Data Privacy and Security:

A Practical Guide for In-House Counsel

2018 Edition

David Zetoony

BRYAN CAVE

bryancave.com | A Global Law Firm

TABLE OF CONTENTS

ABOUT THE AUTHOR

David Zetoony is a partner at Bryan Cave LLP where he leads the firm's international data privacy and security practice. Mr. Zetoony has helped hundreds of clients respond to data security incidents, and has defended inquiries concerning the data security and privacy practices of corporations. He is the author of a leading handbook on data breach response – the Washington Legal Foundation's Data Security Breaches: Incident Preparedness and Response – and the premier research handbooks on data privacy and security class action litigation. He represents clients from a variety of industries ranging from national department stores to international outsourcers.

INTRODUCTION

Five years ago few legal departments were concerned with – let alone focused on – data privacy or security. Most of those that were aware of the terms assumed that these were issues being handled by IT, HR, or marketing departments.

The world has changed. Data privacy class action litigation has erupted and data security breaches dominate the headlines. It is now well accepted that data privacy and data security issues threaten the reputation, profitability, and, sometimes, the operational survival of organizations. It is therefore perhaps not surprising to find that in almost every survey conducted of boards and senior management, data issues rank as one of their three top concerns, if not their single greatest concern. With that backdrop, organizations increasingly look to general counsel to manage data privacy and security risks.

The result has been that many in-house attorneys unexpectedly find themselves responsible for a topic about which they have little experience or training. Coming up-to-speed can be difficult. There are well over 200 laws (just in the United States) that have data privacy and security implications. Whereas very few (if any) law schools offered a single data privacy and security course fifteen years ago, the topic has now matured into its own field of study and field of practice. It's simply not possible to sit down and read a single statute to get caught up.

When we published this handbook for the first time in 2016 in conjunction with the Washington Legal Foundation it received an overwhelming response. In less than a year it had been downloaded by over 3,500 in-house attorneys. Last year's edition saw that number nearly double to over 6,000 attorneys. We are extremely proud of the fact that the handbook has become a desk reference for in-house attorneys worldwide.

The 2018 version includes updates to most sections to account for changes in the law and includes a number of new sections dealing with topics that have grown in popularity, or entered the data privacy and security scene. As with our prior versions, the discussion under each topic is not intended to be a legal treatise. Instead, each section provides a straight-forward overview of the law relevant to that topic, statistics to help understand the issue and benchmark its importance, and a functional list of bullet points or questions to immediately break down an issue. We hope that the handbook provides useful and practical guidance when addressing data-related issues.

DATA PRIVACY

1. Autonomous Vehicles – Data Privacy Issues

In the next five years we will see more and more self-driving vehicles, or autonomous vehicles, hit the market. An "autonomous vehicle" is a vehicle capable of navigating roadways and interpreting traffic-control devices without a driver actively operating any of the vehicle's control systems. Although self-driving vehicles have the potential to drastically reduce accidents, travel time, and the environmental impact of road travel, concerns remain that could delay widespread adoption. Of particular concern are data privacy and security risks.

Seventeen states—Arkansas, California, Colorado, Connecticut, Delaware, Maine, Montana, Nevada, New Hampshire, New Jersey, New York, North Dakota, Oregon, Texas, Utah, Virginia, and Washington—and the District of Columbia have enacted statutes relating to the data privacy issues of data retrieval from event data recorders ("EDRs").[1] EDRs capture driver behavior information, such as the speed of a vehicle, braking pattern, and collision information. These states require obtaining the consent of the vehicle owner or policyholder before one can download data collected from a motor vehicle's EDR. Although these seventeen states have addressed issues relating to data privacy by regulating data retrieval from EDRs, only North Dakota has enacted legislation that specifically mentions "data privacy." That legislation requires the department of transportation to study the data and information stored and gathered by the use of self-driving vehicles.

In addition to these seventeen states, automotive industry representatives have passed their own self-regulatory guidelines to address the data privacy issues of self-driving vehicles. In 2014 the Alliance of Automobile Manufacturers and the Association of Global Automakers enacted a set of "Privacy Principles" for vehicle technology and services.[2] Participating automobile manufacturers commit to comply with seven Privacy Principles, which govern the collection, use, and disclosure of driver behavior information retrieved from self-driving vehicles. These seven Privacy Principles are listed below.

Along with the states and the automotive industry that have enacted regulations regarding data privacy and self-driving vehicles, the federal government has also addressed these unique privacy issues. In December 2016 the National Highway Traffic Safety Administration released a proposal to mandate privacy measures relating to vehicle-to-vehicle (V2V) communications technology, which is used between self-driving vehicles to communicate the speed and location of each vehicle, the number of passengers in each vehicle, and more.[3] Amongst other things, the proposal establishes a system that issues, distributes, and revokes security credentials for V2V devices and reports misbehavior. Additionally, the Federal Trade Commission and the NHTSA held a joint workshop on June 28, 2017 to examine the

---

[1] Seventeen States - Arkansas (Ark. Code § 23-112-107); California (Calif. Veh. Code § 9951); Colorado (CRS § 12-6-401—403); Connecticut (CGS § 14-164aa); Delaware (Del. Code § 3918); Maine (Me. Rev. Stat. Ann. Tit. 29-A § 1971—73); Montana (Mont. Code § 61-12-1001—1004); Nevada (Nev. Rev. Stat. § 484D.485); New Hampshire (N.H. Rev. Stat. § 357-G:1); New Jersey (N.J. Stat. § 39:10B-7—9 (2015 A.B. 3579)); New York (NY Veh. & Traffic Code § 416-b); North Dakota (N.D. Cent. Code § 51-07-28, N.D. 2015 H.B. 1065); Oregon (Ore. Rev. Stat. § 105.925—948); Texas (Tex. Trans. Code § 547.615); Utah (Utah Code § 41-1a-1501—1504); Virginia (Va. Code. §§§§ 38.2-2212(C)(s), 38.2-2213.1, 46.2-1088.6, 46.2-1532.2), and Washington (Wash. Code § 46.35.010—050)—and the District of Columbia (DC ST § 50-2351). *See also Autonomous Vehicles—Self-Driving Vehicles Enacted Legislation*, National Conference of State Legislatures (June 5, 2017), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx.

[2] Auto Alliance Driving Innovation, *Privacy Principles for Vehicle Technologies and Services*, https://autoalliance.org/connected-vehicles/automotive-privacy-2/principles/.

[3] National Highway Traffic Safety Administration, *U.S. DOT advances deployment of Connected Vehicle Technology to prevent hundreds of thousands of crashes*, https://www.nhtsa.gov/press-releases/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands.

consumer privacy and security issues posed by self-driving vehicles.[4] The workshop brought together various stakeholders, including industry representatives, consumer advocates, academics, and government regulators to discuss numerous issues related to self-driving vehicles that collect data.

75%	33	17	$137 billion
The estimated percentage of road traffic that will be occupied by self-driving vehicles by 2040.[5]	The number of states to date that have introduced legislation relating to self-driving vehicles.[6]	The number of states as of December 2016 that have introduced legislation relating to both self-driving vehicles and data privacy.[7]	The amount of money by which the autonomous vehicle technology could shrink the auto insurance sector by 2050.[8]

Privacy Principles enacted by the Alliance of Automobile Manufacturers and the Association of Global Automakers:

1. Transparency - Members should provide owners and registered users with ready access to clear, meaningful notices about the member's collection, use, and sharing of covered information.
2. Choice - Members should offer owners and registered users with certain choices regarding the collection, use, and sharing of covered information.
3. Respect for Context - Members should use and share covered information in ways that are consistent with the context in which the covered information was collected, taking account of the likely impact on owners and registered users.
4. Data Minimization - Members should collect covered information only as needed for legitimate business purposes and retaining covered information no longer than they determine necessary.
5. Data Security - Members should implement reasonable measures to protect covered information against loss and unauthorized access or use.
6. Integrity and Access - Members should implement reasonable measures to maintain the accuracy of covered information and give owners and registered users reasonable means to review and correct personal subscription information.
7. Accountability - Members should take reasonable steps to ensure that they and other entities that receive covered information adhere to these Privacy Principles.

Questions to consider when addressing data privacy issues of self-driving vehicles:

1. What type of information regarding driver behavior information do self-driving vehicles collect, store, and transmit?

---

[4] Federal Trade Commission, *Connected Vehicles: Privacy, Security Issues Related to Connected, Automated Vehicles* (October 23, 2017), https://www.ftc.gov/news-events/events-calendar/2017/06/connected-vehicles-privacy-security-issues-related-connected.

[5] Institute of Electrical and Electronics Engineers, *You Won't Need a Driver's License by 2040* (Sep. 15, 2014), http://sites.ieee.org/itss/2014/09/15/you-wont-need-a-drivers-license-by-2040/.

[6] National Conference of State Legislatures, *Autonomous Vehicles: Self-Driving Vehicles Enacted Legislation* (June 26, 2017), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx.

[7] National Conference of State Legislatures, *Privacy of Data From Event Data Recorders: State Statutes* (Dec. 12, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx.

[8] KPMG, *The Chaotic Middle: The Autonomous Vehicle and Disruption in Automobile Insurance* (June 27, 2017), https://home.kpmg.com/us/en/home/insights/2017/05/the-chaotic-middle-autonomous-vehicle-disruption-automobile-insurance.html?sf94340166=1.

2. Can someone track an individual or a vehicle through access to driver behavior information?
3. How do consumers benefit from the collection and use of their driver behavior information?
4. Who owns driver behavior information and what are their rights to its usage?
5. Will your company be required to grant law enforcement access the driver behavior information?
6. If you have access to driver behavior information, how will you use this information? Will your company use it to serve advertisements?
7. Will the driver behavior information be provided to insurance companies for underwriting purposes or to third parties that develop some kind of a driving score related to where and when individuals travel?
8. How will your company communicate its privacy policies and practices with regard to driver behavior information to consumers?

2. Bring Your Own Device ("BYOD") Policies

Many companies permit their employees to use personal mobile devices, such as smartphones and tablets, to access company-specific information, such as email, under a Bring Your Own Device ("BYOD") policy. BYOD policies can be popular for employees that want to use hand-picked devices and for employers that want to avoid the cost of providing, and maintaining, company-owned devices. Nonetheless, the use of company data on employee owned devices implicates both security and privacy considerations.

23% Percentage of employees that are given corporate-issued smartphones.[9]	39% Percentage of companies that reported "security concerns" were the main inhibitor to full BYOD adoption.[10]	40% The percent of companies that offer BYOD to all employees.[11]
56 Minutes The amount of time per day that one study found employees waste using their mobile device for non-work activity.[12]		~60% Percent of employees that reported they use their mobile devices to access websites blocked by their company.[13]

Consider the following when deciding upon a BYOD policy:

1. **Is the scope of your organization's control over employees' mobile devices consistent with the organization's interest?** Organizations should think about how much interest they have an interest in knowing about their employees' mobile devices.

[9] Gartner, Press Release: Gartner Survey Shows that Mobile Device Adoption in the Workplace is Not yet Mature (Nov. 29, 2016), https://www.gartner.com/newsroom/id/3528217.

[10] Crowd Research Partners, BYOD & Mobile Security at 9 (2016), http://www.crowdresearchpartners.com/wp-content/uploads/2016/03/BYOD-and-Mobile-Security-Report-2016.pdf.

[11] Id. at 7.

[12] Business Daily News, "How Much Time Are Your Employees Wasting on Their Phones?" (July 20, 2017), https://www.businessnewsdaily.com/10102-mobile-device-employee-distraction.html.

[13] Id.

The company's legitimate interest in information can be the basis from which a BYOD policy emerges. For example if the organization simply wants to allow an employee to access work email on a mobile device, then the policies and restrictions should proceed with that focus.

2. **To what extent and for what purpose does the organization monitor employees' use of mobile devices?** Many servers create logs showing when an employee's device accessed the organization's server using certain authentication credentials. As security measures such logs are often appropriate. To the extent that the organization wants to monitor more substantive actions by an employee on a mobile device, such monitoring should be in line with an appropriate purpose.

3. **What procedures are in place to restrict the transfer of data from the organization's network by way of the mobile device?** Organizations often protect against the risk that the organization's data will be "floating" on multiple devices by (a) limiting the types of data accessible to mobile devices (*e.g*., email) and (b) restricting, to the extent possible, how that data can be used on the mobile device (*e.g*., policies on copying and requiring certain security settings). For example, some organizations use sandboxed applications for accessing work-related email. Such apps open email in a program that is separate and apart from the native email system that is built-into the device and they control aspects of the user's experience. For example, they may restrict the user from locally saving any emails, or attachments, to the user's device.

4. **For security purposes, does the organization require a minimum version of the operating system to be in place, and for that version to be fully patched, before an employee can use a mobile device?** Minimum versions ensure that certain security protections and bug fixes are present on the device.

5. **Can data on a mobile device be remotely wiped? By whom?** A best practice for devices that contain confidential or sensitive organization information is to ensure that the data can be remotely deleted from the device by the organization if, for example, the device is stolen or the employee is terminated. This may be relatively easy for some organizations. For example, organizations that use sandboxed application that permit employees to access email on the company's server – but do not store or cache data locally – can typically be deactivated relatively easily and in a manner that does not allow an unauthorized person who may possess the mobile device to gain any access to the company's system. To the extent that an employee was permitted to locally store work-related data (*e.g.,* cache work emails locally, or download attachments), an employer should consider whether it has the right, and the technical means, to remotely wipe the entire device.

6. **What procedure is in place for an employee to report a missing mobile device?** Accidents happen to everyone, but their aftermath can determine whether they become catastrophes. Employees should report a missing device to someone – perhaps the IT department or help desk – so that the organization's device removal policy can be followed.

7. **What steps does the organization take to proliferate its mobile device policies?** Organizations often rely on their IT staff, self-help materials, and employee certifications to ensure (a) employee awareness of the organization policies and (b) enforcement of organization policies.

8. **Do the security measures in place match the sensitivity of the data accessed through the mobile device?** For employees that receive non-sensitive information minimal restrictions may be appropriate. For employees that receive sensitive or confidential information higher restrictions may be appropriate.

9. **Does your BYOD policy facilitate a wage and hour dispute?** Although BYOD programs are widely lauded for increased productivity and "off-the-clock" accessibility, this benefit can expose employers to potential wage-and-hour issues if the BYOD user is a nonexempt employee. If a nonexempt employee is permitted to use a mobile device for work related purposes after working hours, is there a policy that mandates that the employee must report the time that he or she worked? Is there an effective and efficient means for the employee to report such time?

10. **Does the BYOD policy expose the company to additional discovery costs?** In the event that the organization is involved in litigation or a government investigation it could receive a request that the company review its electronic files for evidence that may be relevant to the case. In some situations, a BYOD policy may expose the employee's personal information – e.g., texts, images, emails, and files – to potential disclosure in the litigation. This is particularly true if, pursuant to the BYOD policy, the employee is instructed to use native communication systems on their personal device. For example, if the employee routinely texts clients or other employees from their mobile device. If the employee has not taken care to preserve relevant information – particularly after an investigation or a lawsuit is initiated – it could lead to allegations of evidence spoliation against the company.

3. Collecting Information From Children

The United States has relatively few restrictions on collecting information from children off-line. Efforts to collect information from children over the internet, however, are regulated by the Children's Online Privacy Protection Act ("COPPA"). Among other things, COPPA requires that a website obtain parental consent prior to collecting information, post a specific form of privacy policy that complies with the statute, safeguard the information that is received from a child, and give parents certain rights, like the ability to review and delete their child's information. COPPA also prohibits companies from *requiring* that children provide personal information in order to participate in activities, such as on-line games or sweepstakes.

283	$2.28 / Child	20+	$4 million
Number of complaints received by the FTC about companies violating COPPA.[14]	Estimate by one organization of the average fine per child imposed by the FTC .[15]	Number of enforcement actions taken by the FTC.[16]	The largest COPPA fine imposed by the FTC.[17]

[14] Number of complaints currently maintained by FTC in Consumer Sentinel database as of November 30, 2017. FTC FOIA Response 2018-00257.

[15] http://www.coppanow.com/averagecoppa/ (last viewed Nov. 2016).

[16] FTC, 2014 Privacy and Data Security Update, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2014/privacydatasecurityupdate_2014.pdf

[17] United States v. InMobi Pte Ltd, Case No. 3:16-cv-03474 (N.D. Cal. June 22, 2016), https://www.ftc.gov/system/files/documents/cases/160622inmobistip.pdf.

The following are the most common complaints about children's websites received by the FTC:[18]

48.45%	The website did not obtain proper parental consent
43.72%	The website collected more personal information than was necessary
41.35%	Parents were not given an opportunity to stop information from being disclosed to third parties
24.77%	The website did not have a clear privacy policy
17.67%	The website misrepresented how information was used

What to think about when reviewing your website:

1. Does your website ask children to provide information?

2. If not, does your website automatically collect information about a child's computer or session?

3. Would your website appeal to children?

4. Has the FTC received complaints about your website? If so, how many and what issues were raised in the complaints?

5. Does your website ask for parents' permission to collect information about children?

6. Does your website verify that the parent is the actual parent of a child?

7. Has the verification mechanism been approved by the FTC?

8. Does your website's privacy policy comply with COPPA?

9. Can you limit liability by joining an FTC approved self-regulatory organization (sometimes called a "safe harbor" program)?

10. Which safe harbor program provides the most benefit to your organization?

4. Companies Perceived By The FTC As Top Violators

The Federal Trade Commission collects complaints about organizations that allegedly violate the data privacy, data security, advertising, and marketing laws.

Each month the FTC creates an internal "Top Violators" report that ranks the fifty organizations with the greatest volume of consumer complaints. The report indicates whether each organization listed was included in the previous month's report, whether its rank has changed, and the number of complaints received by the FTC that month. For organizations that are new to the report, the FTC reviews their complaints and summarizes the issue, or issues, that have been raised by consumers.

[18] Based upon analysis of consumer complaints received by the FTC between January 2008 and August 2013.

78%	91.2%
Percentage of the top 20 companies on the FTC's Top Violators Reports that have had a public FTC investigation concerning their advertising, marketing, data privacy, or data security practices.[19]	Percentage of FTC enforcement actions that target a company found in the FTC's complaint database.[20]
394 – 2,795 Quantity of complaints filed per month against the top 50 companies tracked. [21]	

In order to understand the impact of the Top Violator Report to your organization you should consider asking the following questions:

1. Is your organization identified on the current Top Violators Report? Has your organization ever been identified on a Top Violators Report? If you are not listed on the Top Violator's Report, how close is your organization's complaint volume to those organizations that are on the list?

2. Are competitors in your industry identified on the Top Violators Report? If so, if the FTC initiated an investigation of your competitor what impact (if any) would that have on your organization?

3. Are companies which provide service to your organization on the Top Violators Report? If so, do the complaints filed against those service providers suggest legal compliance issues which may put your organization at risk?

4. Are clients of your organization on the Top Violators Report? If so, if a FTC investigation were to be initiated against your client, could it have a negative impact on your organization?

5. Do you have a system in place to quickly identify any pertinent changes to the Top Violator Report?

5. Data Maps and Data Inventories

Knowing the type of data that you collect, where it is held, with whom it is shared, and how it is transferred is a central component of most data privacy and data security programs. The process of answering these questions is often referred to as a "data map" or a "data inventory." Outside of the United States some attorneys may be more familiar with the term "data register."

---

[19] Based upon a review of the top 20 violators from complaints volume between 1/1/2009 – 12/12/2014, excluding companies not subject to FTC jurisdiction and complaints that do not relate to corporate behavior (e.g., imposter or spoofing).

[20] FTC, Fiscal Year 2016 Performance Report and Annual Performance Plan for Fiscal Years 2017 and 2018, p. 49, https://www.ftc.gov/system/files/documents/reports/fy-2017-18-performance-plan-fy-2016-performance-report/fy18_cbj_apr-app.pdf.

[21] FTC, Top Companies Receiving Complaints in Consumer Sentinel (Aug. 1, 2016 – Aug. 31, 2016) (excludes complaints relating to scams connected to impersonating the government).

Although the questions that a data map tries to solve are relatively straightforward, the process of conducting a data map can be daunting for many organizations. In addition, it is important to remember that data constantly changes. As a result, organizations must consider how often to invest the time to conduct a data map and, once invested, how long the information will be useful.

75%	43%
The percentage of privacy officers ranking data inventory and mapping as their highest priority for risk mitigation.[22]	The percentage of companies that already engage in routine data inventory and mapping.[23]

What you should think about when deciding whether to conduct a data map or a data inventory:

1. Which departments within your organization are most likely to have data?

2. Who within each department would you need to speak with to find out what data exists?

3. Is it more efficient to send the relevant people a questionnaire or to speak with them directly? What is the best way to receive information from each person in the organization that collects data so that the information provided can be organized and sorted with information received from others?

4. What information should you collect about the personal data within your organization? For example, is it enough to know where the data is, and who is responsible for it, or should you collect the reason why your organization has the data, how long it is kept, where it is systematically transferred to, and the type of security applied to the data?

5. Is your data map intended to be an inventory (i.e., a description of data at rest), or is it intended to provide dynamic information (i.e., a description of how data moves within and outside of your organization)?

6. Which stakeholders in your organization may have an interest in the outcome of your data map? For example, are there uses that a privacy officer, an information security officer, or a chief information officer, may have in the outcome of the project?

---

[22] Int'l Ass'n of Privacy Prof'ls & TRUSTe, Inc., How IT and Infosec Value Privacy, 2 (2016), https://info.truste.com/Web-Resource-PrivacyVsSecurity-Report_TY.html?asset=K3N9WHC6-605&aliId=33018157.

[23] Int'l Ass'n of Privacy Prof'ls & TRUSTe, Inc., Preparing for the GDPR: DPOs, PIAs, and Data Mapping, 16 (2016), https://www.truste.com/resources?doc=643.

7. Do you have sufficient internal resources to conduct the data map? If not, do you have access to external resources with experience in conducting such exercises?

8. Is your data map going to inventory data that crosses national boundaries? If so, do you want your map to also account for what (if any) legal compliance strategies are being used to facilitate such transfers?

9. If your data inventory is going to examine the retention schedule (if any) applied to the data, are you going to rely on self-reported retention periods or are you going to verify actual retention periods?

10. Do you intend to use the outcome of your data inventory to demonstrate compliance with any specific legal requirements? For example, if your organization is subject to the European Union General Data Protection Regulation do you intend for your data map to satisfy your obligations to demonstrate that your organization applies data minimization and has a permissible purpose for its data processing?

