the agency’s interpretation of the statute.

B. Did Wyndham Have Fair Notice of the Meaning of § 45(a)?

Having decided that Wyndham is entitled to notice of the meaning of the statute, we next consider whether the case should be dismissed based on fair notice principles. We do not read Wyndham’s briefs as arguing the company lacked fair notice that cybersecurity practices can, as a general matter, form the basis of an unfair practice under § 45(a). Wyndham argues instead it lacked notice of what specific cybersecurity practices are necessary to avoid liability. We have little trouble rejecting this claim.

To begin with, Wyndham’s briefing focuses on the FTC’s failure to give notice of its interpretation of the statute and does not meaningfully argue that the statute itself fails fair notice principles. We think it imprudent to hold a 100-year-old statute unconstitutional as applied to the facts of this case when we have not expressly been asked to do so.

Moreover, Wyndham is entitled to a relatively low level of statutory notice for several reasons. Subsection 45(a) does not implicate any constitutional rights here. *Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 499, 102 S.Ct. 1186, 71 L.Ed.2d 362 (1982). It is a civil rather than criminal statute.20 *Id.* at 498–99, 102 S.Ct. 1186. And statutes regulating economic activity receive a “less strict” test because their “subject matter is often more narrow, and because businesses, which face economic demands to plan behavior carefully, can be expected to consult relevant legislation in advance of action.” *Id.* at 498, 102 S.Ct. 1186.

In this context, the relevant legal rule is not “so vague as to be ‘no rule or standard at all.’” *CMR D.N. Corp.*, 703 F.3d at 632 (quoting *Boutilier*, 387 U.S. at 123, 87 S.Ct. 1563). Subsection 45(n) asks whether “the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.” While far from precise, this standard informs parties that the relevant inquiry here is a cost-benefit analysis, *Pa. Funeral Divs. Ass’n v. FTC*, 41 F.3d 81, 89–92 (3d Cir.1994); *Am. Fin. Servs. Ass’n*, 767 F.2d at 975, that considers a number of relevant factors, including the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that would arise from investment in stronger cybersecurity. We ac-

20. While civil statutes containing “quasi-criminal penalties may be subject to the more stringent review afforded criminal statutes,” *Ford Motor Co.*, 264 F.3d at 508, we do not know what remedy, if any, the District Court will impose. And Wyndham’s briefing does not indicate what kinds of remedies it is exposed to in this proceeding.
knowledge there will be borderline cases where it is unclear if a particular company’s conduct falls below the requisite legal threshold. But under a due process analysis a company is not entitled to such precision as would eliminate all close calls. Cf. Nash v. United States, 229 U.S. 373, 377, 33 S.Ct. 780, 57 L.Ed. 1232 (1913) (“[T]he law is full of instances where a man’s fate depends on his estimating rightly, that is, as the jury subsequently estimates it, some matter of degree.”). Fair notice is satisfied here as long as the company can reasonably foresee that a court could construe its conduct as falling within the meaning of the statute.

What appears to us is that Wyndham’s fair notice claim must be reviewed as an as-applied challenge. See United States v. Mazurie, 419 U.S. 544, 550, 95 S.Ct. 710, 42 L.Ed.2d 706 (1975); San Filippo, 961 F.2d at 1136. Yet Wyndham does not argue that its cybersecurity practices survive a reasonable interpretation of the cost-benefit analysis required by § 45(n). One sentence in Wyndham’s reply brief says that its “view of what data-security practices are unreasonable . . . is not necessarily the same as the FTC’s.” Wyndham Reply Br. at 23. Too little and too late.

Wyndham’s as-applied challenge falls well short given the allegations in the FTC’s complaint. As the FTC points out in its brief, the complaint does not allege that Wyndham used weak firewalls, IP address restrictions, encryption software, and passwords. Rather, it alleges that Wyndham failed to use any firewall at critical network points, Compl. at ¶ 24(a), did not restrict specific IP addresses at all, id. at ¶ 24(f), did not use any encryption for certain customer files, id. at ¶ 24(b), and did not require some users to change their default or factory-setting passwords at all, id. at ¶ 24(f). Wyndham did not respond to this argument in its reply brief.

Wyndham’s as-applied challenge is even weaker given it was hacked not one or two, but three, times. At least after the second attack, it should have been painfully clear to Wyndham that a court could find its conduct failed the cost-benefit analysis. That said, we leave for another day whether Wyndham’s alleged cybersecurity practices do in fact fail, an issue the parties did not brief. We merely note that certainly after the second time Wyndham was hacked, it was on notice of the possibility that a court could find that its practices fail the cost-benefit analysis.

Several other considerations reinforce our conclusion that Wyndham’s fair notice challenge fails. In 2007 the FTC issued a guidebook, Protecting Personal Information: A Guide for Business, FTC Response Br. Attachment 1 [hereinafter FTC Guidebook], which describes a “checklist[]” of practices that form a “sound data security plan.” Id. at 3. The guidebook does not state that any particular practice is required by § 45(a), but it does counsel against many of the specific practices alleged here. For instance, it recommends that companies “consider encrypting sensitive information that is stored on [a] computer network . . . [c]heck . . . software vendors’ websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches.” Id. at 10. It recommends using “a firewall to protect [a] computer from hacker attacks while it is connected to the

21. For this reason, we agree with Wyndham that the guidebook could not, on its own, provide ‘ascertainable certainty’ of the FTC’s interpretation of what specific cybersecurity practices fail § 45(n). But as we have already explained, this is not the relevant question.
Internet," deciding "whether [to] install a 'border' firewall where [a] network connects to the Internet," and setting access controls that "determine who gets through the firewall and what they will be allowed to see . . . to allow only trusted employees with a legitimate business need to access the network." Id. at 14. It recommends "requiring that employees use 'strong' passwords" and cautions that "[h]ackers will first try words like . . . the software's default password[ ] and other easy-to-guess choices." Id. at 12. And it recommends implementing a "breach response plan," id. at 16, which includes "[i]nvestigat[ing] security incidents immediately and tak[ing] steps to close off existing vulnerabilities or threats to personal information," id. at 23.

As the agency responsible for administering the statute, the FTC's expert views about the characteristics of a "sound data security plan" could certainly have helped Wyndham determine in advance that its conduct might not survive the cost-benefit analysis.

Before the attacks, the FTC also filed complaints and entered into consent decrees in administrative cases raising unfairness claims based on inadequate corporate cybersecurity. FTC Br. at 47 n.16.

The agency published these materials on its website and provided notice of proposed consent orders in the Federal Register. Wyndham responds that the complaints cannot satisfy fair notice principles because they are not "adjudications on the merits." 22 Wyndham Br. at 41. But even where the "ascertainable certainty" standard applies to fair notice claims, courts regularly consider materials that are neither regulations nor "adjudications on the merits." See, e.g., United States v. Lachman, 387 F.3d 42, 57 (1st Cir.2004) (noting that fair notice principles can be satisfied even where a regulation is vague if the agency "provide[d] a sufficient, publicly accessible statement" of the agency's interpretation of the regulation); Beverly Healthcare–Hillview, 541 F.3d at 202 (citing Lachman and treating an OSHA opinion letter as a "sufficient, publicly accessible statement"); Gen. Elec. Co., 53 F.3d at 1329. That the FTC commissioners—who must vote on whether to issue a complaint, 16 C.F.R. § 3.11(a); ABA Section of Antitrust Law, FTC Practice and Procedure Manual 160–61 (2007)—believe that alleged cybersecurity practices fail the cost-benefit analysis of § 45(n) certainly helps companies with similar practices apprehend the possibility that their cybersecurity could fail as well.23

22. We agree with Wyndham that the consent orders, which admit no liability and which focus on prospective requirements on the defendant, were of little use to it in trying to understand the specific requirements imposed by § 45(a).

23. We recognize it may be unfair to expect private parties back in 2008 to have examined FTC complaints or consent decrees. Indeed, these may not be the kinds of legal documents they typically consulted. At oral argument we asked how private parties in 2008 would have known to consult them. The FTC's only answer was that "if you're a careful general counsel you do pay attention to what the FTC is doing, and you do look at these things." Oral Arg. Tr. at 51. We also asked whether the FTC has "informed the public that it needs to look at complaints and consent decrees for guidance," and the Commission could offer no examples. Id. at 52. But Wyndham does not appear to argue it was unaware of the consent decrees and complaints; it claims only that they did not give notice of what the law requires. Wyndham Reply Br. at 25 ('The fact that the FTC publishes these materials on its website and provides notice in the Federal Register, moreover, is immaterial—the problem is not that Wyndham lacked notice of the consent decrees [which reference the complaints] but that consent decrees [and presumably complaints] by their nature do not give notice of what
Wyndham next contends that the individual allegations in the complaints are too vague to be relevant to the fair notice analysis. Wyndham Br. at 41–42. It does not, however, identify any specific examples. And as the Table below reveals, the individual allegations were specific and similar to those here in at least one of the four or five cybersecurity-related unfair-practice complaints that issued prior to the first attack.

Wyndham also argues that, even if the individual allegations are not vague, the complaints “fail to spell out what specific cybersecurity practices . . . actually triggered the alleged violation, . . . provid[ing] only a . . . description of certain alleged problems that, ‘taken together,’ ” fail the cost-benefit analysis. Wyndham Br. at 42 (emphasis in original). We part with it on two fronts. First, even if the complaints do not specify which allegations, in the Commission’s view, form the necessary and sufficient conditions of the alleged violation, they can still help companies apprehend the possibility of liability under the statute. Second, as the Table below shows, Wyndham cannot argue that the complaints fail to give notice of the necessary and sufficient conditions of an alleged § 45(a) violation when all of the allegations in at least one of the relevant four or five complaints have close corollaries here.


<table>
<thead>
<tr>
<th>CSS</th>
<th>Wyndham</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Created unnecessary risks to personal information by storing it in a vulnerable format for up to 30 days, CSS at ¶ 6(1).</td>
</tr>
<tr>
<td>2</td>
<td>Did not adequately assess the vulnerability of its web application and computer network to commonly known or reasonably foreseeable attacks; did not implement simple, low-cost and readily available defenses to such attacks, CSS at ¶ 6(2)-(3).</td>
</tr>
<tr>
<td>3</td>
<td>Failed to use strong passwords to prevent a hacker from gaining control over computers on its computer network and access to personal information stored on the network, CSS at ¶ 6(4).</td>
</tr>
<tr>
<td>4</td>
<td>Did not use readily available security measures to limit access between computers on its network and between those computers and the Internet, CSS at ¶ 6(5).</td>
</tr>
<tr>
<td>5</td>
<td>Failed to employ sufficient measures to detect unauthorized access to personal information.</td>
</tr>
</tbody>
</table>

Section 5 requires.” (emphases in original, citations and internal quotations omitted).

24. The FTC asserts that five such complaints issued prior to the first attack in April 2008. See FTC Br. at 47–48 n.16. There is some ambiguity, however, about whether one of
In sum, we have little trouble rejecting Wyndham’s fair notice claim.