6. Defining Personal Information

The terms "personal information," "personal data," "personally identifiable information," and "PII" are often left undefined in contracts and treated as if they were terms of art for which there was a single definition. Because different statutes, regulations, and guidance documents define the terms differently, you could either say that they are not terms of art, or that they are terms of art that are highly dependent upon context. The following provides an example of one of the most expansive and one of the most narrow definitions of near identical phrases, and illustrates the degree to which the meaning of such terms can differ depending upon context:

European Union General Data Protection Regulation ("GDPR") definition of "personal data"	Maryland data breach notification statute definition of "personal information"
"any information *relating* to an identified or *identifiable* natural person ('data subject')[24]	"an individual's *first name or first initial and last name* in *combination* with any *one or more of the following data elements*, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: (i) a *Social Security number*; (ii) a *driver's license number*; (iii) a *financial account number* . . .; (iv) an *Individual Taxpayer Identification Number*."[25]

[24] GDPR Article 4(1).

[25] Maryland Commercial Code § 14-3501(d).

Although the above examples are from two different legal regimes (*i.e.,* the European Union and the United States), even within a single legal regime there can be significant discrepancies.

The following provide some practical takeaways when you are drafting, reviewing, editing, or negotiating agreements:

1. If an agreement is intended to involve information relating to data subjects in the European Economic Area it is more likely that the agreement will be interpreted against the backdrop of the GDPR and, therefore, that a statement referencing "personal information" would be interpreted expansively. If the agreement is poorly drafted this can inadvertently put one, or both, parties in breach of the agreement. For example, broad statements that a party will encrypt *all* "personal information" are almost *per se* inaccurate as most parties anticipate that personal information in some forms will be transmitted in a non-encrypted manner. For examples, the parties probably expect communication by email despite the fact that emails contain personal information (e.g., the "to," "from," and "cc" fields contain names) and email is not typically encrypted.

2. If an agreement is intended to involve information only from data subjects in the United States, the term "personal information" is, at best, ambiguous, and a party to the contract, a regulator, or a third party plaintiff could reasonably argue that it is sufficiently broad to include basic identifying information such as a person's name. As a result, if the terms is being used to refer to situations in which particular security measures will be taken (*e.g.,* access controls, encryption, etc.) make sure that it is defined narrowly to include the types of *sensitive* personal information for which such controls would be appropriate.

3. In light of the ambiguities surrounding such terms, it is reasonable to object to agreements that do not define the terms, or that use obtuse definitions that escape practical application to contractual terms (*e.g.,* "personal information" means any information that is treated as personal information under any law, rule, or regulation).

4. The term "personal information," is often too basic to adequately capture the parties' intent with respect to various contractual terms surrounding data privacy or security. As a result, many agreements will use multiple terms that reflect the fact that different protections are needed for different types of data. For example, a contract might contain a broad definition for "personal information," and a specific definition for "sensitive personal information." Heightened data privacy and security protection would typically only apply to the latter definition.

5. Contracts often assume that information does not fall within the scope of "personal information" if names are removed. Indeed, some contracts will explicitly state that personal information does not include information that has been de-identified, aggregated, anonymized, or pseudonymized. These terms, however, can also lead to contracting ambiguity. For example, different industries and different jurisdictions have different standards for how data can be "de-identified" and what methods of de-identification remove a data set from the realm of "personal information."

7. Defining Sensitive Personal Information

Like the terms "personal information," "personally identifiable information," or "PII," the terms "sensitive information," "sensitive personal information," and "special categories of information" are often left undefined in contracts and treated as if they were terms of art for which there was a single definition. Because different statutes, regulations, and guidance documents define the terms differently, you could either say that they are not terms of art, or that they are terms of art that are highly dependent upon context. Either way leaving them within a contract undefined can lead to ambiguity and, ultimately, to disputes. The following provides an example of one of the most expansive and one of the most narrow definitions of near identical phrases, and illustrates the degree to which the meaning of such terms can differ depending upon context:

European Union General Data Protection Regulation ("GDPR") definition of "special" data categories	Federal Trade Commission ("FTC") Definition of "Sensitive" Personal Information
Personal data that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership . . . genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation . . . ."[26]	"The Commission defines as sensitive, at a minimum, data about children, financial and health information, Social Security numbers, and certain geolocation data . . ."[27]

Although the examples are from two different legal regimes (*i.e.,* the European Union and the United States), even within a single legal regime, or a single agency within a legal regime, there can be significant discrepancies.

In terms of practical takeaways consider the following drafting, reviewing, editing, or negotiating an agreement:

1. If an agreement is intended to involve information relating to data subjects in the European Economic Area it is more likely that the agreement will be interpreted against the backdrop of the GDPR and, therefore, that a statement referencing "sensitive information" would be interpreted to include the categories described within the GDPR as "special." If the agreement is poorly drafted this can inadvertently put one, or both, parties in breach of the agreement. For example, broad statements that one party is, or is not, receiving or transmitting, "sensitive information" can easily be inaccurate.

2. If an agreement is intended to involve information only from data subjects in the United States, the term "sensitive information" will most likely be interpreted as including at a minimum bank account numbers, social security numbers, and health information, but there may be ambiguity about whether other data fields such as biometrics, insurance

[26] GDPR, Art. 9(1).

[27] FTC, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers at 47 n.214 (Mar. 2012).

information, or geo-location information were intended to fall under the scope of the term.

3. In light of the ambiguities surrounding such terms, it is reasonable to object to agreements that do not define the terms, or that use obtuse definitions that escape practical application to contractual terms (*e.g.,* "sensitive personal information" means any information that is treated as sensitive under any law, rule, or regulation).

4. Even when the terms are defined within an agreement, it is often difficult (or impossible) to comply with the substantive requirements that the agreement imposes on the collection, use, protection, or disclosure of sensitive information unless the party that transmits such information identifies the information – before or during transmission – as being sensitive.

5. Define the term "sensitive information" by reference to an existing law or statute can also raise unique challenges. For example, if a contract that is intended to apply to data that originates from multiple jurisdiction incorporates by reference the EU's definition of "special categories" of information into the definition of sensitive information it could raise ambiguity as to whether the parties intended all data fields that fall under the definition of special categories within the EU, or all data fields that fall under the definition of special categories within the EU *and* that relate to data subjects in the EU.

8. Email Marketing

Email is ubiquitous in modern life with billions of emails – wanted and unwanted – sent each day. Since its enactment in 2003, the Controlling the Assault of Non-Solicited Pornography and Marketing ("CAN-SPAM") Act has attempted to curb the number of unwanted emails and impose some rules on a largely unregulated frontier. When followed, the CAN-SPAM Act's restrictions give email recipients some control over their inboxes and also maintain fairness in how emails present themselves. Failure to follow the CAN-SPAM Act can lead to penalties of up to $16,000 per violation.

As a practical matter, many organizations use vendors for their email marketing and other email services, and those vendors often assist the organizations in complying with the requirements of the CAN-SPAM Act. Nonetheless, the party whose content is promoted via email must supervise the conduct of its vendors and employees in abiding by CAN-SPAM, or else risk possible sanctions.

$44.00	246 Billion	244.5 Million	14,930
Average return on each dollar of email marketing investment.[28]	Projected number of daily business emails in 2020.[29]	Estimated number of email users in the US at the end of 2017.[30]	Number of complaints received by the FTC in a year concerning unsolicited email.[31]

[28] Allen Finn, 35 Face-Melting Email Marketing Stats for 2017, Wordstream Blog, (December 21, 2017), https://www.wordstream.com/blog/ws/2017/06/29/email-marketing-statistics.

[29] *Id*.

The basic questions to ask regarding CAN-SPAM compliance are:

1. Does your email message include: (a) complete and accurate transmission and header information; (b) a "From" line that identifies your business as the sender; (c) a "Subject" line that accurately describes your message; and (d) an effective "opt-out" mechanism?

2. Does your email either contain an email address, physical address, or other mechanism that the recipient may use for opting-out of future marketing emails?

3. Is your opt-out mechanism effective for at least 30 days after your email is sent?

4. Do you honor all requests to opt-out within 10 days?

5. Does your mailing list include any recipient that has asked not to receive email from your business (opted-out)?

6. Have you tested the effectiveness of your opt-out mechanism?

7. Have you reviewed your vendor contracts to determine each party's responsibilities with regard to CAN-SPAM compliance?

8. Are addresses of people that have opted-out transferred outside of your organization?

9. Does your organization use open relays or open proxies to send marketing email?

10. Have you validated your CAN-SPAM compliance program annually?

9. Email Marketing In Canada (CASL)

On July 1, 2014, the central provisions of the Canadian Anti-Spam Law ("CASL") came into force. [32] These provisions generally prohibit the sending of a Commercial Electronic Message ("CEM") without a recipient's express consent, and unless the CEM contains certain sender identification information and an effective unsubscribe mechanism. CASL provides a number of nuanced exceptions to the express consent requirements of the law. The primary enforcement agency of CASL is the Canadian Radio-television and Telecommunications Commission (CRTC). The CRTC has several compliance tools to enforce CASL, including the issuance of Administrative Monetary Penalties (AMPs) against individuals and organizations that have violated CASL's provisions.

---

30 *Id*.

31 FTC, Consumer Sentinel Network Data Book for January – December 2016, (March 2017), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2016/csn_cy-2016_data_book.pdf.

32 An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act, S.C. 2010, c. 23, Assented to 2010-12-15 ("CASL"), http://lois-laws.justice.gc.ca/eng/AnnualStatutes/2010_23/FullText.html.

Due to CASL's broad applicability, exacting standards, and potentially severe financial penalties, companies that do business in Canada are advised to implement appropriate compliance measures to address the provisions of CASL. Companies sending emails to recipients in Canada must tailor their compliance programs to CASL's complex set of consent exceptions and patchwork of guidelines, interpretations, and enforcement actions. To date, the CRTC has brought only a handful of major CASL enforcement actions, but many investigations are ongoing. Further clarification with regard to the most heavily utilized exceptions is expected. In October 2016, the CRTC assessed the scope of the "conspicuously published" implied consent exception in its first Compliance and Enforcement Decision (CRTC 2016-428).

On July 1, 2017, a private right of action was scheduled to come into force, which would have allowed private lawsuits, including class actions, to be filed against organizations and individuals for violations of CASL. However, on June 7, 2017 Innovation, Science and Economic Development Canada (formerly known as Industry Canada) announced that on June 2, 2017, the Government of Canada, through an Order in Council, repealed the July 1, 2017 implementation of the private right of action under CASL.[33] The Government of Canada has not given any indication whether the repeal of the private right of action will be permanent or whether the Government of Canada may try to re-introduce a private right of action sometime in the future.

$10 million	$1.1 million
The maximum AMP that the CRTC can assess against a company for a violation of CASL.[34]	The largest AMP that has been issued since CASL came into force in July 1, 2014.[35]
950,000+	5,000 – 6,000
CASL related complaints filed with the CRTC between July 1, 2014 and May 16, 2017.[36]	The average number of new submissions that the Canadian Spam Reporting Center receives every week.[37]

Consent Exceptions:

1. CASL does not apply to electronic messages sent:

    a. Internally within an organization.

    b. Between organizations in a relationship, where the message concerns the recipient.

[33] Government of Canada, Government of Canada suspends lawsuit provision in anti-spam legislation, (June 7, 2017), https://www.canada.ca/en/innovation-science-economic-development/news/2017/06/government_of_canadasuspendslawsuitprovisioninanti-spamlegislati.html.

[34] CASL, Section 20(4).

[35] Government of Canada, CRTC Notice of Violation: 3510395 Canada Inc. (Compu.Finder), (March 5, 2015), http://www.crtc.gc.ca/eng/archive/2015/vt150305.htm. However, this AMP was later reduced to $200,000. Canadian Radio-television and Telecommunications Commission, Compliance and Enforcement Decision CRTC 2017-368, (October 19, 2017), http://www.crtc.gc.ca/eng/archive/2017/2017-368.htm.

[36] B:Inform, Canada's Anti-Spam Legislation (CASL): A Statistical Analysis From the Canadian Radio Television and Telecommunications Commission (CRTC), (May 16, 2017), http://www.bakerinform.com/home/2017/5/16/canadas-anti-spam-legislation-casl-a-statistical-analysis-from-the-canadian-radio-television-and-telecommunications-commission-crtc.

[37] CASL, Section 91.

c. In response to an inquiry from the recipient.

d. To satisfy a legal right or obligation.

e. From Canada and accessed in another "listed" country, and the message complies with the "listed" country's spam laws.

f. By a sender who has a "family" or "personal" relationship with the recipient.

g. By or on behalf of a charity soliciting donations.

h. By or on behalf of a political party soliciting donations.

2. CASL applies, but consent is not required where a CEM only:

a. Provides a quote or estimate.

b. Facilitates, completes, or confirms an existing transaction.

c. Provides a warranty, a product recall, or safety information.

d. Provides factual information about products or services.

e. Delivers products, updates, or upgrades that the recipient is entitled to receive.

3. CASL applies, but consent from the recipient is implied where:

a. The recipient and sender have an "existing business relationship."

b. The recipient and the sender have an "existing non-business relationship."

c. The recipient has conspicuously published or provided his or her email address.

Questions to consider when evaluating CASL:

1. Have you performed an assessment of your organization's electronic communications to determine if they qualify as CEMs?

2. Do any consent exceptions apply to your organization or your organization's CEMs, or do you have a special relationship with the recipient such that consent is implied?

3. If no consent exception applies, have you implemented a procedure to capture "express consent," including providing: (i) the purpose of requesting consent; (ii) the name of the entity requesting consent; (iii) a mailing address plus phone number, email, or web address; (iv) a statement that consent can be withdrawn; and (v) an affirmative opt-in mechanism?

4. Do your CEMs include the required sender indemnification information and a functioning unsubscribe mechanism?

5. Do you honor all requests to unsubscribe within 10 days?

6. Does your mailing list include any recipient that has either unsubscribed from your CEMs or no longer qualifies for a consent exception?

7. Do you scrub your mailing list against your organization's "do not e-mail list"?

8. Have you implemented procedures to test the effectiveness of your unsubscribe mechanism?

9. Have you reviewed your vendor contracts to determine each party's responsibilities with regard to CASL compliance?

10. Does your CASL compliance program include senior management involvement, a written policy, risk assessments, record keeping, staff training, and a complaint-handling process?

10. Employee Monitoring

Federal laws prohibit the interception of another's electronic communications, but these same laws have multiple exceptions that generally allow employers to monitor employees' email and internet use on employer-owned equipment or networks. As a result, under federal law, if a private-sector employee uses an organization's telephone or computer system, their employer is generally permitted to monitor their communications. That said, once the personal nature of a communication is determined an employer's ability to continue monitoring the communication may be curtailed. For example, under the National Labor Relations Act, employers cannot electronically spy on certain types of concerted activity by employees about the terms and conditions of employment.

Although monitoring is broadly permitted under federal law, some states require that employers notify employees that they may be monitored. Even in states that do not require notice, employers often choose to provide notice since employees who think that they are being monitored are less likely to misuse corporate systems. It is good practice for an employer to have employees sign a consent or acknowledgment that monitoring may occur and to inform them that personal calls may not be made from particular telephones.

Employers may also monitor what an employee posts to social media. Some states prohibit, however, employers from requesting that an employee provide his or her username and password to a social-media account in order for the employer to see content that was not published publicly. This would include, for example, posts that were made available only to an employee's friends, or personal network. In addition, some states prohibit employers from requiring that their employees accept a friend request that would permit the employer to view friends-only social media posts. Finally, some states prohibit monitoring of telephone calls on an employer's telephone network without the consent of one or both parties to the communication.

~80%	2	15
Percent of employers who actively monitor their employees electronically.[38]	States that require private companies to provide notice to employees of electronic monitoring.[39]	States that introduced or considered legislation in 2016 prohibiting employers from requesting passwords to social media accounts.[40]

What to consider when crafting an employee monitoring policy:

1. Does your organization publish an acceptable use policy?

2. If so, does the acceptable use policy explain what employees may and may not do over the Internet while at work?

3. Does the acceptable use policy explain the disciplinary consequences of violating the policy?

4. Do you have the ability to block or otherwise restrict access to Internet sites that are barred under the acceptable use policy?

5. Does your employee handbook make employees aware of monitoring?

6. Does the state in which the employee works require single or dual consent for monitoring telephone conversations, and have your employees consented?

7. If your organization monitors phone calls, do you have a policy to cease monitoring when a call is clearly personal in nature, and do you follow it?

8. Have you considered whether an employee might be able to argue that they have an expectation of privacy to their work emails or to their work phone calls?

9. Are you monitoring emails to or from password-protected personal accounts?

10. Are your employees using their own computer equipment to send emails or view the Internet?

11. Employer Privacy Policies

In 2005 Michigan became the first state to pass a statute requiring employers to create an internal privacy policy that governs their ability to disclose some forms of highly sensitive information about their employees. Michigan's Social Security Number Privacy Act expressly

[38] Romy Ribitzky, "Active Monitoring of Employees Rises to 78%," ABC News (Apr. 18, 2017) *available at* http://abcnews.go.com/Business/story?id=88319&page=1.

[39] National Conference of State Legislatures, State Laws Related to Internet Privacy, (last checked Dec. 31, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx; these states are: Connecticut (Conn. Gen. Stat. § 31-48d) and Delaware (Del. Code § 19-7-705).

[40] National Conference of State Legislatures, Access to Social Media Usernames and Passwords, (last checked Dec. 31, 2017), http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx.

requires employers to create policies concerning the confidentiality of employees' social security numbers ("SSN") and to disseminate those policies to employees. New York adopted a similar statute. Several other states – Connecticut, Massachusetts, and Texas – have statutes mandating the establishment of privacy policies that could also apply in the employer-employee context.

Companies should check whether they have a written policy concerning the use and disclosure of protected employee personal information. If they do not, they should confirm that none of the states in which they operate currently require such a policy or are planning to do so through new legislation.

5	$500	$275,000
The number of states that have enacted statutes that may require employers to create employee privacy policies.[41]	The fine that can be assessed under New York's statute to employers who unlawfully disseminate an employee's SSN.[42]	The damages awarded to a group of Michigan employees who sued their union after it failed to safeguard their SSN.[43]

What to think about when drafting or reviewing an employee privacy policy:

1. Does the privacy policy capture the main ways in which your organization collects personal information from its employees?

2. Does the privacy policy discuss the confidentiality of employee SSN and other personal information?

3. Does the privacy policy explain how employee SSN and other personal information are protected?

4. Does the privacy policy limit who has access to information or documents that contain employee SSN and other personal information?

5. Does the privacy policy describe how to properly dispose of documents that contain employee SSN and other personal information?

6. Does the privacy policy describe the disciplinary measures that may be taken for violations?

7. How will the policy be distributed to each employee?

8. Can the average employee understand the policy?

9. Does the privacy policy use terms that might be misunderstood or misinterpreted by a regulator or a plaintiff's attorney?

---

41 These states are: Connecticut (Conn. Gen. Stat. § 42-471), Massachusetts (201 Mass. Code Regs. 17.03), Michigan (Mich. Comp. Laws § 445.84), New York (N.Y. Lab. Law § 203-d), and Texas (Tex. Bus. & Com. Code Ann. § 501.052).

42 N.Y. Lab. Law § 203-d(3).

43 John F. Buckley & Ronald M. Green, State by State Guide to Human Resources Law § 1.36 (2015).

10. Does the privacy policy comply with the laws in each jurisdiction in which your organization is subject?

12. Facial Recognition Technology

Facial recognition technology uses algorithms that map facial features – such as the distance between a person's eyes, or the width of a person's nose – and compares those features to a database of the algorithmic output of known individuals. Organizations may use the technology for security (*e.g.,* cameras that "ID" employees or criminals), marketing to consumers (*e.g.,* cameras that "ID" particular customers), or sorting through large quantities of existing digital media (e.g., photograph sorting).

There is currently no federal statute that expressly regulates private-sector use of facial recognition technology. Nonetheless, the FTC, which has authority to prevent unfair and deceptive practices, is interested in the privacy implications of facial recognition technology. The agency has not only issued a set of best practices concerning its use; it has investigated organizations that it believes violated those recommendations.

At least two states have also enacted statutes that govern the technology. Those statutes require that a company (1) notify state residents that the technology is in use, and (2) obtain the consent of those subject to the technology.

1	30%	80	10
Number of years that an organization is allowed to keep biometric data under some state laws after the purpose for which it was collected has expired.[44]	Percentage increase in accuracy of facial recognition algorithms over a three year period.[45]	Number of public comments received following FTC workshop on facial recognition technology.[46]	Number of state data breach notification laws that may apply to facial recognition telemetry if lost or stolen.[47]
$5,000 - $25,000			
The range of possible fines and damages that could be assessed under state law for each violation of a facial recognition statute.[48]			

Practices recommended by the FTC when deploying facial recognition technology:

1. Security. Companies should maintain reasonable data security for consumers' images and facial geometry.

---

44 Tex. Bus. & Com. Code § 503.001(b)(3).

45 National Institute of Standards and Technology, NIST: Performance of Facial Recognition Software Continues to Improve, (June 3, 2014), http://www.nist.gov/itl/iad/face-060314.cfm.

46 *See*, Public Comments, FTC Matter No. P115406.

47 Bryan Cave LLP, Data Breach Notification Survey (2017).

48 *See*, 740 ILCS 14/20 (1)-(4); Tex. Bus. & Com. Code § 503.001(d).

2. Retention and Disposal. Companies should establish and maintain appropriate retention and disposal practices for consumers' images and facial geometry.

3. Notice. Companies should provide "clear notice" when facial recognition technology is being utilized.

4. Opt-in Consent For Materially Different Use. Companies should obtain consumers' affirmative express consent if they use an image in a "materially different manner" than was represented when the facial geometry was collected.

5. Opt-in Consent For Sharing. Companies should obtain consumers' affirmative express consent if they identify anonymous images of a consumer to someone who could not otherwise identify the consumer.

13. Fingerprint Identification Technology

Fingerprint identification technology uses fingerprints to uniquely identify individuals. The technology has been used by law enforcement agencies for decades, and dozens of statutes regulate when government agencies may collect fingerprints, how they are permitted to use them, and with whom they can be shared.

Advances in fingerprint recognition software have lead many private entities to begin using the technology to authenticate consumers. For example, many mobile devices have integrated fingerprint recognition technology to replace, or supplement, passwords or passcodes. Some employers are also using fingerprint recognition technology to increase the accuracy and efficiency of employee timekeeping systems.

There is currently no federal statute that expressly regulates private-sector use of fingerprint recognition software. Nonetheless, the FTC, which has authority to prevent unfair and deceptive practices, may proceed against companies that misrepresent how they use, secure, or disclose captured fingerprints or fingerprint geometry.

Numerous states have enacted statutes concerning the collection of fingerprints by government agencies, by accreditation boards, or in certain regulated industries (e.g., childcare and education). At least two states have also enacted statutes that govern the private sector's use of the technology outside of specific fields and applications. Those statutes generally require that if an organization "captures" a fingerprint's geometry it must provide the consumer with notice and obtain their consent. In addition, if an organization stores fingerprint geometry then it must limit its disclosure to third parties, enact measures to secure the fingerprint from unauthorized access, and limit its retention after it is no longer needed. A number of additional states require that if a company collects fingerprints it take steps to prevent the fingerprint from being acquired when in the process of being destroyed.

120 million Number of fingerprints held by one government agency.[49]	1 in 50,000 Probability of a false match claimed by one mobile device in conjunction with fingerprint recognition software.[50]

[49] FBI, Next Generation Identification (NGI) Monthly Fact Sheet (Oct. 2017) *available at* https://www.fbi.gov/file-repository/ngi-monthly-fact-sheet/view (viewed Dec. 2017).

[50] https://support.apple.com/en-us/HT204587 (last viewed Dec. 2015).

$5,000 - $25,000
The range of possible fines and damages that could be assessed under state law for *each* violation of a fingerprint identification statute.[51]
$1.5 Million
Largest class action settlement / judgment against a company for allegedly collecting fingerprints without providing proper notice and obtaining appropriate consent.[52]

Consider the following when using fingerprint identification technology:

1. Security. Assess the risk that fingerprints and/or fingerprint geometry may be compromised and consider what steps can be reasonably taken to attempt to keep the information secure.

2. Retention and Disposal. Review your retention and disposal practices to see if they specify how long such information should be kept, and how it should be disposed.

3. Notice. Consider providing clear notice to consumers or employees before capturing their fingerprints.

4. Consent. Consider obtaining opt-in consent before capturing or using fingerprints.

5. Sharing. Consider obtaining opt-in consent before sharing fingerprints or fingerprint geometry with any third parties.

14. FTC Tracking Of Privacy Complaints

The FTC collects complaints about companies that allegedly violate the data privacy, data security, advertising, and marketing laws. The result is a massive database of consumer complaints known as "Consumer Sentinel" that is used by the FTC and other consumer protection regulators to identify and investigate enforcement targets.

Regulators can use Consumer Sentinel to search for complaints on any company. They can also request that the database alert them to new complaints about an organization, or connect them with other law enforcement agencies that might have an interest in investigating the same organization. In addition to these functionalities, the FTC also creates a "Top Violator" report and a "Surge" report that track those organizations that the FTC believes may have a suspicious pattern of consumer complaints.[53] The end result is that the vast majority of FTC enforcement actions target companies identified within the FTC's database.

---

[51] *See*, 740 ILCS 14/20 (1)-(4); Tex. Bus. & Com. Code § 503.001(d).

[52] Stipulation of Class Action Settlement, *Sekura v. L.A. Tan Enterprises, Inc.*, Case No. 15-CH-16694 (Cir. Ct. Cook County Ill. June 20, 2016).

[53] FTC Office of Inspector General, Evaluation of the Federal Trade Commission's Bureau of Consumer Protection Resources, OIG Evaluation Report No. 14-003, p. 8 (Oct. 2, 2014), https://www.ftc.gov/system/files/documents/reports/evaluation-ftc-bureau-consumer-protection-resources/2015evaluationftcbcpreport.pdf.

33 million	91.2%	33	195
Number of consumer complaints maintained in Consumer Sentinel.[54]	Percentage of FTC enforcement actions that target a company found in Consumer Sentinel.[55]	Number of government agencies that contribute complaints to the FTC's Consumer Sentinel.[56]	Number of distinct "law violations" tracked by the FTC.[57]
3.1 million Number of non-DNC complaints added to Consumer Sentinel in 2016.[58]			

What to think about when considering the records that the FTC maintains about your organization:

1. Has your organization been identified as a potential enforcement target on the FTC's Top Violator or Surge reports?

2. Does your organization routinely track the quantity of complaints that the FTC maintains about it?

3. Is the volume of complaints filed about your organization above, or below, those of others in your industry?

4. If the FTC, or another regulator, searched for the complaints about your organization what potential compliance issues would they identify?

5. If your organization were investigated by the FTC, is the volume of complaints filed about it easily explained?

6. Is the volume of your complaints trending up, or trending down?

7. Have plaintiffs' law firms investigated your complaint volume?

15. GeoLocation Tracking

Smartphones, websites, and other connected devices (*e.g.,* "wearables") increasingly request that consumers provide their geo-location information. Geolocation information can refer to general information about a consumer's location, such as his or her city, state, or zip

[54] FTC, Consumer Sentinel Network Data Book for January – December 2016, p. 3 (March 2017) (13 million complaints from Consumer Sentinel and 20 million from do-not-call database).

[55] FTC, Fiscal Year 2016 Performance Report and Annual Performance Plan for Fiscal Years 2017 and 2018, p. 59 https://www.ftc.gov/system/files/documents/reports/fy-2017-18-performance-plan-fy-2016-performance-report/fy18_cbj_apr-app.pdf.

[56] FTC, Consumer Sentinel Network Data Contributors, https://www.ftc.gov/enforcement/consumer-sentinel-network/data-contributors (last viewed Nov. 11, 2016).

[57] Based upon Law Violation Codes used within the FTC's Consumer Sentinel database.

[58] FTC, FTC Releases Annual Summary of Consumer Complaints (March 3, 2017), https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints.

code, or it can refer to precise information that pinpoints the consumer's location to within a few feet, such as his or her GPS coordinates.

Organizations request geo-location information for a variety of reasons. For example, many apps – such as transportation or delivery services – require geo-location in order to provide services that are requested by the consumer. Other apps – such as mapping programs, coupon programs, or weather programs – require geo-location information in order to provide consumers with useful information. Because such information has become intertwined, in many cases, with products and services, some organizations require the user to "Accept" or '"Agree"' to the collection of geo-location information as a condition to using a device, application, or website. In addition, when a smartphone app requests the geolocation of a user from the operating system of a smartphone device, the major smartphone devices automatically prompt a user to provide opt-in consent before the devices shares the location information.

Although there is currently no federal statute that expressly regulates the use, collection, or sharing of geolocation data, the FTC has taken the position that precise geolocation information is a form of "sensitive" personal information and has suggested that a failure to reasonably secure such information, or a failure to adequately disclose the collection or sharing of such information, may violate the Federal Trade Commission Act's general prohibition against unfair or deceptive practices.[59] In addition, Congress and state legislatures have considered several proposals that would expressly regulate geolocation information.

Every 10 Minutes	91%
The frequency with which some apps, like weather apps, request geolocation information from a mobile device.[60]	Percentage of adults who "agree" or "strongly agree" that consumers have lost control over how often personal information is collected and used by companies.[61]
73%	19
Percentage of times that an app will share geolocation information with an advertising network when asked.[62]	Number of FTC enforcement actions regarding geolocation practices.[63]
10-20%	
How much more marketers pay for online ads that include geolocation information.[64]	

[59] *See*, Jessica Rich, Prepared Statement of the Federal Trade Commission on S. 2171 The Location Privacy Protection Act of 2014 Before The United States Senate Committee on the Judiciary Subcommittee for Privacy, Technology, and the Law, (June 4, 2014), https://www.ftc.gov/system/files/documents/public_statements/313671/140604locationprivacyact.pdf.

[60] Almuhimedi et. al., Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging, http://www.normsadeh.com/file_download/179.

[61] Mary Madden, Privacy and Cybersecurity: Key findings from Pew Research, Pew Research Center, (January 16, 2015), http://www.pewresearch.org/key-data-points/privacy/.

[62] Elizabeth Dwoskin, Where were you 3 Minutes Ago? Your Apps Know, Wall Street Journal (May 23, 2015), http://blogs.wsj.com/digits/2015/03/23/where-were-you-3-minutes-ago-your-apps-know/.

[63] IAPP Resource Center, Geolocation (last checked Jan. 2, 2018), https://iapp.org/resources/topics/geolocation/?mkt_tok=eyJpIjoiT0RVNU5ERmpNakl6TWpVMCIsInQiOiJWNStcL2JsVmRweE9WbW13Z1NUVFBBeHBwN.

[64] Elizabeth Dwoskin, Where were you 3 Minutes Ago? Your Apps Know, Wall Street Journal (May 23, 2015), http://blogs.wsj.com/digits/2015/03/23/where-were-you-3-minutes-ago-your-apps-know/.

What to consider if your organization collects geolocation information:

1. What is the purpose for which geolocation information is being collected?

2. Are you collecting the least granular (i.e., most general) location information possible in order to effectively provide a product or a service to the consumer?

3. How often do you need to collect geolocation information?

4. Is the user aware that geolocation information is being collected?

5. Does the user have the ability to disable the collection of geo-location information?

6. Does the user have the ability to control how long that information is maintained, how it is used, when it is shared, and whether it is associated with their name?

7. Will the geolocation information be shared with third parties such as advertisers? If yes, how much and how often will you share the information?

8. Is the geolocation information encrypted in transmission from the consumer and/or at rest within your organization?

9. If you receive a request from a data subject to provide them with all of the geolocation information that you maintain about them, how will you respond?

10. If you receive a request from law enforcement to provide you with all the geolocation information that you maintain about a particular data subject, how will you respond?

16. Mobile App Privacy Policies

Many of the most popular mobile apps collect personally identifiable information. Although most app developers are not required to display a privacy policy under federal law, they are contractually required to do so pursuant to the terms and conditions of the websites that market most major mobile device applications (*e.g.,* the Apple Store, or Google Play). In addition, the California Attorney General has taken the position that applications that collect personal information are required to post a privacy policy pursuant to the CalOPPA discussed in the previous section.

$2,500	11%	90%	> 60%
The possible penalty under California law for each app downloaded without a privacy policy.[65]	The percentage of banking related apps reported to contain harmful code.[66]	The percentage of mobile health and finance apps with at least two critical security vulnerabilities.[67]	The percentage of popular dating apps vulnerable to hacker exfiltration of PII.[68]

[65] California Online Privacy Protection Act (CalOPPA), Consumer Fed'n of Cal. Educ. Found. (July 29, 2015), https://consumercal.org/about-cfc/cfc-education-foundation/california-online-privacy-protection-act-caloppa-3/.

Consider the following privacy issues when developing a mobile app:

1. **Does the app have a privacy policy?** Privacy policies are a best practice if the app will be used in connection with personally identifiable information. As discussed above, there is also an argument that they may be required if they solicit information from California residents.

2. **Is the app directed to users younger than 13?** Under the Children's Online Privacy Protection Act ("COPPA"), if the app collects information from children it must include a privacy policy as well as comply with additional requirements imposed under that Act. See the section titled Collecting Information From Children for more information.

3. **How is personally identifiable information stored by the app?** Apps can store data in multiple places, including the device, backups of the device, and the app provider's servers. A best practice is for a mobile app's privacy policy to state accurately where personally identifiable information is stored.

4. **Does the app communicate personally identifiable information to others?** A useful privacy policy accurately states whether data that the user provides is relayed to anyone else.

5. **Does the mobile app provider securely communicate any personally identifiable information?** A 2016 study concluded that 35 percent of apps utilize non-encrypted communications. Consider stating within the app's privacy policy whether the app transmits personally identifiable information, and, if so, whether the information is encrypted in transit.

17. Online Behavioral Advertising

Behavioral advertising refers to the use of information to predict the types of products or services of greatest interest to a particular consumer. Online behavioral advertising takes two forms. "First party" behavioral advertising refers to situations in which a company's website uses information that it obtains when interacting with a visitor. "Third party" behavioral advertising refers to situations in which a company permits others to place tracking technology – such as cookies – on the computers of people who visit the company's website, so that those individuals can be monitored across behavioral advertising networks.

Two self-regulatory associations – the Network Advertising Initiative ("NAI") and the Digital Advertising Alliance ("DAA") – have created standards for companies engaged in third party online behavioral advertising. They have also promoted mechanisms for consumers to opt-out of being tracked. In addition to their self-regulatory two states enacted statutes that

---

[66] Pierluigi Paganini, 11 Percent of Mobile Banking Apps Include Harmful Code, Sec. Affairs (Feb. 7, 2015), http://securityaffairs.co/wordpress/33212/malware/mobile-banking-apps-suspect.html.

[67] Arxan Tech., Inc., 5th Annual State of Application Security Report: Perception vs. Reality, 2 (2016), https://www.arxan.com/wp-content/uploads/2016/07/Consolidated-Report-SINGLE-PAGE.pdf.

[68] IBM Sec. Intelligence, IBM Security Analysis: Dating Apps Vulnerabilities & Risks to Enterprises, 2 (2015), http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SCTE_WG_WM_USEN&htmlfid=WGL03072USEN&attachment=WGL03072USEN.PDF.

require companies to notify consumers if they permit third party behavioral advertising in certain situations.

2	107	289	880
Number of state statutes that may require companies to disclose the use of third party behavioral advertising.[69]	Number of companies that are members of NAI.[70]	Number of companies that are members of DAA.[71]	Number of references on FTC's website to "behavioral advertising"[72]
6 – 31			
The number of tracking cookies placed by the top 5 retailers on their websites.[73]			

What to think about when evaluating your organization's online behavioral advertising practices:

1. Does your privacy policy comply with state law requirements concerning the disclosure of first party online behavioral advertising?

2. Does your privacy policy comply with state law requirements concerning the disclosure of third party online behavioral advertising?

3. Does your organization state or imply that it only permits behavioral advertisers to use its website if those advertisers utilize the opt-out mechanisms of NAI and/or DAA?

4. If so, do all of the behavioral advertisers that you permit to use your website permit opt-out via the NAI and/or DAA mechanisms?

5. Who within your organization has the authority to permit third parties to place cookies on your website?

6. Who within your organization maintains a comprehensive list of all cookies placed on your website?

7. Has the legal department reviewed the contracts with each behavioral advertiser with whom your organization has a relationship to verify that their privacy practices comply with law and with the standards of your organization?

8. Have you audited the cookies that are placed, or tracked, on your website?

9. If so, how often do you plan on auditing them on a going forward basis?

---

69 Cal Bus. & Prof. Code §§ 22575(b)(5)-(7); Del. Code 1204C.

70 Companies listed on http://www.networkadvertising.org/participating-networks as of January 2018.

71 Companies listed on http://www.aboutads.info/participating as of January 2018.

72 Based upon Google search restricted to FTC.gov conducted in January 2018.

73 Top 5 eCommerce retailers as identified by the National Retail Federation in 2017. Quantity of cookies identified by Ghostery on retailer home page on Jan. 2, 2018.

10. Have you verified the accuracy of the description of behavioral advertising contained on your website?

18. Organizing Data Privacy Within A Company

Although organizations have dealt with privacy issues for years, only in the past decade have they begun to view the complexities of privacy as requiring formal organizational structure, dedicated employees, and/or dedicated resources. While in some organizations "privacy" falls within the ambit of the legal department; other organizations have created offices that are focused solely on privacy issues and that report to a Chief Privacy Officer ("CPO"). There is little commonality in how these offices are staffed, funded, or organized. For example, while some CPOs report directly to senior management, others report through a General Counsel or a Chief Compliance Officer.

66% Percentage of CPOs that say privacy is their only responsibility.[74]	9 The average number of years of experience CPOs have in privacy related roles.[75]
72% Percentage of Privacy Offices that are housed within the Legal Department.[76]	27% Percentage of CPOs that report directly to the General Counsel.[77]
3.3 – 25 The range of full time employees retained by Fortune 1000 companies to deal specifically with privacy-related issues.[78]	

If you are creating a privacy office, or reviewing the scope of an existing office, consider the degree to which the office should be responsible for the following functions:

1. Drafting, reviewing, or revising privacy related policies and privacy related procedures *(e.g.,* BYOD policy, website privacy policies, employee privacy codes of conduct).

2. Following privacy related legal developments and trends.

3. Training employees (*e.g*., providing core privacy training to the majority of employees, as well as specialized privacy training for employees that have contact with personal information).

---

74 IAPP, Benchmarking Privacy Management and Investments of the Fortune 1000, p. 13 (2014), https://iapp.org/media/pdf/resource_center/2014_Benchmarking_Report.pdf.

75 *Id.* at 11.

76 IAPP, IAPP-EY Annual Privacy Governance Report 2017, p.xii (2017), https://iapp.org/resources/article/iapp-ey-annual-governance-report-2017/.

77 *Id*. at 66.

78 IAPP, Benchmarking Privacy Management and Investments of the Fortune 1000, p. 17, 20 (2014), https://iapp.org/media/pdf/resource_center/2014_Benchmarking_Report.pdf. Survey found that on average companies in the Fortune 1000 with an "early stage" privacy program had 3.3 FTEs whereas companies with a "mature stage" privacy program had 25 FTEs.

4. Responding to privacy related complaints or questions.

5. Assisting the organization in negotiating contracts in which the organization is providing privacy related representations, warranties, guarantees, or indemnification (*i.e.,* client-facing agreements).

6. Participating in the organization's incident response team.

7. Conducting privacy risk assessments or privacy impact assessments.

8. Assisting the organization when negotiating privacy provisions in contracts in which the organization is providing data to third parties (*e.g.,* reviewing privacy practices of vendors and negotiating appropriate contractual guarantees).

9. Conducting a data inventory or a data map.

10. Monitoring or auditing the organization's privacy-related practices.

11. Reporting to senior management any significant privacy related risks or concerns.

12. Managing the cross-border transfer of information between jurisdictions with different privacy standards.

13. Working with developers, designers, or marketers to design privacy protections into new products, services, or promotions.

19. Passing Data Between Retailers To Facilitate Transactions

Online retailers often learn information about a consumer that may be used by them to help identify other products, services, or companies that may be of interest to the consumer. For example, if a person purchases an airplane ticket to Washington DC, the person may want information about hotels, popular restaurants, or amenities at the airport.

Although online retailers often strive to provide recommendations quickly, and to make a consumer's transition to a third party retailer seamless, the Restore Online Shoppers' Confidence Act ("ROSCA") generally prohibits one online merchant from transferring payment information (*e.g.,* a credit card number) to a second online merchant. ROSCA also prohibits the second online merchant from charging a consumer's payment card or financial account, unless the second online merchant has clearly and conspicuously disclosed to the consumer all material terms of the transaction and received the consumer's express consent to the charge.

$340.3 Billion Amount spent per year by consumers online.[79]	6 Number of Federal Trade Commission enforcement actions initiated under ROSCA.[80]	$1.38 million The amount that the FTC settled with lingerie seller AdoreMe, Inc. over ROSCA enforcement action.[81]	100% Percentage of ROSCA cases that have been filed by the FTC in federal district court, as opposed to an administrative adjudication.[82]

Questions to consider when evaluating the data privacy issues involved in passing information between online retailers:

1. Are consumers being presented with third party products or services when they visit a retailer's website?

2. Are consumers being presented with third party products or services immediately after they visit a retailer's website?

3. Are such items affirmatively selected by the consumer, or added automatically to the consumer's shopping cart?

4. If the consumer decides to purchase such third party products or services, would he or she likely think that your organization, or the third party, is processing the transaction?

5. Is the total cost of each third party product clearly and conspicuously disclosed?

6. If the consumer indicates that he or she wishes to buy a third party product or service, can the consumer easily change that decision?

7. Is contact information being transferred from one retailer to another?

8. Is payment information being transferred from one retailer to another?

9. Is the third party offering a free trial offer? If so will the consumer be charged any money to participate and does the consumer need to take an affirmative act to prevent a charge after the trial period?

10. Is the third party offering a continuity program or membership? If so are the terms of the program clearly and conspicuously disclosed?

---

79 U.S. Census Bureau News, Quarterly retail E-Commerce Sales http://www2.census.gov/retail/releases/historical/ecomm/15q4.pdf.

80 Enforcement actions reviewed as of January 2017.

81 FTC v. AdoreMe, Inc., Case 1:17-cv-09083 , Stipulated Order for Permanent Injunction and Monetary Judgement (November 20, 2017).

82 *Id.*

20. Privacy Certifications and Trustbrands

Privacy certifications, or "trustbrands," are seals licensed by third parties for organizations to place on their homepage or within their privacy policy. The seals typically state, or imply, that the organization which has displayed the seal has high privacy or security standards, or has had its privacy or security practices reviewed by a third party. Some seals also imply that the organization has agreed to join a self-regulatory program that may provide consumers with additional rights, such as a mechanism for resolving privacy-related disputes.

92%	89%	39%
Percentage of consumers that are worried about online privacy.[83]	The percentage of consumers who say they avoid companies that do not protect their privacy.[84]	The percentage of consumers that check for a privacy trust seal before using a website or application.[85]

What to think about when considering whether your organization should purchase a privacy certification:

1. Does the certifying agency have its own privacy or security standards?

2. Do the certifying agency's standards exceed legal requirements?

3. Does your organization's practices meet the certifying agency's standards?

4. If the certifying agency's standards change, is your organization prepared to modify its practices accordingly?

5. Has the certifying agency been investigated by the FTC, or another consumer protection authority, for deceptive or unfair practices?

6. If so, are you confident that the certifying agency's seal and review process is non-deceptive and that association with the agency will not result in negative publicity?

7. Have consumers complained to the FTC about the certifying agency?

8. Does your organization have a mechanism in place to ensure that the license for the seal is renewed each year and/or that the seal is removed from your website if the license expires?

---

83 TRUSTe & Nat'l Cyber Sec. All., U.S Consumer Privacy Index 2016 (2016), https://www.truste.com/resources/privacy-research/ncsa-consumer-privacy-index-us/.

84 Id.

85 Id.

9. Have plaintiff's attorneys used the seal against other organizations by alleging that those organizations agreed to a higher standard of care by adopting the seal?

21. Privacy Due Diligence In A Merger Or Acquisition

The FTC can hold an acquirer responsible for the bad data privacy practices of a company that it acquires. Evaluating a target's data privacy practices, however, can be daunting and complicated by the fact that many "data" issues are first identified months, or years, after a transaction has closed. For example, although it is relatively easy to read a potential target's privacy policies it is far more difficult to verify that the policy is accurate or complete.

To mitigate potential liabilities, Buyer must prioritize data governance, privacy, and security concerns from the outset of an M&A transaction, from initial evaluation to post-acquisition integration. Due diligence should begin with an evaluation of relevant state, federal, and international laws in order to appropriately tailor informational requests directed to the target. Buyer should ask for policy and procedure documents to evaluate the seller's internal controls, such as data inventories, privacy policies, information security policies, data retention policies, incident response plans, and any other data governance related documents. The target's response to due diligence requests should be used to negotiate appropriate pre-closing conditions, indemnities, and the ultimate transaction price.