V. Conclusion

The three requirements in § 45(n) may be necessary rather than sufficient conditions of an unfair practice, but we are not persuaded that any other requirements proposed by Wyndham pose a serious challenge to the FTC’s claim here. Furthermore, Wyndham repeatedly argued there is no FTC interpretation of § 45(a) or (n) to which the federal courts must defer in this case, and, as a result, the courts must interpret the meaning of the statute as it applies to Wyndham’s conduct in the first instance. Thus, Wyndham cannot argue it was entitled to know with ascertainable certainty the cybersecurity standards by which the FTC expected it to conform. Instead, the company can only claim that it lacked fair notice of the meaning of the statute itself—a theory it did not meaningfully raise and that we strongly suspect would be unpersuasive under the facts of this case.

We thus affirm the District Court’s decision.

Background: Professional and amateur sports leagues brought action to enjoin New Jersey from giving effect to law partially repealing state’s prohibitions against sports wagering. The United States District Court for the District of New Jersey, Michael A. Shipp, J., 61 F.Supp.3d 488, entered summary judgment in leagues’ favor and issued permanent injunction. State appealed.
California Data Breach Report

February 2016

Kamala D. Harris, Attorney General
California Department of Justice
California
Data Breach Report
2012-2015

Kamala D. Harris, Attorney General
California Department of Justice

February 2016
# Contents

Message from the Attorney General. ........................................ i

Executive Summary ....................................................... iii

Introduction ................................................................. 1

Findings ........................................................................... 9

Recommendations ......................................................... 27

Appendix A ................................................................. 39

Appendix B ................................................................. 41

Appendix C ................................................................. 51

Notes ................................................................. 61
The California Constitution guarantees every Californian the “inalienable right” to privacy. To ensure that protection, California has been on the cutting edge, adopting the strongest and most sophisticated consumer privacy laws in the United States. But California’s fast-changing economy requires our constant vigilance to ensure that privacy and security protections keep pace with innovation and new threats. Each day, millions of Californians log on to the internet to conduct business, do homework, purchase goods and services, control devices in their homes, play games, and connect with loved ones. Technology such as smartphones, the “internet of things,” wearable devices, and big data are transforming our lives at a rapid pace, while exponentially increasing the amount of personal information that is collected, used, and shared. At the same time, with data becoming more ubiquitous and valuable, the black market for stolen information also continues to expand, increasing the likelihood of hacking by cyber criminals.

With more of our personal information online, it is imperative that organizations employ strong privacy practices. To protect privacy, businesses must have privacy policies that are easy to read and access, inform consumers about material changes to their data handling practices, and carefully select their default settings which often determine how data is collected, used, and shared. Foundational to those privacy practices is information security: if companies collect consumers’ personal data, they have a duty to secure it. An organization cannot protect people’s privacy without being able to secure their data from unauthorized access.

Data breaches, particularly when they involve sensitive information such as Social Security numbers and health records, threaten not only the privacy but also the security and economic wellbeing of consumers. Breaches also impact a wide range of industries, from the health care and financial services sectors to retail and small businesses, and pose a threat to critical infrastructure and national security. Now that organizations rely increasingly on the collection and use of personal information and criminals take advantage of security weaknesses to obtain and profit from that same information, it is more important than ever that all of us redouble our efforts to ensure that this data does not end up in the wrong hands.

The report that follows provides a comprehensive analysis of the data breaches reported to my office from 2012 to 2015. In the last four years, nearly 50 million records of Californians have been breached and the majority of these breaches resulted from security failures.
Furthermore, nearly all of the exploited vulnerabilities, which enabled these breaches, were compromised more than a year after the solution to patch the vulnerability was publicly available. It is clear that many organizations need to sharpen their security skills, trainings, practices, and procedures to properly protect consumers.

Securing data is no doubt challenging, with sophisticated cyber criminals – including some nation states – waging an escalating battle. But many of the breaches reported to us could have been prevented by taking reasonable security measures, and an organization that voluntarily chooses to collect and retain personal information takes on a legal obligation to adopt appropriate security controls.

As we become further immersed in the online world, our lives and our livelihoods depend more and more on our ability to use technology securely. The potential of a digitally connected society is immense, so it is critical that we put the appropriate safeguards in place before individuals feel that they must either abandon their right to privacy or go offline to protect it. This report is a starting point, and a call to action, for all of us—organizations, individuals, and regulators—to work toward a safer and more secure online future.

Sincerely,

Attorney General Kamala D. Harris
Executive Summary

Since 2012, businesses and government agencies have been required to notify the Attorney General on breaches affecting more than 500 Californians. In our latest report, we analyze all such breaches from 2012 through 2015. In it we present our findings on the nature of the breaches that are occurring, what can be learned from them about threats and vulnerabilities, and we make recommendations aimed at reducing the risk of data breaches and mitigating the harms that result from them.

In the past four years, the Attorney General has received reports on 657 data breaches, affecting a total of over 49 million records of Californians. In 2012, there were 131 breaches, involving 2.6 million records of Californians; in 2015, 178 breaches put over 24 million records at risk. This means that nearly three in five Californians were victims of a data breach in 2015 alone.

These breaches occurred in all parts of our economy: retailers and banks, doctors, dentists and hospitals, gaming companies, spas, hotels, restaurants, government agencies, schools, and universities. The majority of the reported breaches were the result of cyber attacks by determined data thieves, many of whom took advantage of security weaknesses. Breaches also resulted from stolen and lost equipment containing unencrypted data, and from both unintentional and intentional actions by insiders (employees and service providers).

Types of Breach

- **Malware and hacking** presents the greatest threat, both in the number of breaches (365, 54 percent) and the number of records breached (44.6 million, 90 percent). This is a growing problem compared to other types of breach, increasing by 22 percent in the past four years, from 45 percent of breaches in 2012 to 58 percent in 2015. The six breaches of more than one million records are all of this type. The retail sector in particular struggles with malware and hacking, which comprises 90 percent of all retailer breaches.

- **Physical breaches**, resulting from theft or loss of unencrypted data on electronic devices, came in a distant second. The relative share of this type of breach declined, from 27 percent of all breaches in 2012 to 17 percent in 2015. The health care sector had the greatest problem with breaches of this type (more than half of all its breaches), and small businesses were more than 50 percent more likely to report a physical breach than were larger businesses.

- **Breaches caused by errors**, predominantly misdelivery (of email, for example) and inadvertent exposure on the public Internet, were a close third, and have held steady at around 17 percent. Half of government breaches were of this type.
Types of Data Breached

- More of the most sensitive personal information – Social Security numbers and medical information – was breached than other data types.

- Social Security numbers were the data type most often breached, involved in just under half of all breaches, for a total of 24 million records containing Social Security numbers. That is nearly half of the 49.6 million records of Californians breached in the four-year period.

- Medical information was included in 19 percent of breaches and 18 million records, and payment card data in 39 percent of breaches and 16 million records.

- As retailers continue their transition to EMV (chip-enabled payment cards), the attractiveness of trying to steal payment card data from in-store systems will decline and the focus of criminals on Social Security numbers will likely increase.

Industry Sectors

- The retail sector had the largest share of breaches, accounting for 25 percent of breaches and 42 percent of records breached in the past four years. Most retail breaches were caused by malware and hacking, and the type of data most commonly breached was payment card data.

- The financial sector accounted for the second largest share of breaches, 18 percent, and for 26 percent of records breached. The sector showed the greatest susceptibility to breaches caused by insiders (employees, service providers), both through unintentional errors and intentional misuse of privileges. The most common type of data breached in this sector was Social Security numbers.

- Health care, with 16 percent of breaches, continued to be particularly vulnerable to physical breaches, although malware and hacking breaches are starting to increase as the sector’s transition to electronic medical records progresses. The most vulnerable information in health care was medical information, such as patient records, and Social Security numbers.

- Despite generally having less data than larger businesses, small businesses were still a significant breach risk and represented 15 percent of all breaches reported. They were most susceptible to hacking and malware attacks, but also experienced physical breaches at a greater rate than larger businesses.
Reasonable Security

Securing data is challenging, with technology evolving rapidly, business practices relying increasingly on the collection and use of personal information, and sophisticated cyber criminals waging an escalating battle. Yet securing information is the ethical and legal responsibility of the organizations with which individuals entrust their personal information. The legal obligations to secure personal information include an expanding set of laws, regulations, enforcement actions, common law duties, contracts, and self-regulatory regimes. California’s information security statute requires businesses to use “reasonable security procedures and practices…to protect personal information from unauthorized, access, destruction, use, modification, or disclosure.” Federal laws, including the Gramm Leach Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA), contain general security requirements for the financial services and health care industries. Authoritative security standards describe the measures that organizations should take to achieve an appropriate standard of care for personal information.

State Breach Laws

As the number of state data breach laws has grown in recent years, there has been an effort to pass a federal law that would preempt state laws. The rationale offered has been a reduction of the burden of complying with the different state laws. The proposals under consideration in Congress, however, have tended to set the bar far below California’s current level of protection. They would also in many cases preempt not only state laws on data breach but also longstanding information security and consumer protection statutes.

Recommendations

1) The 20 controls in the Center for Internet Security’s Critical Security Controls identify a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.

2) Organizations should make multi-factor authentication available on consumer-facing online accounts that contain sensitive personal information. This stronger procedure would provide greater protection than just the username-and-password combination for personal accounts such as online shopping accounts, health care websites and patient portals, and web-based email accounts.
3) Organizations should consistently use strong encryption to protect personal information on laptops and other portable devices, and should consider it for desktop computers. This is a particular imperative for health care, which appears to be lagging behind other sectors in this regard.

4) Organizations should encourage individuals affected by a breach of Social Security numbers or driver’s license numbers to place a fraud alert on their credit files and make this option very prominent in their breach notices. This measure is free, fast, and effective in preventing identity thieves from opening new credit accounts.

5) State policy makers should collaborate to harmonize state breach laws on some key dimensions. Such an effort could reduce the compliance burden for companies, while preserving innovation, maintaining consumer protections, and retaining jurisdictional expertise.
Introduction

Data breaches are growing in scope, affecting more organizations and more people. Much is at stake: data breaches impose financial, reputational, and lost opportunity costs on individuals and organizations. Data breaches also threaten critical infrastructure and imperil national security.

There are real costs to individuals. Victims of a data breach are more likely to experience fraud than the general public, according to Javelin Strategy & Research. In 2014, 67 percent of breach victims in the U.S. were also victims of fraud, compared to just 25 percent of all consumers.

In recognition of this growing threat, starting in 2003, California has required businesses and government agencies to notify California residents when they experience a breach of the residents’ personal information. Since 2012, businesses and government agencies have also been required to notify the Attorney General on breaches affecting more than 500 Californians.

In furtherance of the breach notice law's transparency goals, we post the notices on the Attorney General's website as they are submitted. We also review the breaches, sometimes taking legal action, and always seeking to learn from them. This report is the result of our review and analysis of the 657 data breaches reported to the Attorney General from 2012 through 2015.

In the report we present our findings on the nature of the breaches that are occurring and what can be learned from them about threats and vulnerabilities. We also make recommendations aimed at reducing the risk of data breaches and mitigating the harms that result from them.