$ 3 million	$350 million
Civil penalty imposed by the Federal Trade Commission upon acquirer for data privacy violation of acquisition that occurred prior to closing.[86]	The amount Verizon reduced its purchase price of Yahoo after it discovered a massive unreported data breach during acquisition.[87]

Due diligence questions to consider in a M&A transaction in order to evaluate data privacy related rsisk:

1. Has the target received a regulatory inquiry concerning its data privacy practices?

2. Has the target received litigation claims concerning its data privacy practices?

3. Has the target tracked data privacy complaints submitted to it by consumers?

4. Has the target tracked data privacy complaints submitted by consumers to government agencies, including the quantity and nature of data privacy complaints lodged with the Federal Trade Commission?

5. Is the target subject to a sector specific data privacy law?

[86] United States (FTC) v. Playdom, Case No. 11-00724 (C.D. Cal. May 11, 2011).

[87] TechCrunch, After data breaches, Verizon knocks $350M off Yahoo sale, now valued at $4.48B (February 21, 2017), https://techcrunch.com/2017/02/21/verizon-knocks-350m-off-yahoo-sale-after-data-breaches-now-valued-at-4-48b/.

6. Do the target's internal privacy policies and procedures comply with legal standards?

7. Do the target's external privacy policies and procedures comply with legal standards?

8. Has the target conducted a data map or a data inventory?

9. What are the target's data retention policies?

10. With whom does the target share data?

11. Does the target have a vendor management program in place?

12. What privacy representations has the target made to business partners?

13. Have the vendors used by the target provided appropriate contractual protections?

14. Did the target have an employee, such as a Chief Privacy Officer, who was focused on data privacy issues?

15. If the target conducted operations internationally did it have a strategy in-place for handling the cross-border transfers of information?

22. Radio Frequency Identification ("RFID")

Radio Frequency Identification ("RFID") technology uses electromagnetic fields to transfer data. RFID systems typically operate by attaching tags to objects, devices, or cards. Some tags can be powered by a local power source, such as a battery ("active RFID"). The local power permits them to transmit a signal that may be registered hundreds of meters from an RFID reader. Other tags do not have a local power source and are instead powered by electromagnetic induction from the magnetic fields that are produced by a RFID reading device in close proximity ("passive RFID").

RFID tags have been utilized in many industries. In the manufacturing sector they are used to track parts within a factory, or the location of a final product in a production line. In the agricultural sector they can be implanted in livestock to allow for the identification of animals. In the payments sector, some payment cards were embedded with RFID chips to permit consumers to process a payment by holding their payment card within close proximity of a point of sale device that was enabled with an RFID reader. As payment cards have shifted toward embedded microprocessors ("EMV"), and the financial technology community has embraced alternative wireless transmission protocols, such as Near Field Communication ("NFC") utilized by ApplePay, the use of RFID technology has declined.

Privacy advocates have voiced concern that consumer products that contain personally identifiable information that is intended to be accessible using RFID technology may be susceptible to interception or eavesdropping. Specifically, the media has expressed concern that identity thieves could be able to use remote RFID readers to remotely steal information from RFID enabled payments cards or identification cards. To-date, however, there have been relatively few (if any) confirmed instances of identity theft from RFID eavesdropping.

$17.6 Billion	15	1,066
Estimated size of the market for RFID technology.[88]	Number of states that have enacted privacy statutes focused on RFID technology.[89]	The number of wallets advertised by a prominent retailer as containing RFID blocking technology.[90]

If your organization is considering using RFID technology to track consumers, or to save personal information, you should consider the following:

1. What, if any, personal information does your organization intend to embed in an RFID tag?

2. If the personal information were accessed by an unauthorized party could it lead to identity theft?

3. Will consumers be notified about the type of information contained in the RFID tag?

4. Will consumers have any misconceptions concerning the security of their information?

5. Do you have a process for periodically evaluating any changes concerning the security of RFID tags?

23. Responding To Government Subpoenas And Document Requests That Ask For Personal Information

Federal and state agencies traditionally obtain information for law enforcement purposes using a variety of methods including:

- court issued subpoenas,
- grand jury subpoenas,
- search warrants,
- litigation discovery requests, and
- administrative subpoenas. [91]

---

88 Source: Statista.com *available at* http://www.statista.com/statistics/299966/size-of-the-global-rfid-market/ (last checked Jan. 2018).

89 National Conference of State Legislatures Survey of RFID Privacy Laws *available at* http://www.ncsl.org/research/telecommunications-and-information-technology/radio-frequency-identification-rfid-privacy-laws.aspx (last viewed Jan. 2018).

90 Search of Walmart.com for "RFID Wallet" conducted in January 2018.

91 We use administrative subpoenas here to refer to "all powers, regardless of name, that Congress has granted to federal agencies to make an administrative or civil investigatory demand compelling document production or testimony" U.S. Department of Justice Office of Legal Policy, Report to Congress on the Use of Administrative Subpoena Authorities by

A request by a government agency for personal information about one, or more, consumers may conflict with consumers' expectations of privacy, and, in some instances, may arguably conflict with legal obligations imposed upon an organization not to produce information. For example, if an organization promises within its privacy policy that it will never share the information that it collects with a "third party" and does not include an exception for requests from law enforcement, or government agencies, a consumer could argue that by producing information pursuant to a government request, an organization has violated its privacy policy and committed an unfair or deceptive practice in violation of federal or state law.

335
Number of federal authorities that permit various federal agencies to issue administrative subpoenas.[92]

If you receive a government request for personal information consider the following steps and questions:

1. Does your organization maintain an internal procedure or protocol for how to respond to a government information request?

2. Has your organization made any representations to consumers that might be interpreted as indicating that information will not be provided to the government?

3. Was the information request actually issued by the agency that purported to issue it (*i.e.*, independently confirm with the issuing agency that the request is authentic)?

4. Confirm that the issuing agencies do, in fact, want you to produce personal information.

5. Has the government agency provided notice to the people about whom the information relates of the request?

6. Does the request include a legal basis (e.g., an authorizing statute) for making the information request? If so, does the authorizing statute permit the agency to obtain the type of information requested?

7. Does the authorizing statute require the agency to comply with a specific procedural process prior to requesting the information? If so, has the agency complied?

8. Will complying with the information request pose an undue burden on your organization?

9. Are there any laws or regulations that may allow your organization to resist the information request?

Executive Branch Agencies and Entities Pursuant to Public Law 106-544, [hereinafter DoJ Report] available at https://www.justice.gov/archive/olp/rpt_to_congress.htm.

92 *Id.*

10. Has the request been issued, or reviewed, by a Court?

11. What opportunities does your organization have to negotiate with the agency to limit the quantity of personal information produced and/or to seek administrative or judicial review concerning the agency's need to obtain personal information?

24. Responding To National Security Letters That Ask For Personal Information

National Security Letters ("NSLs") refer to a collection of statutes that authorize certain government agencies to obtain information and simultaneously impose a secrecy obligation upon the recipient of the letter.

Four statutes permit government agencies to issue NSLs: (1) the Electronic Communication Privacy Act,[93] (2) the Right to Financial Privacy Act,[94] (3) the National Security Act,[95] and the (4) Fair Credit Reporting Act.[96] Although differences exist between the letters issued under each statute, in general, all of the NSLs permit a requesting agency to prevent an organization that receives the NSL from disclosing the fact that it received the request, or the type of information that was requested, if disclosure may result in a danger to national security, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of a person. If the recipient of a NSL wishes to challenge a non-disclosure request accompanying a NSL, the recipient may file a petition with a U.S. district court in the district where the person does business,[97] or, the recipient may request that the requesting agency obtain judicial review of the nondisclosure request.[98] In both instances, the requesting agency must file an application with the court setting forth the reasons for the nondisclosure request.

Notwithstanding any nondisclosure requests, NSL recipients may publicly report on a semiannual or annual basis certain information regarding aggregate NSL requests the entity receives.[99] The information that may be reported is limited to identifying in aggregate the rough quantity of NSL requests received (*e.g.*, 0-99 or 0-249) depending on the reporting format chosen.[100]

19,212	16,348	12,870	12,150
Number of NSLs issued in 2013[101]	Number of NSLs issued in 2014[102]	Number of NSLs issued in 2015[103]	Number of NSLs issued in 2016.[104]

93 18 U.S. C. § 2709.

94 12 U.S.C. § 3414.

95 50 U.S.C. § 3162.

96 15 U.S.C. § 1681v; 15 U.S.C. § 1681u.

97 18 U.S.C. § 3511(b).

98 *Id.*

99 50 U.S.C. § 1874.

100 *Id.*

101 Office of the Director of National Intelligence, Statistical Transparency Report: Regarding the Use of National Security Authorities for Calendar Year 2016, April 2017, available at: https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016.

If you receive a NSL, consider the following steps and questions:

1. Does your organization maintain an internal procedure or protocol for how to respond to a government information request, and specifically to a NSL? If so, to the extent permitted under the NSL, follow the procedure to ensure internal awareness of the request.

2. Was the information request actually issued by the agency that purported to issue it? Consider independently confirming with the issuing agency that the request is authentic.

3. Confirm that the issuing agency does, in fact, want you to produce personal information. If so, attempt to negotiate with the issuing agency to reduce the type or volume of personal information requested.

4. Is the issuing agency permitted, under the statutes discussed above, to issue NSLs? If so, does the statute upon which the agency relies apply to your organization? Does the statute upon which the agency relies permit the agency to collect the type of information requested?

5. Will complying with the NSL conflict with any contractual, statutory, or international privacy obligations? If so, consider raising this issue with the requesting agency to determine whether the NSL can be amended to avoid the conflict.

25. Responding To Third Party (Non-Government) Civil Subpoenas And Document Requests That Ask For Personal Information

Litigants in a civil dispute often use subpoenas, subpoenas *duces tecum*, and discovery requests to obtain personal information about individuals who may not be present in the litigation. A request for documents and information that include personal information about third parties may conflict with legal obligations imposed upon an organization not to produce information. For example, if an organization promises within its privacy policy that it will never share personal information with a "third party," and does not include an exception for requests made in civil litigation or through judicial process, a consumer could argue that by producing information pursuant to a subpoena or discovery request an organization has violated its privacy policy and committed an unfair or deceptive practice in violation of federal or state law.

In addition, some states have adopted specific statutes or procedural rules that are designed to protect the privacy interests of absent consumers. For example, California Civil Procedural Rule § 1985.3 prevents a party from issuing a subpoena for personal information from a variety of organizations including medical providers, banks, credit unions, lenders, brokerage firms, or insurance companies, unless the party issuing the subpoena provides a copy to the consumer whose records are sought, and informs them that they have a right to object to the organization furnishing information about them. The rule also requires that the

---

[102] *Id.*

[103] *Id.*

[104] *Id.*

party issuing the subpoena provide the consumer sufficient time to receive, and object, before production is anticipated.

14,641,848	367,937
2016 Statewide Incoming Civil Caseload.[105]	Number of Cases filed in Federal District Courts in 2017.[106]

If you receive a subpoena or document request asking for personal information about consumers consider the following steps and questions:

1. Does your organization maintain an internal procedure or protocol for how to respond to a subpoena or civil discovery request?

2. Has your organization made any representations to consumers that might be interpreted as indicating that information will not be provided to a requesting party, or that your organization will take certain steps (*e.g.,* informing them of the request) before producing such information?

3. Does a law within the state in which the consumer is resident restrict or prevent you from complying with the subpoena? Does a law within the state from which the subpoena is issued restrict or prevent you from complying with the subpoena?

4. Is a protective order in place that would mitigate against privacy harms that might occur from disclosure? If so, is the protective order sufficient to protect a consumer's privacy interest?

5. Has a court already evaluated the information request and weighed the privacy implications of production?

[105] National Center for State Courts, Court Statistics Project, "2016 Civil Caseloads - Trial Courts" http://www.ncsc.org/Sitecore/Content/Microsites/PopUp/Home/CSP/CSP_Intro.

[106] Administrative Office of the United States Courts, "Federal Judicial Caseload Statistics 2017 (Available at: http://www.uscourts.gov/statistics-reports/federal-judicial-caseload-statistics-2017).

26. Social Media Privacy Concerns

The majority of organizations utilize social media to market their products and services, interact with consumers, and manage their brand identity. Many mobile applications and websites even permit users to sign-in with their social media accounts to purchase items or use the applications' services.

While using third party social media websites has significant advantages for businesses, it also raises distinct privacy concerns. Specifically, the terms of use that apply to social media platforms may give the platform the right to share, use, or collect information concerning your business or your customers. To the extent that the social media platform's privacy practices are not consistent with the practices of your own organization, they may contradict or violate the privacy notice that you provide to the public.

84%	97%
Percentage of Fortune 500 companies on Facebook.[107]	Percentage of Fortune 500 companies with a corporate presence on LinkedIn.[108]
69%	500 million
Percentage of online adults who use at least one social media site.[109]	Number of accounts stolen in Yahoo's 2014 data breach.[110]

What to consider when evaluating your organization's use of social media:

1. How would a data breach of social media platforms affect your organization? Do you have a plan if your social media account is breached?

2. Does your organization share information with an intermediate service provider, such as a social media analytics company, to provide or analyze social media services?

3. Is your internal data or customer personal information protected under your agreements with third parties, including social media platforms?

4. What types of customer personal information are solicited, collected, maintained, or disseminated via your social media platforms (*e.g.*, geo-location)?

5. Do you display information or images of users or other people, including your employees? Did the people in the images give their permission and/or sign a release?

---

107 Nora Ganim Barnes & Jessica Griswold, Use of Popular Tools Remains Constant as Use of Instagram Expands Quickly Among the 2016 Fortune 500, http://www.umassd.edu/cmr/socialmediaresearch/2016fortune500/.

108 *Id.*

109 Pew Research Center, Social Media Fact Sheet, http://www.pewinternet.org/fact-sheet/social-media (last visited Dec. 28, 2017).

110 Seth Fiegerman, Yahoo says 500 million accounts stolen, CNN, (September 22, 2016), http://money.cnn.com/2016/09/22/technology/yahoo-data-breach/.

6. Is your client list private? Do your employees connect to your clients on social media?

7. How is information about your customers that is collected from social media sites being stored? Do any third parties have access to that information?

8. Do users log-in to your services or make purchases through a social media platform?

9. What type of personal information do your customers share with you on social media platforms? Does your use comply with the platform's policy for collecting data from users? Do you review the platform's policies regularly?

10. Does your organization have a social media policy governing employees' use of social media, particularly pertaining to sharing confidential customer and organizational data on the platform?

27. Social Security Number Privacy Policies

Social Security Numbers ("SSN") were originally established by the Social Security Administration to track earnings and eligibility for Social Security benefits. Because a SSN is a unique personal identifier that rarely changes, federal agencies use SSN for purposes other than Social Security eligibility (*e.g.,* taxes, food stamps, etc.). In 1974, Congress passed legislation requiring federal agencies that collect SSN to provide individuals with notice regarding whether the collection was mandatory and how the agency intended to use the SSN.[111] Congress later barred agencies from disclosing SSN to third parties. Federal law does not, however, regulate private-sector use of SSN.

In the United States SSN is used throughout the financial sectors to identify unique account holders and to track their transactions and experience between and among financial service providers through the use of credit reports; almost every financial institution requires that a prospective customer provide their SSN in order for the institution to obtain a credit report on the individual. The net result is that SSNs have become a key-identifier used in the establishment of new accounts and, as a result, a key asset used by identity thieves when impersonating a consumer for the purpose of fraudulently opening a new account.

Based upon a growing recognition that SSN are often one of the identifiers used to perpetrate identity theft, state legislatures have passed statutes regulating the private sector's use of SSN. Among other things, these statutes prohibit organizations from printing SSN on consumer cards, sending SSN through the mail, requiring that a consumer transmit SSN unencrypted over the internet, or requiring that individuals use their SSN to access a website without multi-factor authentication. Many states also have statutes that require that companies securely destroy SSN when the information is no longer in use.

[111] The Privacy Act of 1974, 5 U.S.C. § 552a.

1936	$1	$500 / month
Year Social Security Numbers were created.[112]	Cost on the black market to obtain a consumer's SSN.[113]	Civil penalty imposed by one state for failing to adopt a privacy policy when collecting SSN.[114]

Some states have gone beyond regulating the use, disclosure, and destruction of SSN and require that organizations that collect SSN publicly post a privacy policy that explains the following:

(1) how the organization collects SSN,

(2) how the organization uses SSN,

(3) who within the organization will have access to SSN,

(4) how the organization will protect SSN, and

(5) the organization's limitations on SSN disclosure.

Other states require organizations to internally publish privacy policies as part of their employee handbook or procedures manual. In addition to the topics listed above, these internal policy must establish penalties for employees that misuse SSN.[115]

28. Vehicle Event Data Recorders

Event data recorders, also known as "black boxes" or "sensing diagnostic modules," capture information such as the speed of a vehicle and the use of a safety belt. In the event of a collision this information can be used to help understand how the vehicle's systems performed.

In December of 2012, the National Highway Traffic Administration proposed a rule that would require automakers to install event data recorders in all new light passenger vehicles. Although the proposed rule would have required manufacturers to install the devices beginning in 2014, the rule was never finalized. Nonetheless, some estimates indicate that most passenger cars are already equipped by manufacturers with event data recorders.

Since 2005 states have passed statutes designed to address the privacy implications of event data recorders. Although variability exists among the state statutes, most statutes require that a consumer be notified of the existence of the device prior to purchase, and restrict who may access the information on the device.

---

112 Social Security Administration, The First Social Security Number and the Lowest Number, http://www.ssa.gov/history/ssn/firstcard.html.

113 Brian Stack, Experian "Here's How Much Your Personal Information Is Selling For on the Dark Web," (Dec. 6, 2017) *available at* https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.

114 Tex. Bus. & Com. Code § 501.052(a), 501.053(a).

115 Michigan Compiled Laws § 445.84(1)(e), (2).

On December 4, 2015, the federal Driver Privacy Act of 2015 was enacted. The Act makes clear that data collected from an event data recorder belongs to the owner or lessee of the vehicle. The Act also provides that data recorded or transmitted by an event data recorder may not be accessed by a person other than the vehicle's owner or lessee, except in certain defined circumstances.

96%	17	7
Estimate of the number of new passenger cars equipped with event data recorders.[116]	The number of states that have passed legislation protecting the privacy of data on event data recorders.[117]	The number of exceptions included in some state statutes for who may access the data.[118]

What to think about when utilizing event data recorders:

1. If your organization is placing event data recorders on vehicles, are you permitted by state statute to do so?

2. If your organization intends to use event data recorder information, which state statute governs your use?

3. If your organization is using event data recorder information, does the organization (or the use) fall under one of the exceptions set forth in the state statutes?

4. What are the penalties for failing to obtain appropriate consent?

5. If you have obtained consent, is your consent current and valid?

29. Video Viewing Information

The Video Privacy Protection Act ("VPPA") was passed in 1988 in reaction to a fear that people other than a consumer and their video rental store might access information on a consumer's video rental history. This was not an academic concern at the time. Immediately prior to the passage of the VPPA, Judge Robert Bork, who had been nominated to the Supreme Court, had his video rental history published by a newspaper that was investigating whether he was fit to hold office.

Among other things, the VPPA protects consumers by limiting the disclosure of rental and sales records by video tape service providers to the consumer, people who have the consumer's consent, and law enforcement agencies who have a warrant, subpoena, or court

[116] Nat'l Highway Transp. Safety Admin., U.S. DOT Proposes Broader Use of Event Data Recorders to Help Improve Vehicle Safety, (December 7, 2012), http://www.nhtsa.gov/About+NHTSA/Press+Releases/U.S.+DOT+Proposes+Broader+Use+of+Event+Data+Recorders+to+Help+Improve+Vehicle+Safety.

[117] National Conference of State Legislatures, Privacy of data from Event Data Recorders: State Statutes, (December 12, 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx.

[118] *See*, *e.g.*, Ark. Code § 21-112-107 (2015).

order. Recently, the plaintiff's bar has tried to revive the VPPA by applying its provisions to websites that stream movies and digital content, such as iTunes, Amazon Video, and Netflix.

59%	>407 hours	$2,500
Percentage of US homes with access to a subscription-based video-on demand (SVOD) service.[119]	The amount of time spent by an average consumer viewing video content each month.[120]	Potential liability per violation of the VPPA.[121]

If your organization rents, sells, or streams video content consider the following steps to reduce your risk of liability under the VPPA:

1. Does your organization fall under the definition of a video tape service provider or a provider of similar audio visual materials as those terms are defined under the VPPA?

2. Does your organization share information concerning consumers' video viewing habits with any third parties?

3. Which platforms does your organization use to provide access to videos?

4. Does the video platform transmit personal information to third parties?

5. Does your organization obtain consent prior to sharing information about consumers that view video content?

30. Website Privacy Policies

Although financial institutions, health care providers, and websites directed to children are required to create consumer privacy policies under federal law, other types of websites are not. In 2003 California became the first state to impose a general requirement that most websites post a privacy policy.

Under the California Online Privacy Protection Act ("CalOPPA"), all websites that collect personal information about state residents must post an online privacy policy if the information is collected for the purpose of providing goods or services for personal, family, or household use.[122] Since the passage of CalOPPA, most websites that collect information – whether or not they are directed at California residents or are otherwise subject to the CalOPPA – have chosen to post an online privacy policy. Recently, California's Attorney General announced the release of a new form that allows consumers to report potential violations of CalOPPA online. This online reporting tool will increase California's ability to identify and notify entities in violation of CalOPPA.

---

119 Nielsen, The Total Audience Report Q2 2017, http://www.nielsen.com/us/en/insights/reports/2017/the-nielsen-total-audience-q2-2017.html.

120 *Id.* at 20.

121 18 U.S. Code § 2710(c)(2)(A).

122 Cal. Bus. & Prof. Code § 22575, *et seq.*

On January 1, 2016, Delaware followed suit by enacting the Delaware Online Privacy and Protection Act ("DOPPA"). Similar to CalOPPA, DOPPA requires that website and app operators that collect personally identifiable information of Delaware residents conspicuously post a comprehensive privacy policy and conform to other privacy related requirements.[123]

3	10 minutes	244 hours	$0.59
Number of states that require operators of websites that collect PII to disclose a privacy policy.[124]	Average time it takes for a person to read a privacy policy.[125]	The amount of time it would take a person to read the privacy policies of all the unique websites they visit in a year.[126]	The premium that study participants were willing to pay to purchase a $15 item from a website that proactively displayed strong privacy protections from one with no privacy position.[127]

What to think about when drafting or reviewing a privacy policy:

1. Is your organization subject to a federal law that requires that a privacy policy take a particular form, or include particular information?