California's Breach Notice Law

California was the first to enact a data breach notification law, which took effect in 2003. In the twelve years since then, 46 other states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands, as well as foreign jurisdictions around the world, have enacted similar laws.

The California law's original intent was to give early warning to consumers that they were at risk of identity theft so that they could act to protect themselves. The law's impact, however, has been more far-reaching. The law's transparency requirement has motivated organizations to devote greater attention and additional resources to their data privacy
and security practices and has highlighted data insecurity as a matter of concern for policymakers and the general public.

The law requires any person or business that conducts business in California, and any state or local agency, that owns or licenses “computerized data” that includes personal information to notify any resident of California whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person as the result of a breach of security. Entities that maintain such data are required to notify the owner or licensee of the information in the event of a breach of the data. The complete text of the California law can be found in Appendix C.

Scope of Information Covered

When California’s law first took effect, it focused on the type of information used to commit financial identity theft: Social Security number, driver’s license number, and financial account number. The type of information covered by the law has been updated multiple times since then, in response to emerging threats and rapidly changing technology. In 2008, with awareness of burgeoning medical identity theft and its life-threatening impact for California residents, medical and health insurance information were added to the law’s purview. In 2013, with evidence that criminal organizations were targeting online account credentials, the law was amended to also include a user name or email address, in combination with a password or security question and answer that permits access to an online account. In 2015, in recognition of the growing sensitivity of the location information included in the data, data from automated license plate reader systems was added to the definition in the breach law.

Notification Trigger and Timing

The requirement to notify is triggered by the acquisition, or reasonable belief of acquisition, of personal information by an unauthorized person.

Organizations that own or license the data must notify individuals “in the most expeditious time possible and without unreasonable delay.” The law conveys the need for urgency, and by providing a flexible standard, rather than a bright-line rule, it accommodates realities in particular breach situations. It allows for the time needed to determine the scope of a breach and to secure the system, and provides an option for a delay if law enforcement determines that notifying would impede a criminal investigation. An organization that maintains data on behalf of the data owner or licensee is required to immediately notify the owner or licensee of a suspected breach.
Notification Format and Delivery Method

The law’s provisions are aimed at making notices helpful to recipients. As the notices were seen to be difficult to read and understand and were often lacking key information, the law was amended to require plain language and specific pieces of information that provide what individuals need to know to be able to take appropriate defensive actions:

1) the name and contact information of the notifying organization;
2) the types of personal information involved;
3) contact information for the credit reporting agencies in cases involving a breach of Social Security or driver’s license numbers; and
4) the date of the breach, and a general description of the incident (if known at the time of the notification).

Additional information that may be provided in the notice includes what the organization has done to protect individuals and advice on what individuals can do to protect themselves.

Most recently, in 2015, the law was amended to require the use of a format that improves the readability of the notices.

The law has a preference for notification to take the form of a written notice mailed to individuals, but it is flexible in allowing notification by other means in certain situations. When a breach (i) requires notifying more than 500,000 people, or (ii) providing written notice would cost more than $250,000, or (iii) an organization lacks sufficient contact information, the “substitute notice” method may be used. This method requires posting a notice on the organization’s website, notifying statewide media, and sending a notice to available email addresses. In a breach of online account credentials, online notification may be used instead of a written or substitute notice, since that is the normal mode of communication between the breached organization and those affected.

Breach Victim Protection

In an effort to help breach victims, an amendment was passed in 2014 that requires organizations to offer identity theft prevention and mitigation services in breaches of Social Security or driver’s license numbers. Breaches of these are the types of data put individuals at risk of new credit accounts being opened in their names, among other things, and the required services are intended to address such risks.
Other State Breach Notice Laws

The breach notification laws in the 46 other states are similar in many ways, because most are modeled on the original California law. All of them require notifying individuals when their personal information has been breached, prefer written notification but allow using the "substitute method" in certain situations, allow for a law enforcement delay, and provide an exemption from the requirement to notify when data is encrypted.

There are some differences, primarily in three areas: (i) the notification trigger, (ii) the timing for notification, and (iii) the definition of covered information.

Of the 47 states with breach laws, 36 states (77 percent) use the “harm” trigger for notification, generally allowing an organization to be relieved of its obligation to notify if the organization makes a determination that there is no reasonable risk of harm or misuse of the data. California and 10 other states (23 percent) have a standard of acquisition, or a reasonable belief of acquisition, by an unauthorized person, which can be understood as putting the data at risk of harm.

Most state breach laws (85 percent) have essentially the same notification timing provision as California—in the most expedient time possible, without unreasonable delay. Seven states have an outer boundary time limit for notification of individuals, ranging from 30 to 90 days.

There is a range of definitions of personal information. All state laws include the basic types in the original California law (Social Security number, driver's license number, financial account number). Eight states (17 percent), including California, add medical information, and five (11 percent), including California, add online account credentials. Thirteen states (28 percent), including California, add other types of information, with health insurance information, biometric information, and taxpayer ID being the most common.

In addition, 19 states (40 percent), including California, have specific content requirements for notices. Most require what would logically be included in such a notice: a general description of the breach, the types of personal information involved, what the organization is doing in response, and contact information for the organization and for credit reporting agencies. A few have additional, unique content requirements. For example, the Massachusetts law prohibits disclosing the nature of the breach or the number of residents affected in the notice, and the Wisconsin law requires the notice to tell the recipient to make a written request to learn the personal information involved.

Twenty-five states (53 percent) require a breached organization to notify the state Attorney General and/or another government agency.
Federal Data Breach Proposals

As the number of state laws has grown in recent years, there has been an effort to pass a federal breach notice law that would preempt state laws and set a national uniform standard. The rationale offered has been regulatory simplification and reduction of the burden of complying with the different state laws. The proposals under consideration in Congress, however, have tended to set the consumer protection bar very low. And in many cases they would preempt not only state laws on data breach, but also longstanding information security and consumer protection statutes.

In addition to the overly broad preemptive scope, the federal breach law proposals would infringe on state-based innovation. Over the years, states have proven nimble in responding to rapidly changing circumstances that affect their residents. As discussed earlier, California has made several amendments to the law. Preempting the right of states to make such adjustments in the law would deprive their residents and other jurisdictions of valuable insight and information that can inform timely innovation and adaptation to evolving technology.

Not only would most of the federal proposals lower the level of protection provided below that in states with stronger laws, but residents of other states would lose the benefit they now enjoy from the highest-common-denominator approach many organizations take in multi-state breach responses, in effect affording California-level protections to residents of all states.

The federal proposals tend to use very narrow definitions of harm and of personal information and to set overly rigid timelines for notification. The vast majority of state breach laws have a flexible timing provision, which allows for achieving an appropriate balance. While a specific deadline may be intended to prevent major delay, the outer bound may become the de facto standard for notification. The time needed from discovery to notification is also very fact specific. A deadline of 30 or 45 days would be too long in many cases, and might be too short in others. Furthermore, what constitutes a reasonable time for notification today might be unreasonable tomorrow, as technological improvements allow for faster forensic analysis, cheaper and more effectively targeted notice, and an improved ability by companies to quickly provide consumers with remedies.

Many of the federal proposals would also encroach on enforcement by State Attorneys General. Even when allowing enforcement by State Attorneys General, they would do so with restrictions, such as requiring prior notice to federal agencies and enforcement only in federal court. The states have been leaders in privacy protection and have protected their residents from irreparable harm by enforcing state breach laws. Placing such restrictions on State Attorneys General would unnecessarily hamper their ability to protect consumers.
Update on Previous Breach Reports

EMV Developments

In our 2014 data breach report, in the wake of the series of large retailer breaches of payment card data that occurred in 2013, we encouraged the prompt adoption of the improved security offered by chip-enabled payment cards, also known as EMV (named for the three companies that originated the standard: Europay, MasterCard, and Visa). EMV is a replacement for magnetic stripe cards, offering greater security because stolen mag-stripe data can be used to create counterfeit credit cards. EMV creates a one-time code for each transaction, rendering it impossible to use stolen card data to make counterfeit cards for use at the point of sale. The use of counterfeit cards is the most common type of card fraud, responsible for $3 billion, for 45 percent of U.S. card fraud losses in 2014.6

In our report, we recommended that retailers move promptly to update their point-of-sale terminals to be able to read chip-enabled cards, particularly in light of the October 2015 “liability shift.” Prior to the shift, liability for card fraud among the parties was determined by the card brands (Visa, MasterCard, Discover, and American Express). This shift changed the apportionment of liability to make the party with the lower level of security, that is, the one that has not enabled EMV (retailer or card issuer), liable for the cost of fraud resulting from counterfeit card transactions. Card-issuing banks have upgraded their cards, with 98 percent of total payment cards in the U.S. now bearing chips.7 Retailers have more work to do in upgrading their terminals to accept cards bearing chips, and the full transition to EMV is not expected to be complete until the end of 2017. In the meantime, until all retailer terminals have been upgraded, the new chip cards still also retain the vulnerable magnetic stripe, so we can continue to expect breaches of payment card data at the point of sale for a few more years, until all retail terminals are chip-enabled and the magnetic stripe can be eliminated from cards.

As EMV migration advances, we also anticipate seeing a shift in breach targets from “brick-and-mortar” stores sale to online merchants, where stolen card data retains value because the full account number is used for purchases. Data other than payment card data will also increasingly be targeted. For example, Javelin Strategy & Research predicts that businesses that store or transmit Social Security numbers will become high-value targets.8

Health Care Sector Encryption

In both our previous breach reports, we recommended that the health care sector adopt stronger encryption practices to protect medical information on portable devices and consider it for desktop computers as well. We made this recommendation because we saw
that health care was experiencing a much higher rate of breaches of stolen equipment containing unencrypted data than other sectors. The trend in health care breaches in the past two years suggests some improvement in encryption practices. In 2012, 68 percent of health care breaches were the result of stolen or lost equipment, compared to 21 percent of breaches in all other sectors. In 2015, 39 percent of health care breaches were of this type, while in other sectors it accounted for just 13 percent. There is still a long way to go in addressing this preventable type of breach.

Breach Notices

We also recommended making breach notices easier to understand and strengthening the substitute notice procedure. As previously described, the new addition to California’s breach notification law requires breach notices to use a format that will make them easier to understand by prescribing one of two options: (i) use the title “Notice of Data Breach” and the headers “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information;” or (ii) use the form provided in the statute. In addition, the law requires organizations to maintain substitute notices posted on their websites for a minimum of 30 days, and it defines conspicuous posting as being linked on the home page, with the link distinguished from the rest of the page by color, size of type, or by symbols that draw attention to it.

Resources for Consumers

In last year’s report, we also commented on the particular risk that debit cardholders face in payment data breaches and the inadequacy of the usual advice given in breach notices to protect against this risk. To address this and to provide appropriate guidance for consumers on breaches of all types of data, we published Breach Help: Consumer Tips from the California Attorney General. This information sheet provides specific advice for different types of data breached. Regarding debit card data, the advice is to monitor the account online, promptly report any unauthorized transaction, and consider cancelling the card as the best way to protect the linked bank account. Breach Help is just one of a broad range of privacy resources for consumers, in English and Spanish, available on the Attorney General’s website. For more helpful information, visit [www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy).

Advice on what to do in response to a breach notice is available in Breach Help: Consumer Tips from the California Attorney General, at [www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy).
Findings

As noted earlier, from 2012 through 2015, the Attorney General received reports of 657 data breaches that involved the personal information of more than 500 California residents. After increasing for the previous two years, the number of breaches remained essentially flat in 2015.

Figure 1: Number of Breaches, 2012-2015

While the total number of breaches did not increase in the past year, the total number of Californians affected rose dramatically from 4.3 million in 2014 to over 24 million in 2015.

Figure 2: Number of Records Breached, 2012-2015
Figure 3 shows the mean and median breach size by year. While the median breach size has been fairly steady at between 2,000 and 3,000 records, the mean was much higher in 2013 and 2015, due to a few larger breaches.

The jump in size from 2012 to 2013, as discussed in our last breach report, is attributable to two very large breaches at two retailers, LivingSocial and Target, each involving the information of approximately 7.5 million Californians. This explains the considerable difference between the mean (average) breach size in 2013 of 117,621 and the median of 2,388. If the two outliers were omitted, the total number affected for 2013 would have been 3.5 million instead of 18.5 million with a mean of 21,000. In 2014, the largest reported breach, at Shutterfly, affected just under one million Californians.

Breaches reported in 2015 account for half of the over 49 million Californians affected in the past four years. In 2015, there were four incidents that each breached the information of over two million Californians: Anthem at 10.4 million was the largest, followed by UCLA Health at 4.5 million, next was PNI Digital Media with 2.7 million Californian customers of online photo centers (Costco, RiteAid, and CVS) that it services, and finally, T-Mobile/Experian at 2.1 million.
Breach Types

As in previous reports, we categorize breaches by type, as seen in Figure 4 below. \(^9\)

- **Malware and hacking breaches** are caused by intentional intrusions into computer systems by unauthorized outsiders.

- **Physical breaches** result from the theft or loss of unencrypted data stored on laptops, desktop computers, hard drives, USB drives, data tapes or paper documents.

- **Error breaches** stem from anything insiders (employees or service providers) unintentionally do or leave undone that exposes personal information to unauthorized individuals.

- **Misuse breaches** are the result of trusted insiders intentionally using privileges in unauthorized ways.

**Figure 4: Breaches by Type, 2012-2015**

![Pie chart showing Breaches by Type, 2012-2015]

**Malware and Hacking**

More than half of the reported breaches in the past four years are categorized as malware and hacking. This type has accounted for the largest share of breaches every year. This type of breach affected over 44 million records, 90 percent of all records breached. The six biggest breaches are all of this type and together comprise over 70 percent of all records breached. See Figure 5.
Physical Theft and Loss

Breaches resulting from physical theft and loss are the next largest segment, accounting for 22 percent of all breaches from 2012 to 2015. Physical breaches accounted for 2.8 million records, or six percent of all records of Californians breached.

Miscellaneous Errors

Breaches resulting from errors by insiders (employees, service providers) made up 17 percent of total breaches and four percent (two million) of total records breached. As shown in Figure 6, misdelivery of personal information to an unintended recipient, whether by email, postal mail, fax, or other means, was the most common type of error. It comprised 46 percent of the error breaches and eight percent of all breaches, was. The next most common type of error breach is the unintentional posting of information on a public website,
making up 35 percent of error breaches and six percent of all breaches. Other errors that account for the remaining breaches of this type include failing to shred documents or “wipe” digital data from devices when discarding them, and allowing unauthorized employees to have access to data.

Misuse

Misuse of access privileges by insiders accounted for the smallest share of breaches, at seven percent. This type of breach put over 206,000 records of Californians at risk, representing less than one percent of total records breached.

Key Trends in Breach Types

As seen in Figure 7, the incidence of malware and hacking breaches has trended generally up, almost doubling from 2012 to 2015. At the same time, the share of breaches resulting from physical loss and theft has gone down, from 27 percent of breaches in 2012 to 17 percent in 2015. This may reflect a more widespread and effective use of encryption to protect data in transit.

Figure 7: Type of Breach by Year, 2012-2015
As Figure 8 shows, the biggest breaches by far were the result of malware and hacking. Physical breaches came in a distant second, accounting for six percent of records, followed by error breaches at four percent, and breaches resulting from intentional misuse by insiders at under one percent.

**Figure 8: Type of Breach by Number of Records Breached, 2012-2015**

Malware and hacking were the major threat in both share of breaches (54 percent) and share of records breached (90 percent), as shown in Figure 9. While physical breaches were the next most common type, at 22 percent, they tend to be smaller than malware and hacking breaches, accounting for just six percent of total records breached. Breaches caused by insiders, whether from unintentional errors or intentional misuse, are also smaller.
Data Types

The types of data covered by California’s breach law are (i) name, plus Social Security number, driver’s license number, financial account number (such as bank account numbers and payment card numbers), medical information, or health insurance information; and (ii) credentials for online accounts (user ID or email address, plus password or security question and answer).\(^{10}\)

Social Security numbers are among the most sensitive data types, because their abuse is the most difficult type of fraud for consumers to detect, protect against, and recover from. When a single credit or debit card account number is stolen, the victim can discover it in the next bill (if not earlier) and can stop the fraud by closing the account. It is a different story for stolen Social Security numbers. In the hands of identity thieves, Social Security numbers, and to a lesser extent driver’s license numbers, can be used for a variety of purposes. They enable thieves to open new credit accounts, take out loans, apply for and receive government benefits, among other things – all in the victim’s name. They can also be used for other fraudulent purposes, including taking over existing bank accounts and getting health care or government benefits. Criminals have provided stolen Social Security numbers when arrested, resulting in the creation of fraudulent criminal records in the victim’s name. Such uses can take months or sometimes years to detect. Even when detected, undoing the damage can be very challenging because it is almost never possible to change...
your Social Security number. So while the identified fraud may be repaired, the stolen number remains useful to criminals, who can re-victimize individuals repeatedly for years.

Social Security numbers continue to figure significantly in data breaches, and were involved in nearly half (48 percent) of all breaches and in 47 percent of records breached, as shown in Figure 10. Over 18 million Social Security numbers were breached in 2015, primarily in the large incidents at Anthem, UCLA Health, and T-Mobile/Experian. There has been a slow decline in the incidence of Social Security number breaches in the past four years. In 2012, 56 percent of breaches involved Social Security numbers and in each subsequent year this percentage decreased, comprising 43 percent of all breaches in 2015. As noted in the discussion of EMV developments, however, this may rise again in the coming years.

Payment card data was the next mostly likely data type to be breached, and was involved in 39 percent of all breaches. Medical or health insurance information, which most individuals regard as very sensitive, comprised a larger share of records breached, 36 percent compared to 32 percent for payment data.

Driver’s license numbers figured in 11 percent of breaches and 17 percent of records breached. Online account credentials, a data type that was added to the breach law in 2014, were involved in nine percent of breaches. The higher incidence of this data type in records breached, 24 percent, is largely attributable to the big LivingSocial breach in 2013 and the PNI Digital (Costco, RiteAid, CVS) breach in 2015.

**Figure 10: Type of Data by Share of Breaches and Records, 2012-2015**

![Bar chart showing the percentage of breaches and records for different types of data from 2012 to 2015.]

*Note: Total is greater than 100% because some breaches involved more than one data type.*
Looking at the raw numbers, we see that records containing the most sensitive information were breached in larger quantities: 24 million records containing Social Security numbers and nearly 18 million containing medical or health insurance information, as shown in Figure 11. Payment card data is next, in nearly 16 million breached records. More than 12 million breached records included online account credentials.

**Figure 11: Number of Records Breached by Data Type, 2012-2015**

![Graph showing number of records breached by data type]

**Industry Sectors**

We classify the organizations that report breaches to the Attorney General according to the U.S. Census Bureau’s North American Industry Classification System. As shown in Figure 12, the retail industry has seen the largest share of breaches throughout the four-year period, averaging 25 percent of all the breaches in our dataset. The finance sector, which includes insurance, represented 18 percent of the breaches and health care a similar 16 percent. Professional services accounted for seven percent, and government, hospitality, and education five percent each. All other sectors made up 19 percent of total breaches, although none of them accounted for more than 4 percent.
The large size of many of the retail breaches from 2012 to 2015 is evident in Figure 13 as the sector’s share of breaches is only 25 percent but its share of records breached is 42 percent (21 million records). The financial sector, which includes insurance, also had disproportionately larger breaches, with 18 percent of total breaches but 26 percent of all records. The large Anthem breach in 2015 is a major driver here; without that breach, finance’s total share of all records would drop to six percent. The health care sector’s share of records breached (14 percent) is slightly less than its share of breaches (16 percent).
Figure 14 shows the types of breach that occurred within each industry sector. While malware and hacking was the dominant type of breach (54 percent), it did not dominate all sectors. This type accounted for nearly all breaches in the retail sector (90 percent) and for a significant share of breaches in most other sectors. The exceptions are health care and government, where only 16 percent of breaches were of this type.

The incidence of physical breaches also differed across sectors. Over the four years, these incidents of stolen or lost documents or digital devices containing unencrypted data accounted for 22 percent of all breaches, but make up 54 percent of the breaches in health care. Professional services and government also experienced a significant rate of this type of breach, at 32 percent each.

Error breaches were most common in the government and finance sectors, at 50 and 31 percent, respectively.

Breaches resulting from intentional misuse by insiders were a small share in every sector, with only finance and health care seeing a double digit incidence, at 14 and 10 percent, respectively.

We took a closer look at the three largest industry sectors: retail, finance, and health care because together they represented just under 60 percent of all breaches and over 80 percent of records breached. The three sectors have notably different profiles, differing both by type of breach and by type of data involved.
Retail Sector Breaches

There were 163 retail breaches in the four-year period, constituting 25 percent of all breaches, and 90 percent of them were caused by malware and hacking. This is more than twice the rate of other sectors for this type of breach, as shown in Figure 15.

Figure 15: Retail Sector vs. all Others by Type of Breach, 2012-2015

The retail sector breaches were also the largest – involving 21 million records of Californians, 42 percent of the total of over 49 million. Two of the largest breaches were at retailers, Target and LivingSocial, together accounting for 15 million of the records breached.

Most of the retail breaches (83 percent) involved payment card data, with 10 percent (including the LivingSocial breach) involving online account credentials, and 7 percent Social Security numbers.

Financial Sector Breaches

The financial sector, which also includes insurance, accounted for 18 percent (118) of the breaches and 26 percent of the records breached (13 million records). It has a notably different breach profile than retail. As shown in Figure 16, the sector had a significantly lower incidence of hacking and malware – the dominant type of breach – compared to all other sectors (37 percent of its total compared to 58 percent), and just over one third
the incidence of hacking and malware breaches as retail. Breaches resulting from errors by insiders, however, were more than twice as common as in other sectors (31 percent versus 14 percent). The financial sector also experienced nearly three times the share of breaches caused by insiders abusing their access privileges: 14 percent compared to five percent in all others.