2. Does the privacy policy describe the main ways in which your organization collects information?

3. Does the privacy policy describe the ways in which your organization shares information with third parties?

4. Does the privacy policy discuss data security? If so, is the level of security indicated appropriate?

5. Would the privacy policy interfere with a possible merger, acquisition, or sale of your organization's assets?

6. Would the privacy policy interfere with future ways in which your organization may want to monetize data?

7. Does the privacy policy use terms that might be misunderstood or misinterpreted by a regulator or a plaintiff's attorney?

---

123 6 Del.C. § 1201C, *et seq.*

124 California, Delaware, and Nevada.

125 Aleecia M. McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4(3) I/S: A Journal of Law and Policy for the Information Society, 541 (2008).

126 *Id.*

127 Janice Tsai, et al., The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, 6th Workshop on the Economics of Information Security (WEIS), (June 2007), http://www.econinfosec.org/archive/weis2007/papers/57.pdf.

8. Does the privacy policy comply with the laws in each jurisdiction in which your organization is subject (*i.e.,* CalOPPA or DOPPA)?

9. Should the privacy policy only govern information collected via your organization's website, or all information collected by your organization?

10. Does the privacy policy appropriately disclose and discuss network marketing and behavioral advertising?

11. Does the privacy policy need to discuss the tracking that your organization may conduct of its clients or website visitors?

12. Could the privacy policy be understood by the average person?

13. Can the privacy policy be easily viewed on a smartphone or a mobile device?

14. Does the policy provide information to users concerning how they can contact your organization about privacy related questions or complaints?

15. Does the policy discuss what information may be modified or changed by a user?

DATA SECURITY

31. Autonomous Vehicles – Cybersecurity Issues

In the next five years we will see more and more self-driving vehicles, or autonomous vehicles, hit the market. An "autonomous vehicle" is a vehicle capable of navigating roadways and interpreting traffic-control devices without a driver actively operating any of the vehicle's control systems. Although self-driving vehicles have the potential to drastically reduce accidents, travel time, and the environmental impact of road travel, concerns remain that could delay widespread adoption. Of particular concern are data privacy and security risks.

The numerous points of entry into a self-driving vehicle's computer system give clever thieves and cyber terrorists multiple opportunities to take control of vehicles. For example, in 2010, one man in Austin, Texas triggered horns and disabled the ignition systems in more than 100 *non-autonomous* vehicles by hacking into an auto dealer's computer system.[128] Additionally, in 2015, two cybersecurity researches hacked into a vehicle's internal network and paralyzed it on a highway.[129] While hackers like these can control non-autonomous vehicles through entry points like internal network systems, entertainment systems, hand-free cell-phone operations, and satellite radio, self-driving vehicles are even more vulnerable to attacks, because they have all of those entry points plus many more.

The automotive industry has addressed the issue of cybersecurity of self-driving vehicles by creating a series of Automotive Cybersecurity Best Practices ("Automotive Best

[128] Wired, *Hacker Disables More Than 100 Cars Remotely* (Mar. 17, 2010), https://www.wired.com/2010/03/hacker-bricks-cars/.

[129] Wired, *The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse* (Aug. 1, 2016), https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/.

Practices").[130] The Automotive Information Sharing and Analysis Center ("Auto-ISAC") issued the Automotive Best Practices, which guide how individual companies can implement the previously released "Enhance Automotive Cybersecurity" Principle. The Automotive Best Practices cover organizational and technical aspects of vehicle cybersecurity, including governance, risk management, security by design, threat detection, incident response training, and collaboration with appropriate third parties. In effect, the Automotive Best Practices prompt participating members to enhance the security of self-driving vehicles by managing cybersecurity at the product level. The Automotive Best Practices are listed below.

In addition to the automotive industry, the federal government has also issued non-binding guidance to the motor vehicle industry for improving cybersecurity issues of autonomous vehicles. The National Highway Traffic Safety Administration ("NHTSA") first issued guidelines in October 2016,[131] and updated its guidelines in September 2017 (NHTSA Best Practices 2.0).[132] Specifically, in an effort to reduce the probability of a successful cybersecurity attack, those cybersecurity best practices promote a layered approach to vehicle cybersecurity. Like the first version, the updated version recommends that the industry dedicate resources to assessing risk and testing vehicles for cybersecurity vulnerabilities. However, the updated version puts even more emphasis on the importance of responding to incidents than the first version. For example, NHTSA now recommends that entities have a documented process for transitioning to a minimal risk condition when a problem is encountered and consider methods of returning self-driving vehicles to a safe state immediately after being involved in a crash. Additionally, unlike the first version, the updated version includes guidelines for state legislatures and highway safety officials. The NHTSA recommends that those entities document how they intend to account for all applicable Federal, State, and local laws in the design of their vehicles and self-driving vehicles. The NHTSA Best Practices 2.0 have been listed below.

$1.3 Trillion	1.5 million	21	94%
The estimated amount of savings in the U.S. that will be caused by the adoption of driverless cars.[133]	The number of vehicles NHTSA's enforcement authority recalled in July 2015 due to cybersecurity vulnerabilities.[134]	The number of states to date that have introduced and passed legislation relating to self-driving vehicles.[135]	The percentage of fatalities on U.S. roads in 2014 that were caused by human error or faulty decision-making.[136]

[130] Automotive Information Sharing and Analysis Center, *Automotive Cybersecurity Best Practices Executive Summary* (July 21, 2016), https://www.automotiveisac.com/best-practices/.

[131] National Highway Traffic Safety Administration, *Cybersecurity Best Practices for Modern Vehicles* (Oct. 2016), https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

[132] National Highway Traffic Safety Administration, *Automated Driving Systems: A Vision for Safety* (Sep. 2017), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.

[133] Morgan Stanley, *Autonomous Cars: The Future Is Now* (January 23, 2015), http://www.morganstanley.com/articles/autonomous-cars-the-future-is-now.

[134] National Highway Traffic Safety Administration, *Cybersecurity Best Practices for Modern Vehicles* (Oct. 2016), https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

[135] National Conference of State Legislatures, *Autonomous Vehicles: Self-Driving Vehicles Enacted Legislation* (October 23, 2017), http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx.

Automotive Best Practices enacted by the Auto-ISAC, including some of the various specifications:

1. Governance:
   a. Define executive oversight for product security.
   b. Communicate oversight responsibility to all appropriate internal stakeholders.
   c. Establish governance processes to ensure compliance with regulations, internal policies, and external commitments.
2. Risk Assessment and Management:
   a. Establish standardized processes to identify, measure, and prioritize sources of cybersecurity risk.
   b. Monitor and evaluate changes in identified risks as part of a risk assessment feedback loop.
   c. Establish a process to confirm compliance by critical suppliers to verify security requirements, guidelines, and trainings.
3. Security by Design:
   a. Identify and address potential threats and attack targets in the design process.
   b. Layer cybersecurity defenses to achieve defense-in-depth.
   c. Perform software-level vulnerability testing, including software unit and integration testing.
4. Threat Detection and Protection:
   a. Assess risk and disposition of identified threats and vulnerabilities using a defined process consistent with overall risk management procedures.
   b. Identify threats and vulnerabilities through various means, including routine scanning and testing of the highest risk areas.
   c. Report threats and vulnerabilities to appropriate third parties based on internal processes.
5. Incident Response and Recovery:
   a. Document the incident response lifecycle, from identification and containment through remediation and recovery.
   b. Perform periodic testing and incident simulations to promote incident response team preparation.
   c. Notify appropriate internal and external stakeholders of a vehicle cyber incident.
6. Training and Awareness:
   a. Establish training programs for internal stakeholders across the motor vehicle ecosystem.
   b. Educate employees on security awareness, roles, and responsibilities.
   c. Tailor training and awareness programs to roles.
7. Collaboration and Engagement with Appropriate Third Parties:
   a. Engage with industry bodies, such as the Auto-ISAC, Auto Alliance, Global Automakers, and others.
   b. Engage with academic institutions and cybersecurity researchers, who serve as an additional resource on threat identification and mitigation.

---

[136] ABA Section of Administrative Law, *The Fast Lane: Autonomous Vehicles and the Liability Landscape* (Spring 2016, https://www.americanbar.org/content/dam/aba/publications/administrative_regulatory_law_newsletters/tq_spring_ 2016. authcheckdam.pdf.

c. Form partnerships and collaborative agreements to enhance vehicle cybersecurity.

NHTSA Best Practices 2.0

1. System Safety:
   a. Follow a robust design and validation process based on industry standards.
2. Operational Design Domain:
   a. Define and document the Operational Design Domain (ODD) for each self-driving vehicle available for use on public roadways.
   b. The ODD should include, at a minimum, roadway types, geographic area, speed range, environmental conditions, and other domain constraints.
3. Object and Event Detection and Response:
   a. Have a documented process for assessment, testing, and validating of the self-driving vehicle's capabilities.
4. Fallback (Minimal Risk Condition):
   a. Have a documented process for transitioning to a minimal risk condition when a problem is encountered or the self-driving vehicle cannot operate safely.
   b. Fallback strategies should take into account that human drivers may be inattentive, under the influence of alcohol or other substances, drowsy, or otherwise impaired.
5. Validation Methods:
   a. Develop validation methods to appropriately mitigate the safety risks associated with their self-driving vehicle approach.
6. Human Machine Interface:
   a. Consider and document a process for the assessment, testing, and validation of the vehicle's HMI design.
7. Vehicle Cybersecurity:
   a. Follow a robust product development process that includes a systematic and ongoing safety risk assessment for each self-driving vehicle, the overall vehicle design into which it is being integrated, and when applicable, the broader transportation system.
   b. Document how your entity incorporates vehicle cybersecurity considerations into self-driving vehicles, including all actions, changes, design choices, analyses, and associated testing.
8. Crashworthiness:
   a. Consider incorporating information from the advanced sensing technologies needed for self-driving vehicle operation into new occupant protection systems that provide enhanced protection to occupants of all ages and sizes.
9. Post-Crash Self-Driving Vehicle Behavior:
   a. Consider methods of returning self-driving vehicles to a safe state immediately after being involved in a crash, such as shutting off the fuel pump, removing motive power, moving the vehicle to a safe position off the roadway, disengaging electrical power, and other actions that would assist the self-driving vehicles.
10. Data Recording:
    a. Establish a documented process for testing, validating, and collecting necessary data related to the occurrence of malfunctions, degradations, or failures in a way that can be used to establish the cause of any crash.

11. Consumer Education and Training:
    a. Develop, document, and maintain employee, dealer, distributor, and consumer education and training programs to address the anticipated differences in use and operation of self-driving vehicles from those of the conventional vehicles.
12. Federal, State, and Local Laws:
    a. Document how your entity intends to account for all applicable Federal, State, and local laws in the design of their vehicles and self-driving vehicles.

Factors the NHTSA will consider in determining whether a cybersecurity vulnerability compels a recall:

1. The amount of time elapsed since the vulnerability was discovered (e.g., less than one day, three months, or more than six months);
2. The level of expertise needed to exploit the new vulnerability (e.g., whether a layman can exploit the vulnerability or whether it takes an expert to do so);
3. The accessibility of knowledge of the underlying system (e.g., whether how the system works is public knowledge or whether it is sensitive and restricted);
4. The necessary window of opportunity to exploit the vulnerability (e.g., an unlimited window or a very narrow window); and
5. The level of equipment needed to exploit the vulnerability (e.g., standard or highly specialized).

Questions to consider when addressing cybersecurity issues of self-driving vehicles:

1. What are the functions of the new self-driving technology and what are the implications if they were compromised?
2. Who has authority and enforcement power to govern the security system of the self-driving vehicle?
3. Does your company need to notify owners of self-driving vehicles of the risks their vehicle presents?
4. How can your company guard against hacks for control of the vehicle?
5. What is the safety risk to society and the value risk to your company?
6. What can your company do to minimize exposure to the potential loss or damage to owners of self-driving vehicles?
7. How should your company anticipate how the conscious and malicious acts of third parties affect the vehicle?
8. What design decisions could your company make with respect to the risk assessment process?
9. How can your company protect identities of users and avoid tracking users while they are in their self-driving vehicle?
10. Will your company's vehicle cybersecurity protections unduly restrict authorized access by alternative third-party repair services?

32. Bounty or Bug Programs

Data security officers typically look for security risks by monitoring reports from automated security systems, listening to employees' reports of security issues, and/or auditing IT systems. Some security officers, however, rely on a somewhat unusual source – the public. They look to clients, customers, consumers, academics, researchers, amateur hackers, and not-so-amateur hackers to bring security vulnerabilities to their attention. Like many industries

that have embraced crowdsourcing, the idea is that the more people that are involved in finding bugs and security flaws the better a company can make its security.

There is a great deal of debate about the merits of listening to the security concerns of people outside of an organization. On one end of the spectrum, some organizations refuse to discuss any aspect of their security with the public. On the other end of the spectrum, organizations proactively encourage the public to report security vulnerabilities by paying well-meaning hackers (usually called "white hat hackers" or "independent researchers") to report problems. While these organizations view "bounty" programs as commonsense crowdsourcing, others view the concept of paying someone who has hacked a company's system as extortion.

As more companies move to establish bounty programs third parties have begun to offer platforms or frameworks to help organize the programs. Some frameworks provide a forum in which companies can communicate with hackers, a method to facilitate payments to hackers, and guidelines for hackers to follow when identifying vulnerabilities and reporting them to participating companies. Other platforms promote invitation-only communities to test a company's security. For many companies this provides a middle ground that permits them to take advantage of crowd sourcing without inviting the world to test their gates.

The following provides a snapshot of information on bounty programs as well as a checklist for organizations that are considering starting a program, or are evaluating the structure of their existing program.

516	51%	$200k
The number of organizations that have established data security bounty programs.[137]	The percentage of bounty programs that pay a bounty or provide some sort of reward (e.g., swayg).[138]	Maximum reward offered through Apple's bounty program.[139]
$100 to $25,000		
Typical range of rewards offered for programs that pay monetary compensation.		

What to think about if you do not enact a bounty program:

1. What are the practical implications if the organization views the unauthorized access to its network by a white-hat or grey hat hacker as "unauthorized?"

2. What are the practical implications if a "white hat" hacker tries to breach your security with no guidelines on how they should act?

3. Is there a risk that individuals who know of a security vulnerability may provide that information to bad actors instead of providing it, first, to you?

---

137 Statistics from Vulnerability Laboratory, Bug Bounties, Rewards, and Acknowledgements, http://vulnerability-lab.com/list-of-bug-bounty-programs.php (last checked Dec. 26, 2017).

138 Based upon review of data obtained from vulnerability labs, infra.

139 Mikey Campbell, "Apple's Bug Bounty Program Hindered by Low Payouts, Reports Say," ApplieInsider.com (July 6, 2017) *available at* http://appleinsider.com/articles/17/07/06/apples-bug-bounty-program-hindered-by-low-payouts-report-says (last checked Dec. 26, 2017).

4. Is there a risk that individuals who know of a security vulnerability may provide that information to the media or to regulators instead of providing it, first, to you?

5. Would the organization view every unsolicited request for payment by a hacker as extortion?

What to think about if you do enact a bounty program:

1. Will you be encouraging more breaches to your system?

2. Do you have confidence that you can track / monitor successful participants?

3. Will all of your systems be "in scope" for the bounty program?

4. Should certain forms of attack be prohibited (e.g. denial of service attacks)?

5. Will employees be eligible to participate?

6. Will the program be focused on weaknesses to the security of sensitive personal information, to the performance of IT infrastructure, or to both?

7. Will you proactively disclose the level of compensation that a participant should expect?

8. What conditions of confidentiality will you impose on participants?

9. How can you avoid the unintentional access or acquisition of sensitive personal information?

10. Will you utilize a third party that manages, hosts, or provides a framework for your program?

33. Causes of Healthcare Data Breaches

Pursuant to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), covered entities (e.g. healthcare providers and health plans) must notify the Department of Health and Human Services ("HHS") of breaches of unsecured protected health information ("PHI").[140] The information provided to HHS provides companies with a high level of insight concerning the types of breaches that occur in the health care industry.

The data collected by HHS concerning breaches affecting 500 or more individuals within the last 24 months, as of November 20, 2017, shows hacking/IT incidents surpassed unauthorized access or disclosure as the most common forms of data breach in the health sector.

[140] 45 C.F.R. §164.408(a)-(b).

36% The percentage of reported breaches caused by unauthorized access or disclosure.[141]	4% The percentage of reported breaches caused by improper disposal and loss.[142]
15.5% The percentage of reported breaches caused by theft of hardware of all types.[143]	44.5% The percentage of reported breaches caused by hacking/IT incidents.[144]

Things to consider when reviewing your information security program in light of HHS data:

1. Conduct regular risk assessments;
2. Have a formal incident response plan in place;
3. Encrypt data and hardware, such as servers, network end points, mobile and medical devices;
4. Educate employees about HIPAA;
5. Implement different access levels for employees' access to PHI based on their job duties;
6. Immediately stop access to PHI by terminated employees and escort them if necessary;
7. Require a two-step verification process to ensure that mail and email recipients' information is correct before sending invoices or appointment reminders;
8. Transition from paper records to secure, encrypted computer databases;
9. Shred paper records when no longer needed;
10. Prevent break-ins by implementing physical safeguards such as security alarms, security guards, and locks on windows and doors.

34. Class Action Litigation Trends

There is a great deal of misunderstanding concerning data security breach-related class actions. In large part the media and the legal media have exaggerated the quantity (and success) of class action litigation.

The following provides an overview of the risks associated with lawsuits following data security breaches.[145]

---

141 U.S. Dep't of Health and Human Servs. Office for Civ. Rights, Breaches Affecting 500 or More Individuals, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (November 20, 2017).

142 *Id.*

143 *Id.*

144 *Id.*

76	27	3.3%
The total number of data security breach related class actions filed in federal court in a year.[146]	The number of unique defendants that were sued (after multiple pile-on suits were removed).[147]	Percentage of publicly reported data breaches that led to a class action filing.[148]
21	95%	89%
The number of different legal theories used by plaintiffs in their attempt to find a theory of recovery.[149]	The percentage of class action laws suits that were premised, at least in part, on a negligence theory.[150]	The percentage of data breach related class action litigation that involved the exposure of a sensitive category of information.[151]

The following are some of the factors that you should look at when considering the likelihood of receiving a class action complaint following a data breach:

1. Has the media widely reported on your data breach?
2. If so, did the media report your data breach before, or after, the company notified impacted consumers?
3. Was the quantity of records lost lower, or greater, than the average number of records involved in recent class action lawsuits?
4. Did consumers suffer any direct monetary harm?
5. Could the data fields involved lead to identity theft?
6. Has there been any evidence of actual identity theft?
7. Did you offer credit monitoring, identity theft insurance, and/or credit repair services?
8. If so, what percentage of impacted consumers availed themselves of your offer?

---

145 Romanosky, et al, Empirical Analysis of Data Breach Litigation, 11(1) Journal of Empirical Legal Studies June 1, 2012), http://www.econinfosec.org/archive/weis2012/papers/Romanosky_WEIS2012.pdf.

146 Bryan Cave LLP, 2017 Data Breach Litigation Report A Comprehensive Analysis of Class Action Lawsuits Involving Data Security Breaches Filed in United States District Courts at 1 *available at* https://d11m3yrngt251b.cloudfront.net/images/content/9/6/v2/96690/Bryan-Cave-Data-Breach-Litigation-Report-2017-edition.pdf.

147 *Id.*

148 *Id.*

149 *Id.*

150 *Id.*

151 *Id.*

9. Has the jurisdiction in which you are most likely to receive a lawsuit (e.g., where you are incorporated or primarily operate your business) permitted other data security class action complaints to proceed past the pleadings stage?

10. Is a plaintiff's firm looking at government records for information relating to your organization's data security practices? For example, have they submitted requests to the FTC under the Freedom of Information Act?

35. Cloud Computing

Most companies today use some form of cloud computing whether through software-as-a-service, platform-as-a-service, or infrastructure-as-a-service. Cloud computing's cost-effective scalability can offer significant advantages to an organization, but it can also raise significant security concerns. Although many cloud providers offer assurances that their systems are secure, many are also unwilling to contractually guarantee the security of data placed in the cloud and are unwilling to fully indemnify a company in the event that the cloud provider's system is breached.[152]

Despite the marketing puffery regarding how safe the cloud is, history clearly demonstrates that companies must still take careful steps to safeguard their data. With every increasing cybercrime, it has never been more important for customers to take a hard look at their cloud provider's contractual commitments to protect the customer's valuable data.

95%	64%	71%
Percentage of those enterprises that used a cloud service in 2016.[153]	Percentage of eCommerce sites that relied on cloud computing in 2014.[154]	Percentage of companies that view data security as a concern in moving services to the cloud.[155]

To minimize data security risks companies should evaluate the following as they consider cloud service providers:

1. Does data need to be stored in a specific jurisdiction? Some jurisdictions require that data remain within their borders and by utilizing an open cloud environment, where data is transferred freely across borders, a company could inadvertently violate prohibitions concerning the cross-border transfer of data.

---

152 *See*, Steve Norton, Dropbox Confronts Cloud Security Skeptics, Wall Street Journal Online, (May 1, 2015), http://blogs.wsj.com/cio/2015/05/01/dropbox-is-not-part-of-security-problem-says-new-security-chief/?KEYWORDS=cloud+computing.

153 RightScale, RightScale 2016 State of the Cloud Report, http://assets.rightscale.com/uploads/pdfs/RightScale-2016-State-of-the-Cloud-Report.pdf.

154 Claranet, Claranet Research Report: Adoption Trends in Cloud Computing 2011-2014, http://cloudindustryforum.org/images/PDF/CL0072-Claranet-Research-Report-Adoption-Trends-in-Cloud-Computing-2011-2014.pdf.

155 *Id.*

2. Does the cloud service provider agreement set forth whether the vendor is dedicating hardware to the customer? Absent express language, the vendor is likely providing shared hardware to the customer.

3. Does the agreement clearly explain who has rights to the data stored using the cloud service? Depending on the underlying service, some agreements grant the vendor limited rights.

4. To what extent is cryptography used? Is each separate record in the cloud encrypted, or does all data use the same encryption key? The value of these approaches vary based on the sensitivity of the data and the processing costs.

5. Who is responsible for backing up data and at what frequency? Is the cloud provider required to keep patches and security updates current? Which party is responsible for putting appropriate firewalls in place?

6. Does the agreement set forth standards for how the customer can export its data from the vendor? A customer may want to switch from one cloud vendor to another or may simply want to proceed in a different technological direction.

7. Are the appropriate licenses in place to execute software in a cloud computing environment? For example, some software is priced based on the type of server on which it will be run. Meanwhile, the execution of the software in a cloud (or networked) environment may trigger additional considerations.

8. Does the agreement give the customer sufficient flexibility to expand or contract the extent to which it uses the cloud services? One of the advantages of cloud computing is the idea that use can be scaled to match a customer's needs.

9. Are the agreement's terms sufficiently defined to avoid ambiguities over what the vendor has contracted to provide the customer? Trending technology terms often must be defined to ensure all parties perceive them the same way.

10. Does the agreement guarantee to maintain any current APIs or features, or does it promise to evolve to provide future functionality? Depending on the circumstances, schedules can be a useful way to ensure certain necessary functionality remains in the service or developed in the future (i.e., provision of advanced AI functionality).

11. Will the network connections between the vendor and the customer provide sufficient resources, and if not, what contractual recourse does the customer have? Although cloud computing is seen as ubiquitous, engineering realities may curb its availability. Customers should consider that risk when contracting and request adequate service level compensation.

12. Does the agreement require that the vendor maintain any customer industry-specific needs or regulations? Depending on the sensitivity of the data, the customer may be required to certify that the cloud vendor adheres to certain data security standards.

13. Does the agreement give the customer the ability to delete data or transfer data stored by the vendor and confidence that such deletion or transfer can be achieved? For some categories of data, customers must ensure that data is completely removed from the servers.

14. Does the agreement clearly set forth how the parties should communicate in the event of a data breach or service outage? Similarly, does the agreement contain adequate representations about the vendor's steps to prevent either event and whether the vendor will indemnify the customer against any damages should either event occur?

15. Does the cloud vendor have adequate liability coverage? Does the agreement contain carve outs to the limitation of liability for a breach of the data security obligations? Although no one wants the agreement to reach that point, it is important to understand the extent to which the cloud provider is willing to absorb a loss that might impact many (or all) of its customers simultaneously.

36. Credit Card Breaches

For most retailers credit cards are the primary form in which payments are made. Accepting credit cards, however, carries significant data security risks and potential legal liability. In addition to the normal repercussions of a data security breach – *e.g.*, reputation damage, the risk of class action litigation, and the risk of a regulatory investigation – if a retailer's credit card system is compromised the retailer may be contractually liable to its payment processor, its merchant bank, and ultimately the payment card brands (*e.g.*, VISA, MasterCard, Discover, and American Express). In many cases that contractual liability will surpass any other financial obligation that may arise from the breach.

26	130 million	21%
The number of separate contractual penalties, fines, adjustments, fees and charges that the credit card brands may assess upon a retailer.[156]	Largest number of credit card numbers impacted by a breach.[157]	Percentage of data breach class actions that involved credit card data.[158]

Factors retailers should consider when preparing to respond to a credit card data breach:

1. Does your payment processing agreement cap or limit your contractual liability in the event of a data breach?

---

156 American Express Merchant Regulations (April 2014); Discover Merchant Operating Regulations (April 2014); MasterCard Security Rules and Procedures (Feb. 2015); Visa Service Rules (April 2015).

157 Investopedia, "Equifax Hack: 5 Biggest Credit Card Data Breaches (Sept. 8, 2017), https://www.investopedia.com/news/5-biggest-credit-card-data-hacks-history/ (last searched Jan. 14, 2018).

158 Bryan Cave LLP, Bryan Cave 2017 Data Breach Litigation Report, https://d11m3yrngt251b.cloudfront.net/images/content/9/6/v2/96690/Bryan-Cave-Data-Breach-Litigation-Report-2017-edition.pdf (last viewed Jan. 14, 2018).

2. Does your payment processing agreement cap or limit your processor's liability in the event that they suffer a data breach?

3. Do you have a contractual obligation to notify your payment processor or merchant bank in the event of a possible security breach?

4. Have the vendors of your point of sale equipment provided you with indemnification in the event of a breach caused by their equipment?

5. Is a reporting structure, and contact information, included in your incident response plan?

6. Are there any deficiencies identified in your organization's latest "Report on Compliance."

7. If you have cyber-insurance are there any exclusions that would impact its coverage for credit card related breach costs?

8. If you have cyber-insurance is there a sub-limit for Payment Card Industry ("PCI") related liabilities?

9. Do you have a contractual relationship in place with a forensic investigator that is certified by the Payment Card Industry (a "PFI")?

10. Do you have a contractual relationship in place with a forensic investigator that is independent of the Payment Card Industry?

37. Credit Cards and the Payment Card Industry Data Security Standard

For most retailers their primary source of revenue comes from credit card transactions. In order to accept credit cards, a retailer must enter into a contractual agreement with a payment processor and a merchant bank. As discussed above, those agreements typically required that the retailer represent and warrant its compliance with the Payment Card Industry Data Security Standard ("PCI DSS"). Alternatively, they require a representation and warranty that the retailer complies with the rules of the payment card brands (*i.e.,* American Express, Discover, MasterCard, and Visa), and some of the payment brand rules could be interpreted as requiring that a retailer be compliant with the PCI DSS.

The PCI DSS is a standard that originally was established by the payment brands, and later transferred to the Payment Card Industry Security Standards Council ("PCI SSC") for management and further development. The standard sets forth what the payment brands contend is a baseline of technical and operational requirements designed to protect cardholder data. Put differently, many consider the PCI DSS as the minimum requirements that a company must meet in order to accept and process credit cards.

The current version of the PCI DSS was published in April of 2016 and represents the sixth incarnation of the standard.

240+	12 Months
Number of security controls required under the current version of the PCI DSS.[159]	The frequency with which large retailers must audit and certify their compliance with the PCI DSS.[160]

Factors retailers should consider when evaluating their compliance with the 12 requirements of PCI DSS:

1. Are there any concerns about the *scope* of your organization's latest "Report on Compliance" or "Attestation of Compliance?"

2. Are there any deficiencies identified in your organization's latest "Report on Compliance" or "Attestation of Compliance and are you remediating those issues?

3. If PCI non-compliance was identified, did it trigger contractual notification or remediation requirements?

4. If you retained a third party to evaluate your PCI compliance, are you confident in the proficiency of that company and its analysis?

5. Are your vendors contractually required to meet PCI standards?

6. Do your device vendors and manufacturers meet requirements, such as PIN Transaction Security (PTS) standards?

7. Is your Payment Application PA-DSS validated?

8. Are you using a Point to Point Encryption ("P2PE") solution?

9. If so, does your Point-to-Point Encryption solution meet the PCI P2PE standard?

10. Have the vendors that access, transmit or store your credit or debit card data provided you with appropriate indemnification in the event of a breach caused by their equipment?

38. Credit Monitoring Services

Organizations are not generally required to offer services to consumers whose information was involved in a breach.[161] Nonetheless, many organizations choose to offer credit reports (*i.e.,* a list of the open credit accounts associated with a consumer), credit monitoring (*i.e.,* notification when new credit accounts are opened), identity restoration services (*i.e.,*

[159] Payment Card Industry, Data Security Standard v 3.2, https://www.pcisecuritystandards.org/security_standards/documents.php ("PCI DSS 3.2").

[160] *See, e.g.,* American Express Merchant Operating Guide (Oct. 2016).

[161] Connecticut is the first state to require a company to offer an affected individual credit monitoring if the affected individual's name and Social Security Number are involved in a breach.

helping a consumer restore their credit or close fraudulently opened accounts), and/or identity theft insurance (*i.e.,* defending a consumer if a creditor attempts to collect upon a fraudulently opened account and reimbursing a consumer for any lost funds). If you do offer one of these services a 2014 California statute and a 2015 Connecticut law prohibit charging consumers for them.

Although many consumers believe that credit-related services should be offered following a breach, many (if not most) data breaches do not involve information that could be used to open a credit account. As a result, credit-related services often do not protect consumers from any harm that might result from the breach that triggered the offering. In addition, some courts have viewed offers of credit-related services that an organization makes as a gesture of goodwill as an acknowledgement (at least at the pleading stage in litigation) that consumers' credit is, in fact, at risk.[162] While that fallacy can be ultimately rectified in litigation, it may prevent a company from obtaining early exit through a motion to dismiss and instead force them to develop a record in order to file an early motion for summary judgment.

58%	25%	6x	4
Percentage of consumers that believe an organization should provide credit monitoring following a breach.[163]	Percentage of companies that offer some form of identity theft related service in their breach notification letters.[164]	The odds of being sued are 6 times lower when an organization offers free credit monitoring.[165]	The number of credit monitoring services that have been investigated by the FTC for unfair or deceptive practices.
\$0.25 - \$2.00 Approximate cost of one year of credit-related services per consumer depending upon the number of impacted individuals, the type of information breached, and the services offered.			

What to think about when evaluating identity theft related service providers:

1. What specific services will you be offering to consumers? Do those services "match" the type of data loss that occurred? If not, might it cause consumer confusion?

2. Will the service provider attempt to charge consumers to upgrade the offering (*i.e.,* upsell)? If so, will recipients of the free service perceive that it is not, in fact, free?

3. Will the service provider allow other companies to cross-market products to enrollees? If so, will recipients of the service perceive that their privacy has been violated?

---

162 *See*, Remijas v. Neiman Marcus Group, LLC, No. 14-3122 (7th Cir. July 20, 2015).

163 Ponemon Institute, The Aftermath of a Mega Data Breach: Consumer Sentiment, (April 2014), http://www.ponemon.org/local/upload/file/Consumer%20Study%20on%20Aftermath%20of%20a%20Breach%20FINAL%202.pdf.

164 *Id.*

165 Romanosky, et al, Empirical Analysis of Data Breach Litigation, 11(1) Journal of Empirical Legal Studies June 1, 2012), http://www.econinfosec.org/archive/weis2012/papers/Romanosky_WEIS2012.pdf.

4. Is the service provider permitted to retain information about enrollees after they stop providing service?

5. Has the service provider given adequate assurance (and indemnifications) if the information that you provide to them (e.g., customer lists, lists of impacted consumers, or lists of impacted employees) itself becomes breached?

6. Are you indemnified if the service provider's products are alleged to be unfair or deceptive?

7. Are you indemnified if the service provider is negligent in providing monitoring services?

8. Have you been given a copy of all materials, including marketing materials, enrollment terms, insurance contracts, etc., that relate to the service being offered so that you know what your customers/employees are being provided?

9. What service level guarantees are provided for how quickly enrollees will be able to reach the credit monitoring company?

10. Has the service provider received any complaints, either from regulators or consumers, about its product offering or service?

39. Cyber-Extortion

Extortion refers to situations where a third party demands that an organization pay money (or take some other action) or suffer an adverse consequences. Modern day extortion often takes the form of "cyber-extortion" – where the threat and adverse consequence involves the disclosure of an organization's information or an attack on an organization's electronic infrastructure.

There are many different examples of cyber-extortion in practice, but some of the most common include infecting an organization's computer systems with malware that requires payment to unlock or remove (*i.e.,* ransomware), exploiting a security vulnerability identified by the extorter, threatening to disclose an organization's security vulnerabilities to the press or to other hackers, or even threatening to disclose an organization's security vulnerabilities to government regulators.

The following provides a snapshot of information concerning cyber-extortion as well as a checklist for organizations that are confronted by an extortion demand:

17,146	85%
The number of cyber-extortion reports that the FBI received in a recent year.[166]	Estimate of the percentage of cyber-extortion cases that are not reported.[167]

[166] FBI, 2016 Internet Crime Report *available at* https://pdf.ic3.gov/2016_IC3Report.pdf.

[167] NYA International, Cyber Extortion Risk Report (Oct. 2015) at 3.

$2,500 to $800,000
Range of unsolicited demands related to alleged security vulnerabilities made to Bryan Cave clients.

What to think about when considering a cyber extortion demand:

1. How confident are you that a threat has been made against the organization? Is it possible that the situation involves a white hat or grey hat hacker who does not intend to threaten the organization?

2. Is the threat credible?

3. If the exploitation of a security vulnerability is threatened, can the organization identify the vulnerability without the aid of the extortionist?

4. If the disclosure of non-public information is threatened, is there any evidence that the information has not already been disclosed or shared with others?

5. If the cyber-extortion was conducted in conjunction with the theft of personal information, does your organization have to report the event under data breach notification statutes regardless of whether the extortion demand is paid?

6. Does your organization have systems in place to mitigate any impact of the extortionist carrying through with their threat? For example, if the threat involves the destruction of data (*e.g.,* ransomware) does your organization have a disaster recovery system from which impacted data can be restored?

7. If an extortion demand is paid what is the likelihood that your organization will receive similar demands in the near future?

8. If your organization were to pay the demand is it likely that the recipient of the funds may be associated with terrorism or located in a restricted country?

9. Is cyber-extortion covered under your cyber insurance policy?

10. If information concerning the extortion, or your decision to pay (or not pay) were made public are you prepared to respond to inquiries from the public, the media, and regulators?

40. Cyber Insurance

Most organizations know they need insurance to cover risks to the organization's property like fire or theft, or their risk of liability if someone is injured in the workplace. But, a substantial portion of organizations don't carry coverage for data breaches despite numerous high profile breaches. While many insurance companies offer cyber insurance, not all policies are created equal.

24%	64%	43%
Percentage of companies that had cyber-insurance.[168]	Percentage of companies that believed their exposure to cyber risk would increase in the next 24 months.[169]	Percentage of companies that did not plan to purchase cyber insurance in the next 24 months.[170]

Why is buying cyber insurance difficult?

1. There is little standardization among competing policies; as a result it is hard to comparison shop.

2. Policies' exclusions often swallow coverage; as a result, assessing the value of a policy is difficult unless you have extensive experience with the types of liabilities that arise following data breaches.

3. Policies often cover security but not privacy risks.

Items to review when shopping for cyber insurance:

1. Do the sub-limits on coverage match the corresponding risks?

2. Does the policy include sub-retentions (sub-deductibles) that are unlikely to be reached?

3. Does exclusion prevent payment for the largest risks, *e.g.*, charges that arise following a credit card breach, common theories alleged in class actions, etc.?

4. Is voluntary notification of affected consumers covered?

5. Will credit monitoring for affected consumers be covered?

6. Who does the insurer have on panel for legal representation, forensic investigations, and/or crisis management?

41. Cybersecurity Disclosures

In October of 2011, the U.S. Securities and Exchange Commission ("SEC") issued guidance regarding a public company's obligations to disclose cybersecurity risks and cyber incidents (the "Cybersecurity Disclosure Guidance").[171] The Cybersecurity Disclosure Guidance applies to all SEC registrants and relates to disclosures under the Securities Act of 1933 and the Securities Exchange Act of 1934.

---

168 Ponemon Institute, 2017 Global Cyber Risk Transfer Comparison Report (Apr. 2017), http://www.aon.com/attachments/risk-services/cyber/2017-Global-Cyber-Risk-Transfer-Report-Final.pdf.

169 *Id.*

170 *Id.*

171 Securities and Exchange Commission, CF Disclosure Guidance Topic No. 2: Cybersecurity, Oct. 13, 2011, www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

The SEC staff acknowledged in the Cybersecurity Disclosure Guidance that no existing disclosure requirement explicitly refers to cybersecurity risks and cyber incidents, but has made clear that there are a number of disclosure requirements that might impose an obligation on an issuer to disclose such risks and incidents. The Cybersecurity Disclosure Guidance specifically discusses disclosures required when discussing a company's risk factors, Management Discussion & Analysis, business descriptions, legal proceedings, financial statements and disclosure controls and procedures. The staff stated that as with other operational and financial matters, issuers "should review, on an ongoing basis, the adequacy of their disclosures relating to cybersecurity risks and cyber incidents," with a view to ensuring timely, comprehensive and accurate information that a reasonable investor would consider material. The staff also made clear that if a cyber incident occurs, such as a data breach, registrants should be certain to disclose any material impact of the incident on their business operations and explain how they have taken steps to mitigate damage.

Since the original publication of the Cybersecurity Disclosure Guidance, the SEC has remained focused on the implications of cybersecurity on public companies and regulated financial service firms. In 2014 the SEC's Office of Compliance Inspections and Examinations issued a national exam program alert providing a framework for assessing cyber risk and announcing a plan to examine a sampling of registered broker-dealers and investment advisors to review their cybersecurity preparedness. All public companies should evaluate their current disclosures to ensure that they are consistent with the Cybersecurity Disclosure Guidance and should consider implementing a readiness plan to ensure appropriate and timely disclosures in the event of a cyber incident.

85%	46%	79%
The percentage of Fortune 500 companies that identified cybersecurity risk in a SEC filing in 2012 (the year after the SEC issued the Cyber Disclosure Guide).[172]	The percentage of Fortune 500 companies in 2012 that described the extent of cybersecurity risk as "critical," "significant," "materially harmful," or "seriously harmful" to their business operations.[173]	The percentage of boards of directors that reported they were more involved in cybersecurity then they were 12 months ago.[174]

What every public company should consider concerning cybersecurity disclosures:

1. Evaluate the company's procedures for assessing the materiality of cybersecurity matters and implement a regular schedule of ongoing review, perhaps in connection with the company's regular quarterly reporting processes.

2. Determine what disclosure should be made in the company's SEC filings based on the company's exposure to a cybersecurity incident and the materiality of actions being taken proactively by the company to mitigate risk.

---

172 Willis, Fortune 500 Cyber Disclosure Report, 2013, http://www.willis.com/documents/publications/Services/Executive_Risks/2013/FinexNA_Cyber_Update_v2.pdf.

173 *Id.*

174 2017 BDO Cyber Governance Survey (Sept. 2017) https://www.bdo.com/insights/assurance/corporate-governance/2017-bdo-board-survey/2017-bdo-cyber-governance-survey (last viewed Jan. 14, 2018).

3. Review the company's current disclosures and compare those disclosures to peer companies with similar cybersecurity risks and issues.

4. Consider establishing a disclosure readiness plan in the event of a cyber incident. Review the implications for such a plan of active shelf registration statements, share buyback programs and other ongoing securities market activities.

5. Ensure involvement by the board of directors or the risk management committee of the board in the cybersecurity risk assessment and disclosure planning.

42. Data Breach Notification Laws

Although Congress has attempted to agree on federal data breach notification legislation, there is no national data breach notification law that applies to most companies. Instead, 48 states, plus the District of Columbia, Puerto Rico, Guam, and the Virgin Islands, have each enacted their own statutes addressing an organization's notification obligations in the wake of a data breach involving personal information. The only states without such laws are Alabama and South Dakota, although their citizens may be covered in some situations by the data breach laws of other states.

While state data breach laws are similar, they are not uniform. The following summarizes some of the key provisions of state data breach notification laws and highlights areas in which state laws diverge. In the event of a breach involving records of consumers who live in multiple states, the laws of each of those states should be reviewed to ensure that the organization is complying with all notification requirements.

52 Number of states and territories with a breach notification law.	2 Number of states that do not have a breach notification law.
54% Percentage of state laws that require notifying regulators after some breaches.	19% Percentage of state laws that expressly confer a private right of action to consumers if the statutes is violated.

What to consider when evaluating state data breach laws:

1. In which jurisdiction do the data subjects reside? Do the laws of those jurisdictions purport to be extraterritorial?

2. Is your organization exempt from the applicable state data breach laws?

3. What types of personal information are covered by the applicable statutes?

4. Do the applicable statutes only require notification if the breach is "material?" If so, what language does the statute use to determine whether a breach is material?

5. If notification to consumers is required, how much time does the statute give you to provide notice?

6. Do the applicable statutes require that you notify state regulators?

7. Do the applicable statutes require that notification letters contain specific types of information?

8. Do the applicable statutes prohibit you from including some types of information in a notification letter?

9. What form should the notification take? A letter? An email? A telephone call?

10. Do the applicable statutes require your organization to notify any third parties?

43. De-Identification, Anonymization, and Pseudonymization

De-identification of data refers to the process used to prevent personal identifiers from being connected with information. The FTC indicated in its 2012 report *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* that the FTC's privacy framework only applies to data that is "reasonably linkable" to a consumer.[175] The report explains that "data is not 'reasonably linkable' to the extent that a company: (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data."[176] With respect to the first prong of the test, the FTC clarified that this "means that a company must achieve a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device."[177] Thus, the FTC recognizes that while it may not be possible to remove the disclosure risk completely, de-identification is considered successful when there is a reasonable basis to believe that the remaining information in a particular record cannot be used to identify an individual. The FCC has adopted in its Broadband Privacy Order the FTC's three-part de-identification test.[178]

De-identification is not a single technique, but rather a collection of approaches, tools, and algorithms that can be applied to different kinds of data with differing levels of effectiveness. In 2010, the National Institute of Standards and Technology (NIST) published the *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* that provides a set of instructions and de-identification techniques for federal agencies, which can also be used by non-governmental organizations on a voluntary basis. The guide defines "de-identified information" as "records that have had enough PII removed or obscured, also referred to as masked or obfuscated, such that the remaining information does not identify an individual and

---

[175] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, (March 2012), available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[176] *Id*. at iv.

[177] *Id*. at 21.

[178] *Protecting the Privacy of Customers of Broadband and other Telecommunications Services*, Notice of Proposed Rulemaking, WC Docket No. 16-106, 30 FCC Rcd ___ (2016), para. 106, *available at* http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1103/FCC-16-148A1.pdf.

there is no reasonable basis to believe that the information can be used to identify an individual."[179]

18	<.25%	10% to 60%	4
The number of specific types of data that must be removed from a health record to qualify under the HIPAA "Safe Harbor" De-Identification Method.[180]	The re-identification risk found by two studies of health records that had been de-identified using field suppression methods.[181]/[182]	The re-identification risk range in a limited dataset (a dataset that has been partially de-identified, but that still includes dates, city, state, zip code, and age). [183]	The number of randomly chosen observations of an individual that could be used to uniquely identify 95% of "mobility traces" (a record of locations and times that a person or vehicle visited over a year).[184]
Key Definition: "**Anonymization"** of data refers to a subcategory of de-identification whereby data can never be re-identified. This differs from de-identified data, which is data that may be linked to individuals using a code, algorithm, or pseudonym.			
Key Definition: "**Pseudonymization**" of data refers to a procedure by which personal identifiers in a set of information are replaced with artificial identifiers, or pseudonyms.			
Key Definition: "**Aggregation**" of data refers to the process by which information is compiled and expressed in summary form.			

NIST has identified the following five techniques that can be used to de-identify records of information:

1. Suppression: The personal identifiers can be suppressed, removed, or replaced with completely random values.

2. Averaging: The personal identifiers of a selected field of data can be replaced with the average value for the entire group of data.