The type of data most commonly involved was Social Security numbers, which figured in 75 percent of financial sector breaches.

**Figure 16: Financial Sector vs. all Others by Type of Breach, 2012-2015**

![Figure 16](image)

**Health Care Sector Breaches**

The health care sector accounted for 16 percent of breaches (103) and 14 percent (6.8 million) of Californians’ records breached over the four years.

As we have noted in previous reports, the health care sector differs from the others in having a significantly higher incidence of breaches resulting from physical theft and loss: 54 percent compared to just 16 percent in all other sectors. See Figure 17.
Physical breaches have declined in health care in the past two years, from a high in 2013 of 72 percent of all health care breaches compared to 18 percent in all other sectors, to 39 percent in 2015, compared to 13 percent in other sectors. The industry appears to be improving in its use of encryption to protect data on laptops and other portable devices, but there is still a long way to go in addressing this preventable type of breach.

At the same time, the incidence of malware and hacking breaches in health care has been rising, from five percent in 2012 to 21 percent in 2015. As the transition to electronic medical records continues, the health care sector will increasingly face the same challenges in securing digital data that other sectors have been grappling with for several years. Given the extreme sensitivity of the data involved in health care breaches, this is a challenge that the industry must meet.

Health care breaches tend to involve the most sensitive types of personal information. Social Security numbers figure in 50 percent of health care breaches, and medical information in 69 percent.

Small Businesses

In order to see whether the experience of small businesses with data breach is different from that of larger businesses, we used the Small Business Administration’s size standards to identify the small businesses in our dataset.12 While there are differences for different
industry sectors and revenues are also a factor, small businesses are generally those with fewer than 500 employees. Government agencies and non-profit organizations are not covered by the SBA standards, and we were not able to confirm the status of some businesses. We distinguished three groups by size: (i) known small businesses; (ii) known larger businesses; and (iii) government agencies, non-profits, and businesses of unconfirmed size.

As shown in Figure 18, 16 percent of the organizations in our dataset are confirmed as small businesses and 56 percent as larger, or non-small, businesses. The share of small businesses increased over the four years, from 12 percent in 2012 to 17 percent in 2015. This may indicate that hackers are increasingly also targeting more vulnerable small businesses, given they often have fewer resources to dedicate to security, and/or it may reflect a growing awareness among small businesses of the requirement to notify the Attorney General of data breaches, which became law in 2012.

**Figure 18: Breaches by Size of Business, 2012-2015**

Small businesses differed from larger businesses in having a smaller share of financial sector entities and larger shares of health care and professional services. As shown in Figure 19, 18 percent of the small businesses in our dataset were financial, compared to 24 percent of larger businesses. On the other hand, 28 percent of small businesses were in health care, compared to 17 percent of larger businesses, and 14 percent were in professional services, compared to eight percent for larger entities.
We found that small businesses were more likely to have breaches resulting from physical theft and loss, as shown in Figure 20. This may be attributable to some extent to the industry makeup of the group. Small businesses show a larger representation of health care and professional services, both sectors that experience physical breaches at a higher rate than other sectors.

**Figure 19: Industry Sector by Size of Business, 2012-2015**

![Figure 19: Industry Sector by Size of Business, 2012-2015](image)

**Figure 20: Type of Breach by Size of Business, 2012-2015**

![Figure 20: Type of Breach by Size of Business, 2012-2015](image)
Not surprisingly, small businesses had smaller breaches, involving a total of just over one million records, compared to 46 million for larger businesses. The mean (average) small business breach involved 9,850 records, compared to 123,704 for larger businesses.

**Additional Findings**

*Identity Theft Prevention and Mitigation Services*

The new breach law requirement that companies must offer identity theft services to victims in certain breaches appears to be having an impact. From 2012 through 2014, organizations did not provide such services in 30 percent of breaches of Social Security or driver’s license numbers. As shown in Figure 21, when the law took effect in 2015, the failure rate dropped to half that, 15 percent.

![Figure 21: Social Security & Driver’s License Number Breaches Where Identity Theft Prevention Services Not Offered, 2012-2015](image)

**Timing of Notification**

The law requires notifying individuals of a breach “in the most expedient time possible and without unreasonable delay.” The average (mean) time from discovery of a breach to notification of those affected was 40 days, and the median was 30 days. In 25 percent of the breaches consumers were notified in 16 days or less, and in 75 percent of them notification was made in 50 days or less. The time from discovery to notifying the Attorney General was similar, 44 days on average, with a median time of 31 days. These figures are for the 73 percent of breaches for which we have the date of discovery.
Substitute Notice

Organizations in nearly all of the 657 breaches reported provided notice by mail directly to individuals; the substitute notice method was used in 33 breaches (five percent). In those instances, organizations delivered the notice via websites, the news media, and sometimes also email. Retailers accounted for 12 of the substitute notices, restaurants and hotels for 12, with the others from a variety of sectors. All but three of the substitute notices were for breaches of payment card data, where the method was likely used because of insufficient contact information to permit direct written notices. The other three involved online account credentials.

Notification of Law Enforcement

Organizations report having notified law enforcement in 62 percent of breaches (340), and filing a police report in 26 percent (172). All state laws allow for a delay in notification if law enforcement says notifying would impede an investigation. The use of such a delay was reported in just seven percent (44) of the breaches in our dataset. The average time to notify those affected in such cases was 60 days, compared to 40 days when there was no law enforcement delay.

Repeaters

Over the four years, 24 organizations reported two data breaches. There were five organizations that reported three (California Correctional Health Care Services, California Department of Public Health, HSBC Bank, St. Joseph Health System, Yolo Federal Credit Union), one that reported four (California Department of Corrections and Rehabilitation), and two that reported five (Kaiser and Massachusetts Mutual Life Insurance Company). This does not include card-issuing financial institutions such as American Express and Discover that notified their cardholders of payment data breaches that occurred at merchants.
Recommendations

In reviewing four years of data breaches, we have seen certain patterns that suggest lessons to be learned. We offer these recommendations to organizations as part of the collective effort to improve privacy and security practices and reduce the number, size, and impact of data breaches. The first recommendation concerns a minimum standard of care for personal information. The next three recommendations encourage organizations to adopt specific practices that can help consumers, by reducing the risk of a breach and/or mitigating the impact when breaches do occur. The final recommendation addresses the proliferation of state breach laws and proposed federal legislation.

(1) Reasonable Security: The Standard of Care for Personal Information

As data breaches continue and the stakes increase, organizations must be vigilant and proactive to ensure more effective protection for personal information and other critical data. This starts with basic privacy practices. Limiting the personal information collected and retained can provide the strongest protection; if an organization does not have data, the data cannot be breached. But good privacy practices are also reliant on a foundation of good security: an organization cannot protect people's privacy without being able to secure their information from unauthorized access.

Security is challenging.

Securing information in the online world is very challenging. The adversaries are sophisticated. Large criminal enterprises, including transnational organizations and even nation-states, are engaged in attacking our information assets and stealing data. Their motivations are varied, running the gamut from financial gain, to corporate espionage, business disruption, and even cyber warfare. Cyber threats are constantly evolving, and the fight is asymmetrical, with organizations having to protect their systems against everything all the time, while an attacker only has to be successful once.

There are also internal challenges, both technological and human. Organizational information assets and data have become widely distributed in multiple locations, including outside the organization's physical control (e.g., in the cloud and on the hand-held devices of employees and vendors). This exposure is exacerbated by an emerging data-driven business model, where organizations are amassing huge quantities of information and retaining it for possible future use, sometimes indefinitely. In addition, employees and vendors can be careless in their handling of personal information or are able to intentionally steal information by taking advantage of security holes.
Furthermore, security solutions are complex, requiring integrating technology with processes to ensure that the technology is properly deployed and used. For example, some breaches of retail point-of-sale systems have resulted from installation errors by equipment installers, even though the technology itself was not faulty.

Security is a responsibility.
While there is no perfect security, organizations have a responsibility to protect personal information. External adversaries cause most data breaches, but this does not mean that organizations are solely victims; they are also stewards of the data they collect and maintain. People entrust businesses and other organizations with their data on the understanding that the organizations have a both an ethical and a legal obligation to protect it from unauthorized access.

Neglecting to secure systems and data opens a gateway for attackers, who take advantage of uncontrolled vulnerabilities. In its annual Data Breach Investigations Reports, Verizon has regularly pointed out that 99.9 percent of exploited vulnerabilities were compromised more than a year after the controls for the vulnerability had been publicly available. If organizations choose to amass data, and then fail to uphold their responsibilities as data stewards, they are also culpable.

The legal obligation to secure information is contained in an expanding set of laws, regulations, enforcement actions, common law duties, contracts, and self-regulatory regimes. California has an information security statute (California Civil Code § 1798.81.5) that requires all businesses that collect personal information on California residents to use “reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction use, modification, or disclosure.”

There are major federal information security laws and related regulations, including the Gramm Leach Bliley Act (GLBA) for the financial services industry, the Health Insurance Portability and Accountability Act (HIPAA) for health care entities and their business associates, and the Federal Information Security Management Act (FISMA) for federal agencies.

Just like California law, the federal legal regimes invoke a concept of providing “reasonable” and/or “appropriate” information security in order to fulfill an organization’s responsibilities.

Regulators have also offered security guidance. The Federal Trade Commission has drawn lessons from more than 50 of its security enforcement actions to develop a best practices guide entitled Start with Security: A Guide for Business. The Federal Communications Commission developed tips for smaller organizations which it published in Cybersecurity
for Small Business. The California Attorney General has provided recommendations on how smaller businesses can reduce their risk of cyber security incidents in Cybersecurity in the Golden State.

Security is a process. Information security laws and regulations generally require a risk management approach. In essence, this means organizations must develop, implement, monitor, and regularly update a comprehensive information security program. The required security risk management process generally includes the same basic steps, starting with assigning responsibility for information security within the organization, and continuing as follows:

1) **Identify** information assets and data to be secured.
2) **Assess** risks to the assets and data.
3) **Implement** technical, administrative, and physical controls to address identified risks.
4) **Monitor effectiveness** of controls and update as risks, business practices, and controls evolve.

*Figure 22: Security Risk Management Process*
Security is based on standards.
The risk management process will only achieve reasonable security if the risks to information assets and data are identified and effective security controls are implemented. That’s where standards come in. Security standards define the scope of security controls, the criteria for evaluating their effectiveness, the techniques for ongoing assessment and monitoring, and the procedures for dealing with security failures.17

There are a number of authoritative information security standards that organizations can and do use to develop their programs. These standards are updated periodically and are aligned on the basic security process and the defensive controls to be implemented. Among the best known standards are those published by the National Institute of Standards and Technology (NIST), in particular Special Publication 800-53 and the Framework for Improving Critical Infrastructure Cybersecurity.18 The International Organization for Standardization’s ISO/IEC 27002:2013 is also foundational.19 In addition to the comprehensive technical standards, there are catalogs and lists of known security vulnerabilities.20

While there is no dearth of information on the security risk management process and standards for security controls, synthesizing all of this information and prioritizing the actions to take can be a challenge. The Center for Internet Security’s Critical Security Controls for Effective Cyber Defense (the Controls) is designed to address this challenge.21

**Recommendation 1:**
The 20 controls in the Center for Internet Security’s Critical Security Controls define a minimum level of information security that all organizations that collect or maintain personal information should meet. The failure to implement all the Controls that apply to an organization’s environment constitutes a lack of reasonable security.