3. Generalization: The personal identifiers can be reported as being within a given range or as a member of a set (i.e., names can be replaced with "PERSON NAME").

---

179 National Institute of Standards and Technology, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), (April 2010), available at http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf.

180 45 C.F.R. 164.514.

181 Peter K. Kwok and Deborah Lafky, "Harder Than You Think: A Case Study of Re-identification Risk of HIPAA Compliant Records," Joint Statistical Meeting, August 2, 2011.

182 Kathleen Benitez and Bradley Malin, "Evaluating re-identification risks with respect to the HIPAA privacy rule," J. Am Med Inform Assoc. 2010; 17:169-177.

183 *Id.*

184 Yves-Alexandre de Montjoye et al., "Unique in the Crowd: The privacy bounds of human mobility," Scientific Reports 3 (2013), Article 1376.

4. Perturbation: The personal identifiers can be exchanged with other information within a defined level of variation (i.e., DOB may be randomly adjusted -5 or +5 years).

5. Swapping: The personal identifiers can be replaced between records (i.e., swapping the ZIP codes of two unrelated records).

The European Union has identified the following additional de-identification techniques:[185]

1. Noise Addition: The personal identifiers are expressed imprecisely (i.e., weight is expressed inaccurately +/- 10 lb).

2. Differential Privacy: The personal identifiers of one data set are compared against an anonymized data set held by a third party with instructions of the noise function and acceptable amount of data leakage.

3. L-Diversity: The personal identifiers are first generalized, then each attributed within an equivalence class is made to occur at least "*l*" times. (i.e., properties are assigned to personal identifiers, and each property is made to occur with a dataset, or partition, a minimum number of times).

4. Pseudonymization – Hash Functions: The personal identifiers of any size are replaced with artificial codes of a fixed size (i.e., Paris is replaced with "01," London is replaced with "02," and Rome is replaced with "03").

5. Pseudonymization – Tokenization: The personal identifiers are replaced with a non-sensitive identifier that traces back to the original data, but are not mathematically derived from the original data (i.e., a credit card number is exchanged in a token vault with a randomly generated token "958392038").

44. Document Retention Periods

Data minimization can be a powerful – and seemingly simple – data security measure. The term refers to retaining the least amount of personal information necessary in order for an organization to function. Less information means that there is less that the organization needs to protect, and less opportunity for information to be lost or stolen.

In practice data minimization requires organizations to fully understand where they collect information, why they collect information, and where it is stored. It also requires difficult decisions regarding what information the organization will likely need in the future from a business perspective, and what impact having limited consumer or employee records may have on potential legal disputes if they arise. For example, an organization that chooses to implement a 30 day or 60 day automatic "roll off" policy for employee email may not be able to identify email exchanges between an employee and a vendor that relate to a contract dispute that arises months later.

[185] Article 29 Working Party, Opinion 05/2014 on Anonymization Techniques, WP216, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

> 8,000 emails	6.5 million
Average size of employee inbox.[186]	Number of pages of Word data files that could be on a 100GB hard drive.[187]

"The indiscriminate collection of data violates the First Commandment of data hygiene: Thou shall not collect and hold onto personal information unnecessary to an identified purpose. Keeping data on the off-chance that it might prove useful is not consistent with privacy best practices."

- FTC Chairwoman Edith Ramirez[188]

What to think about when designing a retention policy:

1. Do you systematically track all of the data fields that your organization collects from consumers and employees?

2. Do you systematically apply retention periods to each data field that you collect?

3. Do those retention periods reflect the current business needs, or estimates as to possible future business needs?

4. For a particular data field, what time period is typical in your industry and for the type of data at issue?

5. What data and documents are you legally required to retain, and for how long must they be retained?

6. If you decide to retain data and documents for longer than you are required to do so how does it increase, or decrease, your legal risk?

7. What steps are taken to irrevocably destroy data that is no longer needed?

8. Are there any contractual requirements that require you to keep data for a certain duration?

9. Does the retention policy include an annual review process?

10. Who is responsible for enforcing the retention policy, reviewing it, and auditing it?

45. Encryption

Encryption refers to the process of converting data into a form that is unreadable unless the recipient has a pre-designated algorithm, a "key," and a password to convert the information

[186] Dave Troy, The Truth About Email: What's A Normal Inbox? (April 5, 2013) https://pando.com/2013/04/05/the-truth-about-email-whats-a-normal-inbox/.

[187] *See*, netdocuments, File Sizes and Types, https://support.netdocuments.com/hc/en-us/articles/205219000-File-Sizes-and-Types.

[188] Edith Ramirez, The Privacy Challenges of Big Data: A View From the Lifeguard's Chair, Keynote Address Technology Policy Institute Aspen Forum, (August 19, 2013), https://www.ftc.gov/public-statements/2013/08/privacy-challenges-big-data-view-lifeguard%E2%80%99s-chair.

into readable text. Most statutes, regulations, and agencies that require that companies utilize encryption to protect data do not mandate that a specific encryption standard (*i.e.,* algorithm) be used. Some statutes do require, however, that companies use an encryption key that is at least 128-bits in length.

When examining whether a company's use of encryption is reasonable and appropriate for the type of data collected and the risks posed to that data, regulators often examine whether a company utilizes encryption "at rest" and/or "in transit." Encryption "at rest" refers to encryption applied to data while it is being stored. Encryption "in transit" refers to encryption applied to data while it is being transmitted across a network. Depending upon the type of software being used, and the architecture of a database, encryption at rest may significantly impair the ability of the data to be accessed and used efficiently. Regulators also look to whether the encryption standardize utilized either at rest or in transit has been publicly compromised or known vulnerabilities.

6 Number of states that require that sensitive information be encrypted when sent across public networks.[189]	1 Number of states which explicitly require that sensitive information be encrypted when sent wirelessly.[190]	1 Number of states which explicitly require that sensitive information be encrypted when stored on laptops or on portable devices.[191]
52 Data breach notification statutes that contain a safe harbor for encrypted data.[192]		
87% The number of locked devices in 2016 that the FBI claimed it could access despite widespread encryption technology.[193]		
$900,000 Amount the FBI paid a private security firm to identify a vulnerability in the iPhone5c that would allow the Bureau to crack phone's encryption.[194]		

What to think about when designing, or reviewing, an encryption policy:

1. What types of data does our organization encrypt?

2. Is the data encrypted at rest?

3. Is the data encrypted in transit?

189 Bryan Cave Survey of State Safeguard Statutes (2015).

190 *Id.*

191 *Id.*

192 *Id*. Applies where the encryption key has not been acquired.

193 The FBI's Approach to the Cyber Threat, *remarks delivered by James Comey, Director of the Federal Bureau of Investigation* (August, 30, 2016), available at: https://www.fbi.gov/news/speeches/the-fbis-approach-to-the-cyber-threat.

194 CNBC, Senator Reveals that the FBI Paid $900,000 to Hack into San Bernadino Killer's iPhone (May 8, 2017) *available at* https://www.cnbc.com/2017/05/05/dianne-feinstein-reveals-fbi-paid-900000-to-hack-into-killers-iphone.html.

4. Is the data encrypted when stored on personal storage devices?

5. What encryption standards are used at rest and/or in transit?

6. Are those encryption standards considered "strong" within the security community?

7. Does your state require a specific encryption standard?

8. Is there evidence that the encryption key could have been compromised?

9. Is there a process to review the sufficiency of the encryption standard periodically (*e.g.,* once per year)?

10. Has your organization contractually agreed to maintain a specific encryption standard?

46. Forensic Investigators

Many competent IT departments lack the expertise, hardware, or software to preserve evidence in a forensically sound manner and to thoroughly investigate a security incident. In-house counsel needs to be able to recognize such a deficiency quickly – and before evidence is lost or inadvertently destroyed – and retain external resources to help collect and preserve electronic evidence and investigate the incident.

Although in the midst of an emergency you may feel that you have relatively little leverage to negotiate preferable terms in a service agreement with a forensic investigator, given the sensitivity of the information to which the investigator will have access, it is essential to make sure that your service agreement protects your organization.

$3.86 million	$141,479	$35,175
Highest amount spent on a forensic investigation.[195]	Average amount spent on a forensic investigation.[196]	Median amount spent on a forensic investigation.[197]
$265 - $3.86 million Range of forensic investigation costs.[198]		

What to consider when retaining a forensic investigator:

1. Does the forensic investigator have sufficient expertise to conduct the investigation?

---

[195] Statistics based upon cyber liability insurance claims between 2014 to 2017. Net Diligence, 2017 Cyber Claims Study, p. 8 (2017), https://netdiligence.com/wp-content/uploads/2017/10/2017-NetDiligence-Claims-Study_Public-Edition.pdf.

[196] *Id.*

[197] *Id.*

[198] *Id.*

2. Does the forensic investigator have sufficient capacity to immediately deploy resources to timely investigate the incident?

3. Is there a master service agreement already in place?

4. Does the agreement contain data security provisions that are appropriate for a contractor that is likely to gain access to sensitive personal information?

5. Does the agreement contain data privacy provisions that are appropriate for a contractor that is likely to gain access to sensitive personal information?

6. Is the agreement structured to protect attorney-client privilege?

7. Does the forensic investigator understand what you expect of them to maintain attorney-client privilege?

8. Does the agreement include sufficient protections in the event that the forensic investigator is itself breached?

9. If the organization has cyber-insurance, is the forensic investigator a preferred provider and/or approved by the insurer?

10. Does the forensic investigator represent a business partner that may have an interest in the incident? If so, is there a potential conflict of interest?

47. Healthcare Business Associates

The Health Information Technology for Economic and Clinical Health ("HITECH") Act modified the Health Insurance Portability and Accountability Act ("HIPAA") by expanding the definition of Business Associates ("BA") and their responsibilities and liabilities. A BA is a "person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity."[199] A BA includes:

1. Health Information Organizations

2. E-Prescribing Gateways

3. Persons/entities that for, or on behalf of, a Covered Entity:

   - Create or received PHI
   - Maintain or store PHI even if they do not or can not access the PHI
   - Offer personal health records
   - Provide data transmission services if they routinely access the PHI[200]

Subject to certain exceptions, the HIPAA rules require that covered entities enter into contracts with their BA's to ensure that the BA's will appropriately safeguard PHI.[201] Exceptions

[199] U.S. Dep't of Health & Human Servs., Business Associates, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (November 20, 2017).

[200] 45 C.F.R. § 160.103(3).

to the BA standard includes: (1) disclosures by a covered entity to a health care provider for treatment of the individual; (2) disclosures to a health plan sponsor, provided that the group health plan's documents have been amended to limit the disclosures; and (3) the collection and sharing of PHI by a health plan that is a public benefits program. [202] It is important to determine whether a BA contract is required due to the potential for heavy penalties. In 2016, the U.S. Department of Health and Human Services fined a hospital over $1.5 million when it discovered a six month period during which PHI was transferred to the hospital's BA without an agreement in place.[203]

The Federal Office for Civil Rights ("OCR"), which enforces HIPAA and HITECH, has identified BAs as one of its top enforcement priorities. Under HIPAA and HITECH, BAs are directly liable for compliance and subject to the following monetary penalties:

Violation Category	Each Violation	Maximum Penalty per Identical Provision Violated in Calendar Year
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1000 - $50,000	$1,500,000
Willful Neglect – Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect – Not Corrected	$50,000	$1,500,000

Companies that are considered BAs, or companies that are contracting with a BA, should consider the following checklist when evaluating their compliance with HIPAA and HITECH:

1. Verify that a Business Associate Agreement is in-place with all service providers that handle PHI.
2. Designate a security officer.
3. Perform a Security Risk Assessment.
4. Implement administrative, physical, and technical safeguards to protect PHI.
5. Identify and report breaches of security.
6. Develop policies for HIPAA / HITECH compliance.
7. Impose disciplinary actions where employees or vendors violate HIPAA / HITECH obligations.

---

201 45 C.F.R. § 164.308(b)(1).

202 U.S. Dep't of Health & Human Servs., Business Associates, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html (November 30, 2017).

203 HealthITSecurity, $1.5M HIPAA Settlement Fine for North Memorial Health Care (Mar. 17, 2016), https://healthitsecurity.com/news/1.5m-hipaa-settlement-fine-for-north-memorial-health-care.

8. Maintain HIPAA and HITECH relevant documentation for such periods as required by law.

48. Healthcare Data Breach Enforcements and Fines

The Department of Health and Human Services' ("HHS") Office for Civil Rights ("OCR") is responsible for enforcing the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Enforcement of the Privacy Rule began on April 14, 2003, while enforcement of the Security Rule began on April 20, 2005. Furthermore, covered entities and business associates were required to comply with the HIPAA Breach Notification Rule beginning on September 23, 2009.[204]

The OCR relies on complaints filed by third parties, self-reports of data breaches, and media reports to identify targets for compliance reviews. If a covered entity or business associate is found to have committed serious violations during a compliance review, HHS may require the entity to enter into a "Resolution Agreement" ("RA") that may include a fine and a corrective action plan.

167,321 Number of HIPAA complaints received by OCR since 2003.[205]	857 Number of compliance reviews initiated by OCR since 2003.[206]
52 Number of cases that OCR has settled or imposed a civil money penalty since 2003.[207]	$72 million Total fines collected for HIPAA violations.[208]
$5.55 million Largest fine assessed by OCR to date.[209]	

[204] The HIPAA Breach Notification Rule requires covered entities and their business associates to notify the HHS Secretary, individuals, and in some cases, provide notice in media, regarding breaches of unsecured protected health information.

[205] U.S. Dep't of Health and Human Servs., Enforcement Highlights, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (November 20, 2017) (results as of Oct. 31, 2017).

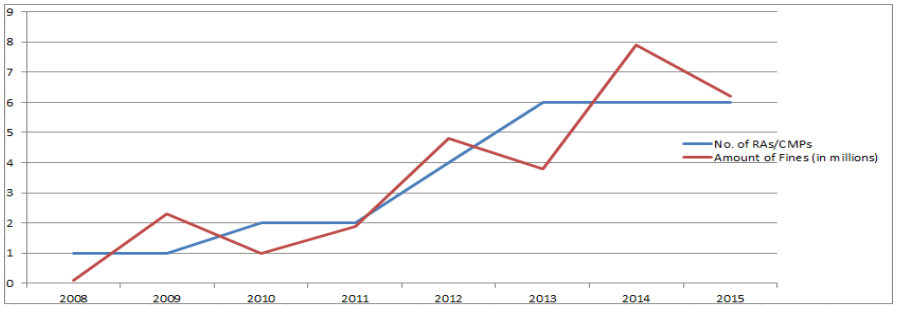
[206] *Id.*

[207] *Id.*

[208] U.S. Dep't of Health and Human Servs., Resolution Agreements, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/enforcement-highlights/index.html (November 20, 2017).

[209] Advocate Health Care Settles Potential HIPAA Penalties for $5.55 Million, http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ahcn/index.html (November 11, 2016).

Trends in Enforcement Activities and Fines[207]



What to consider when assessing the impact of an OCR investigation:

1. While enforcement activities and fines are projecting upward, they appear stable between 2014-2015.

2. Only a minority of investigations lead to fines and penalties.

3. Cooperation in government-initiated compliance reviews is key to reducing the risk of a penalty.

4. Having multiple incidents, even if minor on their own, tends to trigger an investigation and lead to fines and RAs.

5. All entities, regardless of size, are at risk of being found non-compliant and facing large fines in an investigation.

49. Incident Response Plans

The best way to handle any emergency is to be prepared. When it comes to data breaches incident response plans are the first step organizations take to prepare. Furthermore, many organizations are required to maintain one. For example, any organization that accepts payment cards is most likely contractually required to adopt an incident response plan.

The EU's new General Data Protection Regulation ("GDPR"), set to go into effect May 2018, further enhances the importance of incident response plans. The GDPR is a regulation that applies to any business which processes the personal information of EU citizens. While the GDPR does not explicitly require that organizations have an incident response plan, it requires organizations to report data breaches within 72 hours of discovering them. Organizations who do not comply may be subject to heavy fines. Thus, having an incident response plan in place will likely be essential to an organization's ability to comply with the GDPR's notification obligation.

An organization with a fully functional incident response plan can significantly reduce the cost of the data breach by identifying, responding and containing the breach quickly. A good incident response plan does not attempt to predict every type of breach that may occur. Rather the fundamental components of an incident response plan is that it establishes the framework for who within an organization is responsible for investigating a security incident, what resources that person has at their disposal (inside and outside of the organization), and when a situation

should be elevated to others within the organization. They can also provide a reference guide for the type of actions common to most security investigations.

$19 per record The amount per compromised record that having an incident response team reduces the cost of a data breach.[210]	~1 million The amount on average that breach containments that take more than 30 days cost more than those that take less than 30 days to contain.[211]
25% Percentage of companies that have an incident response plan that is applied consistently across the enterprise.[212]	

What are an organization's top concerns when it comes to incident response plans?

1. The plan has little relationship to how the organization actually handles security incidents.

2. The plan has never been tested.

3. The plan does not cover all of the issues that arise in a data security incident.

Checklist for drafting an effective incident response plan:

1. The plan assigns a specific person or group to lead an investigation.

2. The plan provides incident reporting procedures including a clear plan for escalating information about an incident.

3. The plan discusses the need for preserving evidence.

4. The plan incorporates legal where appropriate to preserve attorney-client privilege.

5. The plan discusses how the organization will communicate externally concerning an incident.

6. The plan includes contact information for internal resources.

7. The plan includes contact information for pre-approved external resources.

---

210 Ponemon Institute, 2017 Cost of Data Breach Study (June 2017), https://www.ponemon.org/library/2017-cost-of-data-breachstudy-united-states.

211 *Id.*

212 Ponemon Institute, The Second Annual Study on the Cyber Resilient Organization: Executive Summary 2 (Nov. 2016), http://info.resilientsyst ems.com/ponemon-institute-study-the-2016-cyber-resilient-organization.

8. The plan is reviewed annually.

9. The plan is tested in order to identify weak points and document lessons learned.

50. Passwords

Many consumers, and many employees, have dozens of passwords for access to different systems, services, networks, device, and terminals. From a corporate perspective, many companies have at least two policies that impact passwords – a password selection or management policy, and a security policy that may include how passwords maintained by the company are secured

A password selection or management policy discusses an organization's standards for password assignment, and password strength (*i.e.*, how complex the password that a user selects must be in order to avoid the password from being stolen or guessed). For organizations that maintain lists of passwords, several states have enacted legislation that require the organization to "implement and maintain reasonable security measure to protect" the username and passwords that are in their possession. As a result, whether the organization maintains a system that allows third party users to create password controlled accounts is often a factor that is considered when conducting a data security assessment. One of the primary concerns is that even if the service or database for which the username and password are used may not be sensitive, or house other categories of sensitive information, people often re-use their usernames and passwords for multiple services or systems. As a result, if a bad actor is able to obtain a username and password for an individual that relates to a non-sensitive system maintained by one organization, the bad actor may be able to leverage those credentials to try to access a sensitive system held by a different organization.

9	10%	4%
Number of states that arguably require that an organization protect username and passwords within its possession.[213]	Number of people that use one of the top 25 "worst" passwords (i.e., most easily guessed by hackers)."[214]	Number of people that one study found still use the password "123456."[215]
81%		
Percentage of hacking-related data breaches that leveraged a weak or stolen passwords.[216]		

What to think about when designing or reviewing, a password selection or use policy:

1. The more characters required for a password generally the more difficult it is for an attacker to guess. Consider whether it is practical to require a long password (e.g., twelve or more characters).

[213] Bryan Cave Survey of State Safeguard Statutes (2015).

[214] Http://www.teamsid.com/worst-passwords-2016 (last viewed June 2017).

[215] Http://www.teamsid.com/worst-passwords-2016 (last viewed June 2017).

[216] Verizon, 2017 Data Breach Investigations Report at 3 (10th Ed.).

2. If only alphabetic characters are allowed there are 26 different combinations that an attacker needs to consider for each character of the password. Allowing (or requiring) a larger character set increases the number of possible combinations. As a result consider making passwords case sensitive (i.e., increasing the range of possibilities by an additional 26 characters), and utilize numbers (increasing the range of possibilities by an additional 10 characters) or symbols (further increasing the range of possibilities for each character).

3. Avoid reusing the same password over and over again for different websites or databases. Requiring a unique password configuration from users / employees may help prevent the reuse of passwords permitted by other websites.

4. Two-factor authentication refers to the practice of requiring two separate forms of identification when logging into a system. While one of those forms may be a password, the second form would ideally be unrelated to a knowledge-item of the user. For example, a one-time generated token sent to the users mobile device could serve as the second factor. Consider whether using a two-factor authentication system is practical.

5. If you lose an individual's username and password, it may trigger, in some jurisdictions, a requirement that you notify the individual and/or a state regulator.

51. Negotiating Payment Processing Agreements

Credit cards are the primary form of payment received by most retailers. In order to process a credit card a retailer must enter into an agreement with a bank and a payment processor (a "Payment processing agreement").

Payment processing agreements often have a significant impact on a retailer's financial liability in the event of a data breach. In many cases, the contractual liabilities that flow from a payment processing agreement surpass all other financial liabilities that arise from a data breach including the cost to investigate an incident, defend litigation, and defend a regulatory investigation.

3,199	$67 million	25,000
The number of companies that offer payment processing services in the United States.[217]	The amount of Target's contractual liabilities to its payment processor in connection with just one of the four major payment brands.[218]	The word count of a typical payment processing agreement.

The following checklist describes common data security related provisions to look for within most payment processing agreements:

[217] Visa, Global Registry of Service Providers, http:www.visa.com/splisting/searchGrsp.do (search conducted of "United States" region of operation). Search was last conducted January 14, 2018.

[218] Robin Sidel, Target to Settle Claims Over Data Breach: Retailer to pay Visa issuers up to $67 million, Wall Street Journal, (August 18, 2015), http://www.wsj.com/articles/target-reaches-settlement-with-visa-over-2013-data-breach-1439912013.

1. Incorporation of Payment Brand Rules. Most payment processing agreements incorporate by reference the rules, regulations, and guidelines of the payment brands (*e.g.,* American Express, Discovery, MasterCard, and/or Visa). When negotiating a payment processing agreement it is important to determine whether the obligation to abide by the payment brand rules is unilateral (*i.e.,* is imposed only upon the merchant) or reciprocal (*i.e.*, is imposed upon the merchant, the acquiring bank, and the payment processor).