Formerly known as the SANS Top 20, the Controls are now managed by the Center for Internet Security (CIS), a non-profit organization that promotes cybersecurity readiness and response by identifying, developing, and validating best practices.22 The Controls were originally developed by federal agencies in 2008 and since then have been the product of a public-private partnership that includes cyber security experts from government and the private sector in the U.S., as well as around the world.

Informed by lessons learned from actual attacks and breaches, the Controls are a consensus list of the best defensive controls to detect, prevent, respond to, and mitigate damage from cyber attacks. They are updated periodically to keep up with technological advances.
and changing threats, and are aligned with the most authoritative comprehensive security standards and legal requirements. (See Appendix B.)

Overview of the CIS Critical Security Controls

The Controls are a recommended set of 20 security measures with a high payoff; they are the priority actions that should be taken as the starting point of a comprehensive program to provide reasonable security. In a SANS report on adoption and implementation of the Controls, they are described as providing “the prioritized guidance that cost-conscious executives are looking for when determining where best to invest their limited technology budgets.” Adopters also reported valuing the Controls for providing a clear way to present and manage progress on security and risk posture.

Implementing the Controls will not prevent every attack, but it will significantly reduce the risk and impact of the commonly occurring breaches we have seen in the past several years. The set of 20 Controls constitutes a minimum level of security – a floor – that any organization that collects or maintains personal information should meet.

The Controls are listed in priority order, and they act in concert. For example, in order to be able to protect data on laptops and other portable devices (the twelfth Control, called CSC 12), an organization must first know what devices it has and where they are (CSC 1).

The Center for Internet Security provides specific guidance and resources for implementing the Controls. Each Control is presented with an explanation of why it is critical, followed by specific actions (sub-controls), and by procedures and tools for implementing it. A set of tools for implementing the first five controls, which are the first steps to take, has been developed specifically for small organizations.

The controls are intended to apply to organizations of all sizes and are designed to be implementable and scalable. The depth and complexity of the specific actions (called sub-controls) are greater for larger entities and for entities that maintain highly sensitive personal information. Organizations can implement the controls by adopting the sub-controls that fit the size, complexity, and criticality of their systems, as well as the nature of their data. For example, while a small business might take an inventory of its computers and other devices with a manual count, a larger organization could use an automated process to identify the equipment connected to its network.

The following table summarizes the Controls, grouped by the type of action they feature. The complete list of Controls is found in Appendix A.
Our review of the 657 data breaches reported to the Attorney General in the past four years suggests that many could have been prevented or at least detected and corrected more rapidly had the basic security measures in the Controls been implemented.

**Malware and Hacking Breaches**

More than half the breaches in our dataset were the result of malware and hacking, the intentional unauthorized intrusion into computer systems by outsiders. As previously noted, breaches of this type were responsible for 90 percent of the records put at risk, affecting nearly 45 million California residents.

There are multiple vulnerabilities that can enable this type of breach. One is the role of insiders in responding to social engineering. One such exploit, phishing, has been recognized as a key delivery vector for malware for several years. Employees are tricked into clicking on a link in a phishing email that downloads malicious software. Verizon reports that 23 percent of recipients now open phishing emails and 11 percent click on the attachments. Phishing is also used to trick employees into giving up their credentials, allowing attackers to steal data from their computers. Thieves use personal information gleaned from social media and other sources to identify insiders with administrative access privileges, targeting them for spear-phishing to get their credentials or posing as them to get access to critical systems.

There are security controls that address this vulnerability. Training employees to recognize phishing attacks is, of course, vital (CSC 17). Limiting administrative privileges to a strict job-required basis reduces the number of “super-user” employees who can be spear-phished (CSC 5).

In addition, strong authentication is a control that protects against the use of stolen credentials (CSC 5, CSC 7). Multi-factor or multi-channel authentication for administrators...
and for employees or vendors with remote access to internal systems requires adding an out-of-channel mechanism, such as a text message sent to a cellphone to get a one-time-use code. An attacker would not only have to phish for user ID and password, but would also have to physically steal the employee’s cellphone.

Other preventive measures include creating a software inventory, “whitelisting” the authorized programs and then preventing unauthorized software from being installed or executed on the system (CSC 2) and securely configuring equipment to prevent the exploitation of open ports or default passwords (CSC 3).

Unsupported and unpatched software is a serious vulnerability. Keeping up-to-date in patching newly discovered security vulnerabilities is critical (CSC 4). This includes upgrading to new versions of browsers and other critical software when earlier versions are no longer supported and patched. Applications exposed to the public Internet present a significant threat vector, and it is critical that organizations use up-to-date, patched and supported browsers. When an older browser version is no longer supported by a developer, security gaps go unaddressed and users are left exposed to data leaks and breaches.

Other basic measures also contribute to a strong defense, including boundary defenses (CSC 12) and controlling ports and other vulnerable access points (CSC 9). Maintaining and analyzing audit logs also allows for early detection of the use of stolen credentials, brute-force attacks on passwords, and other anomalous activity on the network (CSC 6).

**Physical Theft and Loss Breaches**

Breaches resulting from unencrypted data on stolen or lost devices are particularly prevalent in the health care sector and they tend to involve the most sensitive types of information, Social Security numbers and medical information. As we have noted in previous data breach reports, breaches of this time are preventable. Applicable controls include inventorying devices, and using encryption to protect the data, particularly on mobile devices (CSC 1) (CSC 13). Implementing these controls could have protected more than 2.7 million California residents whose personal information was put at risk by these avoidable breaches.

**Error Breaches**

Many breaches resulting from errors can be prevented or their impact mitigated by several controls. Errors by insiders that resulted in breaches included sending information by email...
to unintended persons, disposing of digital devices without first “wiping” the data, and unintentionally making information available to unauthorized persons by posting it on a website. Errors like these led to 111 breaches, affecting more than two million Californians in the past four years. Security controls that would be particularly effective in addressing these vulnerabilities include training and awareness directed to staff and vendors who handle sensitive information (CSC 17), and using strong encryption and data loss prevention software (CSC 13). Monitoring the flow of data (CSC 13) can flag and even prevent the unintentional (or intentional, for that matter) emailing of unencrypted Social Security numbers and other personal information outside the network.

**Misuse Breaches**

Breaches caused by employees or service providers who intentionally make unauthorized use of privileges or resources are also addressed by the Controls. Limiting access privileges on a “least privilege” basis (i.e., the minimal level of access that allows users to do their specific jobs), along with monitoring with a particular focus on the limited number of privileged “super users,” are critical (CSC 4, CSC 5). Also relevant are the strategic use of encryption to protect sensitive data and the deployment of automated tools at perimeters to monitor for sensitive data leaving the network and block unauthorized attempts to exfiltrate it (CSC 13). These and others of the Controls would reduce the risk of internal misuse of access, a type of breach that affected over 200,000 California residents.

While the analysis above is certainly not exhaustive, it is offered to show that a significant portion of the breaches that put the personal information in over 49 million records at risk in the past four years were the result of the exploitation of known vulnerabilities for which there are known controls.

**(2) Multi-Factor Authentication**

**Recommendation 2:**

Organizations should not only use multi-factor authentication to protect critical systems and data, but should also make it available on consumer-facing online accounts that contain sensitive personal information. Such accounts include online shopping accounts, health care websites and patient portals, and web-based email accounts.
The combination of username and password is currently the most basic way to authenticate individuals in the online world, to verify that they are who they say they are. Its effectiveness as a security measure relies on the user's ability to devise passwords unique to each account, ensure that the passwords are sufficiently complex, change them periodically, keep them secret, and remember all of the user's username/password combinations. It also requires the organizations that rely on password authentication to secure those usernames and passwords.

This authentication system is failing. We don't use unique passwords for each of our accounts because it would simply be too hard to remember them all. This makes successfully hacked online account credentials very valuable to data thieves, because stolen credentials for one account often allow access to many others.

Making matters worse, many individuals do not use strong passwords that are difficult to guess. For several years, the most common passwords have been “123456,” “password,” “12345678,” “qwerty,” and “12345.” Nor do individuals change their passwords as often as they should. And organizations do not always take appropriate measures to protect passwords. Accordingly, we have seen many breaches over the past few years in which hackers targeted huge repositories of online account credentials that were not adequately secured.

A stronger form of online authentication uses multiple factors, from independent categories of credentials. Multi-factor authentication pairs “something you know,” such as a password or PIN, with “something you have,” such as your cellphone or a physical one-time-password token, or “something you are,” such as a biometric like a fingerprint. For example, after inputting a password, the user receives a text on his or her cellphone, providing a one-time-use code to enter to log into the account. This means that for hackers or thieves to be successful, they would not only have to acquire the password but would also have to steal the victim's phone. Financial institutions have used multi-factor authentication for access to online bank accounts for nearly a decade, sometimes supplementing username and password with biometrics such as “keystroke dynamics” that recognizes a user's unique typing pattern or with other factors, such as a one-time-password generator.

This form of authentication should be used by all organizations to help protect access to critical systems and sensitive data, such as medical information, financial information, Social Security numbers, as well as company confidential information like intellectual property and trade secrets. Multi-factor authentication is included in the CIS Critical Security Controls for administrative access (CSC 5.6), organizational email accounts (CSC 7), remote login access to company systems (CSC 12.6), and user accounts on the company network (CSC 16.11).
Multi-factor authentication should also be more widely available for consumer-facing online accounts that contain sensitive personal information. Such accounts include online shopping accounts, health care web sites and patient portals, and web-based email accounts.

We want to draw particular attention to the importance of protecting individuals’ email accounts. Our email accounts serve as our online calling card, as we shop, bank, and use social networks. Someone who takes over another person’s email account can move around the Internet masquerading as that person. Access to an email account also provides a treasure trove of information to use in phishing and other social engineering exploits, as well as information on financial accounts that can be used to take them over. Many, but not all, of the major consumer email providers offer multi-factor authentication. We recommend that the others do so as well, promptly.

(3) Encryption of Data in Transit

Recommendation 3:
Organizations, particularly health care, should consistently use strong encryption to protect personal information on laptops and other portable devices, and should consider it for desktop computers.

We made the recommendation to encrypt data in transit in our previous breach reports, and although improvement appears to have been made, there are still some sectors lagging behind. As discussed above, encryption is a key Control for protecting data on portable devices (CSC 13).

Government and professional services experience breaches resulting from stolen or lost equipment containing unencrypted data at a higher rate than the average for breaches in all sectors.

But the most striking, and most disturbing, example is health care. More than half (55 percent) of the breaches in this sector are the result of a failure to encrypt, compared to just 16 percent of breaches in all other sectors. Moreover, this sector’s breaches involve the most sensitive types of personal information: medical information and Social Security numbers.

As we have said in the past, breaches of this type are preventable. Affordable solutions are widely available: strong full-disk encryption on portable devices and desktop computers when not in use.²⁸ Even small businesses that lack full time information security and IT staff can do this. They owe it to their patients, customers, and employees to do it now.
Recommendation 4: Organizations should encourage those affected to place a fraud alert on their credit files when Social Security numbers or driver’s license numbers are breached.

As discussed earlier in the report, the transition to the use of more secure EMV payment cards will increase the criminal demand for Social Security numbers, and the abuse of Social Security numbers is the most difficult type of fraud for consumers to detect, protect against, and recover from.

There are services for consumers that offer early detection of new account fraud, and we are seeing that Californians are now more likely to receive the benefit of such services. As discussed earlier, in 2015 a new law took effect that requires an organization that is the source of a breach of Social Security numbers or driver’s license numbers to offer identity theft prevention and mitigation services at no cost to the affected individuals for no less than 12 months. Since then, we have seen over a 20 percent increase in these services being offered in such breaches.

These identity theft prevention and mitigation services generally include credit monitoring, which alerts consumers to new account activity in their credit records, and remediation assistance in the event of actual identity theft. A credit freeze is the strongest protection against new account fraud, but for some individuals the freeze can be cumbersome, as it must be lifted (for a fee) whenever an individual wants to apply for new credit, insurance, or employment.

There is an additional measure, which is free, fast, and effective in preventing new account fraud: a fraud alert. A fraud alert provides protection against the use of a stolen Social Security number to apply for and open new accounts. Consumers can place a fraud alert on their credit files with a single phone call or online. When a merchant checks the credit history of someone applying for credit the merchant gets a notice that there may be fraud on the account. This alerts the merchant to take steps to verify the identity of the applicant. Providing additional identification is generally difficult for an identity thief, which is why the fraud alert is effective. An alert lasts for 90 days and can be renewed.

Many of the notices on Social Security or driver’s license number breaches sent in 2015 do mention the availability of a fraud alert, but the information is most often buried in the
details about ordering credit reports and enrolling in the identity theft prevention and mitigation service offered. We recommend that all organizations encourage notice recipients to place a fraud alert in this type of breach, and make the information on how to do it more prominent in their notices.

(5) Harmonizing State Breach Laws

Recommendation 5:
State policy makers should collaborate in seeking to harmonize state breach laws on some key dimensions. Such an effort could preserve innovation, maintain consumer protections, and retain jurisdictional expertise.

The proliferation of state data breach notification laws has led to calls for regulatory simplification. Proposals in Congress would set a uniform standard by preempting state laws on data breach and often on data security as well. The standards proposed, however, would lower the bar, thereby providing less consumer protection for Californians, and because in multi-state breaches the highest standard tends to prevail, less protection for residents of other states as well.

An alternative approach to achieving the goal of easing the compliance burden is to harmonize state breach laws on some key dimensions. While the state laws have often been characterized as a “patchwork,” there is a clear pattern to that patchwork as we discussed in our analysis of all the state data breach notification laws. Furthermore, compliance with the highest standard typically meets the obligations of a number of lower standards, thus minimizing the number of patches in the quilt. We recommend that state-level policy makers including state legislators and Attorney Generals’ offices collaborate in identifying opportunities to highlight the common pattern and reduce some of the differences. Such an effort could result in simplifying compliance, while preserving consumer protections, flexibility in adapting to changing threats, and the benefits of jurisdictional expertise.
## Appendix A

### The CIS Critical Security Controls for Effective Cyber Defense

<table>
<thead>
<tr>
<th>CSC 1</th>
<th>Inventory of Authorized and Unauthorized Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC 2</td>
<td>Inventory of Authorized and Unauthorized Software</td>
</tr>
<tr>
<td>CSC 3</td>
<td>Secure configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers</td>
</tr>
<tr>
<td>CSC 4</td>
<td>Continuous Vulnerability Assessment and Remediation</td>
</tr>
<tr>
<td>CSC 5</td>
<td>Controlled Use of Administrative Privileges</td>
</tr>
<tr>
<td>CSC 6</td>
<td>Maintenance, Monitoring, and Analysis of Audit Logs</td>
</tr>
<tr>
<td>CSC 7</td>
<td>Email and Web Browser Protection</td>
</tr>
<tr>
<td>CSC 8</td>
<td>Malware Defenses</td>
</tr>
<tr>
<td>CSC 9</td>
<td>Limitation and Control of Network Ports, Protocols, and Services</td>
</tr>
<tr>
<td>CSC 10</td>
<td>Data Recovery Capability</td>
</tr>
<tr>
<td>CSC 11</td>
<td>Secure Configurations for Network Devices such as Firewalls, Routers, and Switches</td>
</tr>
<tr>
<td>CSC 12</td>
<td>Boundary Defense</td>
</tr>
<tr>
<td>CSC 13</td>
<td>Data Protection</td>
</tr>
<tr>
<td>CSC 14</td>
<td>Controlled Access Based on the Need to Know</td>
</tr>
<tr>
<td>CSC 15</td>
<td>Wireless Access Control</td>
</tr>
<tr>
<td>CSC 16</td>
<td>Account monitoring and Control</td>
</tr>
<tr>
<td>CSC 17</td>
<td>Security Skills Assessment and Appropriate Training to Fill Gaps</td>
</tr>
<tr>
<td>CSC 18</td>
<td>Application Software Security</td>
</tr>
<tr>
<td>CSC 19</td>
<td>Incident Response and Management</td>
</tr>
<tr>
<td>CSC 20</td>
<td>Penetration Tests and Red Team Exercises</td>
</tr>
</tbody>
</table>

*The CIS Critical Security Controls for Effective Cyber Defense, Version 6.0, October 15, 2015, is available from the Center for Internet Security at www.cisecurity.org/. The document is licensed under a Creative Commons Attribution—Non Commercial—No Derivatives 4.0 International Public License. The link to the license terms can be found at https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode.*
## Appendix B

### The Critical Security Controls Master Mapping (Excerpt)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>-------------------------------</td>
<td>-----------------</td>
<td>-------------------</td>
<td>----------------</td>
<td>--------</td>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------</td>
<td>---------------------</td>
<td>----------------</td>
<td>-------</td>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------</td>
<td>---------------------</td>
<td>----------------</td>
<td>-------</td>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>SC-39: Process Isolation</td>
<td>DE.CM-4</td>
<td>A.12.2.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SC-44: Detonation Chambers</td>
<td>DE.CM-5</td>
<td>A.13.2.3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SI-3: Malicious Code Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SI-4: Information System Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SI-8: Spam Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA-7: Continuous Monitoring</td>
<td>DE.AE-1</td>
<td>A.13.1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA-9: Internal System Connections</td>
<td></td>
<td>A.13.1.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CM-2: Baseline Configuration</td>
<td></td>
<td>A.14.1.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CM-6: Configuration Settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CM-8: Information System Component Inventory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SC-20: Secure Name /Address Resolution Service (Authoritative Source)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SC-21: Secure Name /Address Resolution Service (Recursive or Caching Resolver)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SC-22: Architecture and Provisioning for Name/Address Resolution Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SC-41: Port and I/O Device Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SI-4: Information System Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------</td>
<td>---------------------</td>
<td>---------------</td>
<td>-------</td>
<td>-------------------------</td>
<td>------------</td>
</tr>
<tr>
<td><strong>CSC 10:</strong> Data Recovery Capability</td>
<td>CP-9: Information System Backup</td>
<td>PR.IP-4</td>
<td>A.10.1.1</td>
<td>164.308(a)(7): Contingency Plan - Data Backup Plan R</td>
<td>Encryption</td>
<td>4.3</td>
</tr>
<tr>
<td></td>
<td>MP-4: Media Storage</td>
<td></td>
<td></td>
<td>164.308(a)(7): Contingency Plan - Testing and Revision Procedure A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>164.310(d)(1): Device and Media Controls - Data Backup and Storage A</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CSC 11:</strong> Secure Configurations for Network Devices</td>
<td>AC-4: Information Flow Enforcement</td>
<td>PR.AC-5</td>
<td>A.9.1.2</td>
<td></td>
<td>Network Security</td>
<td>1.1-1.2</td>
</tr>
<tr>
<td></td>
<td>CA-3: System Interconnections</td>
<td>PR.IP-1</td>
<td>A.9.1.2</td>
<td></td>
<td></td>
<td>2.2</td>
</tr>
<tr>
<td></td>
<td>CA-7: Continuous Monitoring</td>
<td>PR.PT-4</td>
<td>A.13.1.1</td>
<td></td>
<td></td>
<td>6.2</td>
</tr>
<tr>
<td></td>
<td>CA-9: Internal System Connections</td>
<td></td>
<td>A.13.1.3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CM-2: Baseline Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CM-3: Configuration Change Control</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CM-5: Access Restrictions for Change</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CM-6: Configuration Settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CM-8: Information System Component Inventory</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MA-4: Nonlocal Maintenance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SC-24: Fail in Known State</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SI-4: Information System Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------</td>
<td>---------------------</td>
<td>-----------------</td>
<td>-------</td>
<td>-------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>CSC 12:</strong> Boundary Defense</td>
<td>AC-4: Information Flow Enforcement</td>
<td>PR.AC-3</td>
<td>A.9.1.2</td>
<td>Network</td>
<td>1.1-1.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AC-17: Remote Access</td>
<td>PR.AC-5</td>
<td>A.12.4.1</td>
<td>Security</td>
<td>8.3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AC-20: Use of External Information Systems</td>
<td>PR.MA-2</td>
<td>A.12.7.1</td>
<td>Security</td>
<td>10.8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA-3: System Interconnections</td>
<td>DE.AE-1</td>
<td>A.13.1.1</td>
<td>Monitoring</td>
<td>11.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA-7: Continuous Monitoring</td>
<td></td>
<td>A.13.1.3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA-9: Internal System Connections</td>
<td></td>
<td>A.13.2.3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CM-2: Baseline Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SA-9: External Information System Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SC-7: Boundary Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SC-8: Transmission Confidentiality and Integrity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SI-4: Information System Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CSC 13:</strong> Data Protection</td>
<td>AC-3: Access Enforcement</td>
<td>PR.AC-5</td>
<td>A.8.3.1</td>
<td>164.308(a)(4): Information Access Management - Isolating Health care Clearinghouse Function R</td>
<td>3.6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>AC-23: Data Mining Protection</td>
<td>PR.DS-5</td>
<td>A.10.1.2</td>
<td>164.312(a)(1): Access Control - Encryption and Decryption A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA-7: Continuous Monitoring</td>
<td>PR.PT-2</td>
<td>A.13.2.3</td>
<td>164.312(e)(1): Transmission Security - Integrity Controls A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA-9: Internal System Connections</td>
<td></td>
<td>A.18.1.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R-9: Information Spillage Response</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MP-5: Media Transport</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SA-18: Tamper Resistance and Detection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SC-8: Transmission Confidentiality and Integrity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SC-28: Protection of Information at Rest</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SC-31: Covert Channel Analysis</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SC-41: Port and I/O Device Access</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SI-4: Information System Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------</td>
<td>---------------------</td>
<td>-----------------</td>
<td>-------</td>
<td>-----------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>CSC 14: Controlled Access Based on the Need to Know</td>
<td>AC-1: Access Control Policy and Procedures</td>
<td>PR.AC-4</td>
<td>A.8.3.1</td>
<td>164.308(a)(1): Security Management Process - Information System Activity Review R</td>
<td>1.3-1.4</td>
<td>4.3</td>
</tr>
<tr>
<td>AC-6: Least Privilege</td>
<td>PR.DS-2</td>
<td></td>
<td>164.312(a)(1): Access Control - Encryption and Decryption A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC-24: Access Control Decisions</td>
<td>PR.PT-2</td>
<td></td>
<td>164.312(c)(1): Integrity - Mechanism to Authenticate Electronic Protected Health Information A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CA-7: Continuous Monitoring</td>
<td>PR.PT-3</td>
<td></td>
<td>164.312(a)(1): Access Control - Automatic Logoff A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MP-3: Media Marking</td>
<td></td>
<td></td>
<td>164.312(d): Person or Entity Authentication - R</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RA-2: Security Categorization</td>
<td></td>
<td></td>
<td>164.312(e)(1): Transmission Security-Integrity Controls A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SI-4: Information System Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

47
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>-------------------------------</td>
<td>-------------------</td>
<td>---------------------</td>
<td>-----------------</td>
<td>-------</td>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------</td>
<td>----------------------</td>
<td>----------------</td>
<td>-------</td>
<td>--------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>CSC 19:</strong> Incident Response and Management</td>
<td>IR-1: Incident Response Policy and Procedures</td>
<td>PR.IP-10</td>
<td>A.6.1.3</td>
<td>164.308(a)(6): Security Incident Procedures - Reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IR-2: Incident Response Training</td>
<td>DE.AE-2</td>
<td>A.7.2.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IR-3: Incident Response Testing</td>
<td>DE.AE-4</td>
<td>A.16.1.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IR-4: Incident Handling</td>
<td>DE.AE-5</td>
<td>A.16.1.4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IR-5: Incident Monitoring</td>
<td>DE.CM-1-7</td>
<td>A.16.1.7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IR-6: Incident Reporting</td>
<td>RS.RP-1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IR-7: Incident Response Assistance</td>
<td>RS.CO-1-5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IR-8: Incident Response Plan</td>
<td>RS.AN-1-4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IR-10: Integrated Information Security Analysis Team</td>
<td>RS.MI-1-2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>CSC 20:</strong> Penetration Tests and Red Team Exercises</td>
<td>CA-2: Security Assessments</td>
<td>A.14.2.8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA-5: Plan of Action and Milestones</td>
<td>A.18.2.1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA-6: Security Authorization</td>
<td>A.18.2.3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA-8: Penetration Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>RA-6: Technical Surveillance Countermeasures Survey</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>SI-6: Security Function Verification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PM-6: Information Security Measures of Performance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PM-14: Testing, Training, &amp; Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This table is excerpted from the Critical Security Controls Master Mappings Tool, available at [http://www.cisecurity.org/critical-controls/tools/AuditScripts_CISControlv6_Mappings.xlsx](http://www.cisecurity.org/critical-controls/tools/AuditScripts_CISControlv6_Mappings.xlsx). It is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.
Appendix C

California Data Breach Notification Statutes
Civil Code Section 1709.29

a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described in paragraph (2) under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (i), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[FORM OMITTED]
(E) For an electronic notice described in paragraph (2) of subdivision (i), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies, if the breach exposed a social security number or a driver’s license or California identification card number.

(3) At the discretion of the agency, the security breach notification may also include any of the following:

(A) Information about what the agency has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.

(e) Any agency that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(f) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.
(g) For purposes of this section, “personal information” means either of the following:

1. An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
   A. Social security number.
   B. Driver’s license number or California identification card number.
   C. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
   D. Medical information.
   E. Health insurance information.
   F. Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

2. A user name or email address, in combination with a password or security question and answer that would permit access to an online account.

(h) 1. For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

2. For purposes of this section, “medical information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

3. For purposes of this section, “health insurance information” means an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.

4. For purposes of this section, “encrypted” means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

(i) For purposes of this section, “notice” may be provided by one of the following methods:

1. Written notice.
2. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.
3. Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information.
Substitute notice shall consist of all of the following:

(A) Email notice when the agency has an email address for the subject persons.

(B) Conspicuous posting, for a minimum of 30 days, of the notice on the agency's Internet Web site page, if the agency maintains one. For purposes of this subparagraph, conspicuous posting on the agency's Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

(C) Notification to major statewide media and the Office of Information Security within the Department of Technology.

(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for an online account, and no other personal information defined in paragraph (1) of subdivision (g), the agency may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached to promptly change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the agency and all other online accounts for which the person uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for login credentials of an email account furnished by the agency, the agency shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the agency knows the resident customarily accesses the account.

(j) Notwithstanding subdivision (i), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

(k) Notwithstanding the exception specified in paragraph (4) of subdivision (b) of Section 1798.3, for purposes of this section, “agency” includes a local agency, as defined in subdivision (a) of Section 6252 of the Government Code.
California Civil Code Section 1798.82

(a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language, shall be titled “Notice of Data Breach,” and shall present the information described in paragraph (2) under the following headings: “What Happened,” “What Information Was Involved,” “What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[FORM OMITTED]
(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver’s license or California identification card number.

(G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

(3) At the discretion of the person or business, the security breach notification may also include any of the following:

(A) Information about what the person or business has done to protect individuals whose information has been breached.

(B) Advice on steps that the person whose information has been breached may take to protect himself or herself.
(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, “personal information” means either of the following:

1. An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
   - (A) Social Security number.
   - (B) Driver’s license number or California identification card number.
   - (C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.
   - (D) Medical information.
   - (E) Health insurance information.
   - (F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5.

2. A user name or email address, in combination with a password or security question and answer that would permit access to an online account.
(i) For purposes of this section, “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, “medical information” means any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, “health insurance information” means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

(4) For purposes of this section, “encrypted” means rendered unusable, unreadable, or indécipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.

(j) For purposes of this section, “notice” may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the person or business has an email address for the subject persons.

(B) Conspicuous posting, for a minimum of 30 days, of the notice on the Internet Web site page of the person or business, if the person or business maintains one. For purposes of this subparagraph, conspicuous posting on the person’s or business’s Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.

(C) Notification to major statewide media.
(4) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for an online account, and no other personal information defined in paragraph (1) of subdivision (h), the person or business may comply with this section by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer.

(5) In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (h) for login credentials of an email account furnished by the person or business, the person or business shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method described in this subdivision or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account.

(k) Notwithstanding subdivision (j), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.
Notes


2 Privacy enforcement actions are posted on the Attorney General’s website when they are final, at https://oag.ca.gov/privacy/privacy-enforcement-actions.

3 In some breaches, more than one organization notified those affected. For example, in the 2015 Anthem breach, in addition to Anthem’s notice, seven employers for which Anthem was a service provider submitted notices that they’d sent to their employees, resulting in eight sample notices for the single Anthem breach submitted to the Attorney General. Also in 2015, a breach at a service provider to a number of California wineries resulted in 23 notices being submitted from different wineries. Similarly, a breach in a service provider to major drug stores resulted in three notices submitted by the different stores. In some payment data breaches at retailers or restaurants, card-issuing banks also notified their cardholders, resulting in multiple sample notices for the same breach being submitted to the Attorney General. In such cases of multiple notifications of a single breach, all the notices submitted are published on the website at www.oag.ca.gov/ecrime/databreach/list. For analytical purposes, however, each breach was counted only once. Thus the total number of breaches reported to the Attorney General from 2012 through 2015 is 657, while the number of sample notices published on the website for the same period is 699.

4 The three U.S. states without breach notice laws as of the end of 2015 are Alabama, Mew Mexico, and South Dakota.

5 See legislative committee analyses of SB 1386 (Peace) and AB 700 (Simitian) of 2002, at www.leginfo.legislature.ca.gov.

6 Lost and stolen cards used at the point of sale made up 12 percent of card fraud losses, and card-not-present fraud (online, phone) 43 percent, see http://tsoys.com/engenuity-journal/chip-and-pin-vs-chip-and-signature-a-rivalry-nears-historic-proportions.cfm.


8 Javelin Strategy & Research, op.cit., p. 6.

9 The categories of breaches are based generally on Verizon’s Vocabulary for Event Recording and Incident Sharing (VERIS) Framework, a taxonomy designed to provide a common language for describing security incidents. Because of limitations in our knowledge of the details of some breaches, we did not use the full spectrum of VERIS categories. For more on VERIS, see http://veriscommunity.net/.
As of January 1, 2016, the definition of personal information in the breach law also includes data from automated license plate reader systems, along with a name.

The North American Industry Classification System (NAICS) sectors used in the breach report are Retail, Finance and Insurance, Health Care, Professional Services, Government (Public Administration), Hospitality (Accommodation and Food Service), Education, and Other. The Other category includes agriculture, utilities, information, manufacturing, wholesale trade, transportation, real estate and waste management, no one of which accounted for more than 5 percent of the breaches in our dataset. The most recent version of the NAICS is available at www.census.gov/cgi-bin/ ssisd/naics/naicsrch?chart=2012.

The Small Business Administration has established size standards for for-profit industries, based on annual receipts and number of employees. The standards are set according to the North American Industry Classification System (NAICS) code for a business. The size standards are used to determine eligibility for the SBA programs; see more at www.sba.gov/category/navigation-structure/contracting/contracting-officials/small-business-size-standards.


On the other hand, the Massachusetts data security regulations require businesses to follow a process to develop a comprehensive written information security program, but also include some specific measures to be included in the program. See Massachusetts General Law Chapter 93H and implementing regulations 201 CMR 17.00 et seq.


In addition to the CIS Critical Security Controls, the Center for Internet Security manages the Multi-State Information Sharing and Analysis Center (MS-ISAC) used by state governments, and the CIS Security Benchmarks. More at www.cisecurity.org/.

A mapping of the CIS Critical Security Controls to NIST SP 800-53, the NIST Framework, ISO 27002, HIPAA, the Federal Financial Institutions Examination Council Examiners Handbook, and several other security standards is available at www.cisecurity.org/critical-controls/tools/AuditScripts_CISControlv6_Mappings.xlsx.


In an effort to assist smaller organizations, the Center and the National Governors Association have launched a National Cyber Hygiene Campaign, a plain-language, low-cost approach to basic cyber security that focuses on the first five controls. The Campaign is developing Tool Kits, which are works in progress, including instructions, technical guidance, links to additional resources, and tips on measuring the implementation and effectiveness of the controls. Information on the National Campaign for Cyber Hygiene is available at www.cisecurity.org/cyber-pledge/.


In a recent case, the FTC settled with a provider of dental office management software, alleging that Henry Schein Practice Solutions, Inc., falsely advertised the level of encryption used to protect patient data. The complaint referenced NIST’s Advanced Encryption