2. Incorporation of the Payment Card Industry Data Security Standard. Many payment processing agreements reference the PCI DSS and require that a merchant be, and remain, in full compliance with the requirements of the PCI DSS. When negotiating a payment processing agreement it is important to determine whether you are, or are not, currently in compliance with the PCI DSS, and whether the obligation to comply with the PCI DSS is unilateral or reciprocal. Put differently, does the agreement require just the merchant to comply with the PCI DSS or does it require all parties to comply with applicable portions of the standard? Note that even if a payment processing agreement does not expressly incorporate the PCI DSS, if the payment processing agreement incorporates the Payment Brand Rules, the Payment Brand Rules may themselves incorporate the PCI DSS by reference.

3. Incorporation of Other Rules, Guidelines, or Procedures. Some merchant banks and payment processors maintain their own procedures, protocols, or "operating guidelines," and attempt to incorporate those documents by reference into a payment processing agreement. If you are negotiating an agreement that incorporates bank or processor specific rules, be sure to ask for a copy of those documents. Note that many banks do not make such documents public (*e.g.,* they are not available online); a contracting party must specifically ask for a copy or request access to a password restricted repository.

4. Indemnification. Most merchant banks and payment processors attempt to require that a merchant indemnify them for any fine, penalty, assessment, or other contractual liability, imposed by the payment brands upon the merchant bank or the payment processor as a result of a data security incident that occurs at the merchant. In many situations these "assessments" form the greatest financial liability imposed upon the merchant after a data breach.

5. Assignment of Rights. If a merchant is required to indemnify a merchant bank and/or payment processor for fines, penalties, assessments, or other contractual liabilities imposed by the payment brands, the merchant has a strong interest in being able to appeal, or contest, those liabilities before they are incurred. Some merchant banks and payment processors have assigned, or subrogated, their rights vis-à-vis the payment brands to the merchants. Doing so ensures that the merchant is able to "stand in the shoes" of the bank and the payment processor to ensure that the assessments that are issued (and which the merchant must pay under an indemnification obligations) are reasonable and appropriate.

6. Applicable Law: Payment processing agreements typically contain a broad mandate that the merchant comply with applicable laws and regulations. Often such agreements will specifically reference data privacy and security laws. As

with other sections in the agreement, it is important to note whether obligations to comply with privacy and security laws are unilateral or reciprocal.

7. Subcontractors: Does the payment processing agreement attempt to hold the merchant responsible for the acts and omissions of its third party service providers? Some payment processing agreements also require that a merchant disclose its use of third party subcontractors that accesses/stores/transmits PCI data to its bank and/or payment processor.

8. Data Security Incidents: Payment processing agreements typically require that a merchant notify a bank or a payment processor of a data breach. Consider whether the agreement contains a time period that may be difficult to comply with (*e.g.,* immediate notification) or one that may be commercially practical *(e.g.,* notification within 72 hours of discovery of an incident)? As with other provisions in the payment processing agreement, is the breach notification obligation unilateral or reciprocal?

9. Reserve: Many payment processing agreements permit a merchant bank or payment processor to establish a reserve in the event of a data security incident. Often a bank or a payment processor will attempt to negotiate a provision which permits them to fund the reserve using the proceeds from any credit card transaction. If a reserve provision is proposed consider whether there are sufficient terms to protect the merchant such as:

    - A cap on the total reserve amount.
    - A daily cap on the percentage of sales Vendor may withhold when establishing a reserve.
    - Is the reserve amount tied to a calculation based on objective risk criteria.
    - Is there a termination of the reserve and payment of funds.
    - Is the reserve comingled with other merchant's funds.

10. Vendor Liability: Reciprocity is a constant theme when evaluating a payment processing agreement. In the context of liability, consider whether your payment processing agreement holds your bank and payment processor liable for breaches that occur within their systems, whether they are required to indemnify you for damages that would relate to such a breach, and whether any cap that applies to their damages is similar to any cap that applies to the merchant's damages.

52. Ransomware

Some forms of cyber extortion are automated and not targeted at any specific victim. For example, "ransomware" refers to a type of malware that prevents users from accessing their systems unless, and until, a ransom is paid. Although variants of ransomware operate differently many encrypt the contents of a victim's hard drive using asymmetric encryption in which the decryption key is stored on the attacker's server and is available only after payment of the ransom. Victims typically discover the ransomware when they receive an on-screen message instructing them to transfer funds using an electronic currency, such as bitcoin, in order to receive the decryption key and access to their files. "CryptoLocker" is the most famous ransomware family and first appeared in 2013.

The real cost of ransomware is downtime and lost productivity due to lack of access to systems for customers and employees. Damage to brand or reputation that occurs as a result of the downtime can also be substantial.

In November 2016, the FTC issued guidance for businesses on how to avoid and respond to ransomware attacks in its *How to defend against ransomware*[219] and *Ransomware – A closer look*.[220]

The following provides a snapshot of information concerning ransomware:

2,673	$1,077	1 in 5	Every 40 seconds
The number of entities that reported being victimized by ransomware in 2016.[221]	The average ransom amount associated with ransomware.[222]	Businesses that paid the ransom never got their data back.[223]	A company is hit with ransomware.[224]
$5,000 - $20,000			
Typical range per day of lost business and damages due to ransomware downtime.[225]			

What to think about if your organization is impacted by ransomware:

1. Is the ransomware designed to export data before encrypting it?

2. If so did the impacted data contain any personally identifiable information that might implicate a data breach notification statute?

3. Is it possible for your organization to recover the impacted files using backup systems?

4. Is the variant of ransomware involved associated with a known criminal enterprise?

5. Should your organization contact law enforcement?

6. Should your organization make the attack publicly known?

7. If your organization were to pay the ransom demand, is it likely that the recipient of the funds may be associated with terrorism or located in a restricted country?

---

219 FTC, How to defend against ransomware (November 10, 2015), https://www.consumer.ftc.gov/blog/how-defend-against-ransomware?utm_source=govdelivery.

220 FTC, Ransomware – A closer look, (November 10, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2016/11/ransomware-closer-look?utm_source=govdelivery.

221 FBI, 2016 Internet Crime Report, at 10, IC3.gov (last viewed Nov. 11, 2017).

222 Symantec, 2017 Internet Security Threat Report (Apr. 2017), at 59.

223 Kaspersky Security Network, Security Bulletin 2016, https://securelist.com/kaspersky-security-bulletin-2016-story of-the-year/76757/ (last viewed Nov. 14, 2017).

224 *Id.*

225 Imperva, Ransomware Rising: Thoughts from 170 Cyber Security Pros (Feb. 13, 2017).

8. Is cyber-extortion and/or ransomware covered under your cyber insurance policy?

9. What systems within your organization are at the greatest risk of a ransomware attack, and are they protected?

10. Have you prepared sufficient backups of critical systems and data?

53. Reputation Management

The reputational injury following a data breach can be severe. Indeed, reputational injury – including lost customers – often surpasses legal liability.

Effective management of the reputational impact of a data security incident requires a proactive and reactive strategy. The proactive strategy assumes that the organization will control when, and what, information will be conveyed to the public, media, and impacted consumers. For many organizations the proactive strategy that they choose is to wait until their investigation of an incident is complete so that they can provide the public with the most accurate and meaningful information.

The reactive strategy anticipates that the public may be alerted to a possible security incident at a time when the organization may not have full or complete information. The reactive strategy must carefully balance responding to requests from the public for details that may not be known to the organization. While the pressure to provide information can be significant, providing inaccurate, incomplete, or preliminary information can confuse consumers, increase the likelihood of legal liability, and, in the long run, lead to worse reputational injury. Due to the complexities involved, many companies retain third party communications, public relations, or reputational consultants to help manage reputational impact.

75%	65%	31%
Percentage of people that reported that they "trusted" family owned businesses.[226]	Percentage of consumers in one study which reported that they lost trust in an organization that experienced a data breach.[227]	Percentage of consumers in one study that discontinued a relationship with an organization that experienced a data breach. [228]
$149 - $2,000,000 Range of money spent on public relations and other crisis services costs following a data breach.[229]		

[226] 2017 Edelman Trust Barometer, Special Report: Family Business, https://www.edelman.com/trust2017/family-business-trust/

[227] Ponemon Institute & Centrify, The Impact of Data Breaches on Reputation & Share Value, 12 (May 2017), https://www.centrify.com/media/4737054/ponemon_data_breach_impact_study.pdf.

[228] *Id.*

[229] Net Diligence, 2017 Cyber Claims Study, 8 (2017), https://netdiligence.com/wp-content/uploads/2017/10/2017-NetDiligence-Claims-Study_Public-Edition.pdf.

What to think about when retaining a consultant to help manage the reputational impact of a security incident:

1. Has the consultant dealt with data breaches in the past? If so, was the strategy advocated by the consultant effective in controlling the reputational impact and quantity of media exposure?

2. Has the consultant dealt with data breaches in the industry in which you operate?

3. What was the most publicized breach that they handled? (Remember that high publicity does not necessarily signify an effective reputation-management strategy).

4. What other breach-related services do they provide? If reputation-management is not the main focus of the consultant, is their practice sufficiently specialized in that area?

5. What is the consultant's general approach to responding to media inquiries about a security incident when a forensic investigation is not complete?

54. Security Due Diligence In A Merger Or Acquisition

When a company is acquired, the buyer ultimately becomes responsible for the data security practices of the company that it acquired. This is true with regard to litigation risks, reputational risks, and regulatory risks. For example, the FTC can hold an acquiring company responsible for the bad data security practices of a company that it acquires. Evaluating a potential target's data security practices, however, can be daunting and complicated by the fact that many "data" issues arise months, or years, after a transaction has closed. For example, the FTC has investigated data security breaches and unlawful data collection practices that occurred years *before* the company was acquired, but were discovered months *after* a transaction closed.

21 months	9 months
Number of months hackers penetrated a target's systems *before* the target was acquired and investigated by the FTC.[230]	Number of months hackers continued to penetrate a target's systems *after* the target was acquired and investigated by the FTC.[231]

When you are involved in a merger or acquisition consider the following due diligence questions relating to data security during the course of the transaction:

1. Is the target subject to a sector specific data security law?

2. Has the target received a regulatory inquiry concerning its data security practices in the past two years?

[230] *See*, In the Matter of Reed Elsevier and Seisint, FTC Docket No. C-4226 (July 29, 2008), https://www.ftc.gov/enforcement/cases-proceedings/052-3094/reed-elsevier-inc-seisint-inc-matter.

[231] *Id.*

3. Has the target received litigation claims concerning its data security practices?

4. How many data security incidents has the target experienced? Is the quantity reported commensurate with what would be expected given the industry, type of data held by the target, and quantity of data held by the target? Remember that too few incidents can be as much of a "red flag" as too many.

5. What data breaches has the target experienced? Is the quantity reported commensurate with what would be expected given the industry, type of data held by the target, and quantity of data held by the target?

6. Does the target have a Written Information Security Program ("WISP")? If so, is it appropriate given the type and quantity of data held by the target?

7. Does the target have an Incident Response Plan ("IRP"). If so, is the IRP appropriate and effective?

8. How has the target dealt with prior security incidents and security breaches?

9. Has the target conducted and documented internal security assessments?

10. Has the target conducted and documented external security assessments (e.g., penetration tests, vulnerability scans, data security audits)?

11. If the target accepts payment cards, are any areas of non-compliance with the Payment Card Industry Data Security Standard ("PCI DSS") identified in their most recent Report on Compliance ("ROC")? Does the ROC appear to accurately describe the target's network and payment card infrastructure?

12. Has the target conducted a data map or a data inventory?

13. What are the target's data retention policies?

14. Does the target have a vendor management program in place? If so, how has the target evaluated the security practices of its vendors and subcontractors?

15. Does the target have dedicated employees focused on data security issues (*e.g.,* a Chief Information Security Officer)?

55. Selecting a Qualified Security Assessor ("QSA")

Retailers that accept credit cards are typically required by the payment card brands to show that they are in compliance with the Payment Card Industry Data Security Standards or "PCI DSS" at least once a year. How a retailer is permitted to show compliance depends in part on whether the retailer has a history of data security issues (*e.g.,* have they suffered a breach) and the quantity of credit cards that the retailer transacts each year. Typically retailers that have either had a data security breach, or transact large quantities of credit cards, are required to retain a Qualified Security Assessor or "QSA" to conduct an audit and to provide an independent report showing whether the retailer is, or is not, in compliance with the PCI DSS. Retailers that have not experienced a data breach and transact relatively few cards are often permitted to self-certify their compliance with the PCI DSS. Self-certification is usually

accomplished by the completion of a Self-Assessment Questionnaire ("SAQ") and an Attestation of Compliance ("AOC").

A QSA is a company that has been certified by the PCI Security Standards Council ("PCI SSC") to validate compliance with the PCI DSS. The independence, effectiveness, and consistency of QSAs has recently been called into question. Among other things, the Federal Trade Commission ("FTC") has initiated an investigation of the QSA-industry.[232]

By understanding what the FTC is looking at when evaluating QSAs retailers can perform their own due diligence to try to avoid allegations by the FTC, or others, that a QSA's examination is insufficient. The FTC's investigation is focused on the following issues that may impact a QSA's judgment in terms of a retailer's PCI DSS compliance:

1. The percentage of the QSA's revenue that comes from providing QSA services.

2. How often the QSA determines that retailers are not in compliance with the PCI DSS.

3. How QSAs bid, negotiate, price, and scope the audits that they perform.

4. The extent to which QSAs rely upon representations made by a retailer's employees.

5. The extent to which QSAs utilize sampling as part of their assessments.

6. The extent to which QSAs are willing to share "draft" reports with retailers that flag areas of non-compliance, but generate final reports that show full compliance if the retailer remediates areas of concern.

7. The extent to which QSAs are willing to issue final reports that show compliance based on assurances that a retailer will remedy a deficiency in the future.

8. The rate at which the retailers that a QSA certifies as compliant experience data breaches.

9. Whether QSAs have policies and procedures to prevent potential conflicts of interest.

10. How QSAs assess whether the risk of a PCI DSS deficiency has been appropriately mitigated by a "compensating control."

[232] Commission Orders to File Special Reports to Collect Information Regarding Data Security Auditors (file No. P155402).

The following provides a snapshot of information when evaluating a QSA:

193	9	≥3
The number of companies certified as QSAs in the United States.[233]	The number of QSAs that have been ordered to provide information to the FTC concerning their methods for conducting assessments.[234]	The number of QSAs that have been implicated in public lawsuits following data security breaches.[235]

56. Sharing Threat Indicators With The Government

After a security incident is identified organizations often consider whether to share information concerning the incident with government agencies. If the incident involved criminal conduct, federal law enforcement agencies – such as the Federal Bureau of Investigation or the United States Secret Service – may be interested in investigating and attempting to prosecute those responsible. It's also possible that law enforcement already may be investigating similar incidents and can share information that may help in your investigation. For example, they may be able to identify IP addresses associated with bad actors, security vulnerabilities that are being exploited within other organizations, or evidence that might suggest that criminals successfully obtained information from your organization.

The "Cybersecurity Act of 2015" is designed to promote the ability of organizations to identify data security incidents, and to share that information with law enforcement. The Cybersecurity Act has three main provisions. First, it provides a safe harbor from liability for organizations that monitor information systems for cyber threats. Under the safe harbor an organization cannot be sued for engaging in monitoring that complies with the Act. Second, if a threat is identified the Act provides a safe harbor for the organization to share that information with federal agencies. Third, if an organization chooses to share a cyber threat indicator or a defensive measure with the Federal government, any privilege that might have attached to the information shared (*e.g.,* attorney client privilege) is not waived.

What to consider when deciding whether to share information with the government:

1. Most organizations are not required to share information with the federal government concerning cyber threats or data security incidents. The Cybersecurity Act of 2015 does not compel sharing, it is designed to protect organizations that voluntarily choose to share information.

2. The Cybersecurity Act of 2015 only protects information shared with the *federal* government. If you are considering sharing information with state or local government agencies you should consider whether doing so may result in liability or privilege waiver.

---

233 PCI SSC website https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors (last viewed Jan. 14, 2018).

234 FTC to Study Credit Card Industry Data Security Auditing, Commission Issues Orders to Nine Companies that Conduct Payment Card Industry Screening (Mar. 7, 2016) *available at* https://www.ftc.gov/news-events/press-releases/2016/03/ftc-study-credit-card-industry-data-security-auditing.

235 QSAs responsible for certifications in the CardSystems, Target, and Heartland breaches appear to have been involved in the resulting litigation as possible defendants.

3. The safe harbors in the Cybersecurity Act of 2015 require that a company follow guidelines for what information can be shared, and how that information must be shared. You should carefully review the requirements before disclosing information to the government to make sure that you can utilize the protections under the Act.

4. To the extent that you have contractual or other statutory obligations not to share information with the government, it is uncertain whether courts will interpret the Cybersecurity Act of 2015 as immunizing your organization from liability if you choose to voluntarily share information.

The following provides a snapshot of info regarding threat monitoring and information sharing with the government:

46,000	83%
Number of members in Infragard – a forum created by the FBI for the private and public sector to share threat indicators.[236]	Percentage of Fortune 500 companies that participate in Infragard – an organization created by the FBI to facilitate the sharing of cyber threat information.[237]

57. Tax Filing Fraud

Tax returns and W-2s are information rich documents. Among other things they contain the name and Social Security Number of an employee, as well as information concerning their salary and address, and personal behavior and characteristics (*e.g.,* the charities that they support, their sources of income, their investments, and their relationships with financial institutions). Because of the type of data that they hold, each year cyber-attackers target these documents. If an attacker is successful at obtaining a tax return or a W-2, the attacker may attempt to sell the sensitive information contained in the file, may attempt to use tax-related documents (*e.g*., an employee's W-2) to submit a fraudulent income tax return in the hope of obtaining a refund owed to an employee, or both.

There are many methods by which attackers attempt to obtain tax related information. The most visible have been attempts to hack the Internal Revenue Service itself; unfortunately several of those attempts have been successful and have led to the loss of information about hundreds of thousands of tax payers.[238] Other attackers attempt to obtain tax documents from accountants or tax preparers, or from employers. For example, in 2016 IRS Commissioner Kohn Koskinen highlighted spear phishing attempts against human resource departments: "This is a new twist on an old scheme using the cover of the tax season and W-2 filings to try tricking people into sharing personal data. Now the criminals are focusing their schemes on company payroll departments . . . If your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent

[236] https://www.infragard.org/ (last viewed Jan. 2018).

[237] According to InfraGard website 413 out of 500 companies on the Fortune 500 have a representative in InfraGard. https://www.infragard.org/Application/General/Fortune500 (last viewed Jan. 2018).

[238] Jonathan Chew, *The IRS Says Identity Thieves Hacked Its Systems Again,* Fortune (Feb. 10, 2016) *available at* http://fortune.com/2016/02/10/irs-hack-refunds/ (last checked Dec. 29, 2017).

about confirming the identity of people requesting personal information about employees."[239] The following provides a snapshot of information regarding tax filing fraud.

1026	403%
The number of phishing scams for W2's reported to the IRS in January of 2016.[240]	The percentage increase in reported phishing attempts between January 2015 and January 2016.[241]

Employers should consider taking the following steps to help prevent a data breach of your employee tax records:

1) If you receive a request from an executive to email large quantities of employee information, verify that request by telephone with the executive before responding.

2) If you don't know the executive personally (*e.g.,* would not recognize his voice), make sure that when you verify the request you use an internal telephone number or find their telephone number in an internal directory (*i.e.,* don't trust any telephone numbers within an email).

3) If the request appears legitimate, consider transmitting the data using a secure connection (*e.g.,* a SFTP site) and not by email.

4) If you need to transmit tax information by regular email, encrypt the document that contains the information before sending it. If you company does not have separate encryption software, most versions of Microsoft Word and Adobe Acrobat provide for native encryption.

5) Never use a formulaic or easy-to-guess password for an encrypted file (e.g. employee's last name).

6) Do not publicly post any information that your employees may need to access their tax related information online. For example, if your payroll processor provides you with a business or company ID or code, that information should not be published on the internet as it typically forms a component of the layered security designed to protect tax information.

7) Track the rate of tax related fraud reported to your Human Resource department each year. If the quantity of tax reported fraud is significantly greater this year than it was in previous years, consider investigating whether your data may have been breached.

8) If you have fallen victim to email phishing, talk to your outside counsel about notification requirements and whether it makes sense to provide employees with credit monitoring services.

---

239 https://www.irs.gov/newsroom/irs-alerts-payroll-and-hr-professionals-to-phishing-scheme-involving-w2s

240 https://www.irs.gov/uac/Newsroom/Consumers-Warned-of-New-Surge-in-IRS-Email-Schemes-during-2016-Tax-Season-Tax-Industry-Also-Targeted .

241 *Id.*

9) If you discover that your employees' data was breached consider whether to notify the Internal Revenue Service and/or state revenue services, in addition to any government agencies that you may be required to notify (*e.g.,* a state attorney general).

10) Even if you have not had a breach, be prepared to answer questions from employees who have experienced tax related identity theft. Statistically many of your employees will experience identity theft this year and while the source of the information loss is probably not your company, or your vendors, your employees may assume that your system has been breached because the information used by the attacker to perpetrate fraud contained employee-related facts.

58. Third Party Vendor Management Programs

Third-party service providers present difficult and unique privacy and cybersecurity challenges. Vendor management is important throughout the life of a relationship with your service provider. Vendor diligence starts during the vendor selection process, continues through contract negotiation, and ends when the parties terminate their relationship. The goal is to effectively improve the service your vendors provide and mitigate the risk inherent in the vendor relationship.

$78 billion => $235 billion	62%	30%
The amount companies spent on cloud services in 2011, compared to the projected amount that companies are estimated to spend by 2017.[242]	The percentage of companies that evaluate the security risks of their third-party vendors.[243]	The percentage of breaches attributable to a third party supplier.[244]

What to consider when evaluating a vendor agreement:

1. What data and information will you be sharing with your vendor?

2. Does your vendor agreement require that the vendor use your data only to provide services to your company?

3. Under what terms is your vendor required to keep your data confidential?

4. Is your vendor required to comply with government requests to produce your data?

---

242 IHS Market, The Cloud: Redefining the Information, Communication and Technology Industry, (February 2014), http://press.ihs.com/press-release/design-supply-chain/cloud-related-spending-businesses-triple-2011-2017.

243 PricewaterhouseCoopers, US cybersecurity: Progress stalled Key findings from the 2015 US State of Cybercrime Survey, (July 2015), http://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf.

244 Beazley, Beazley Breach Insights – July 2017, (August 1, 2017), https://www.beazley.com/news/2017/beazley_breach_insights_july_2017.html.

5. Is your vendor required to keep your data in a logically distinct manner?

6. What are the laws and industry regulations that apply to your company with which your vendor will be required to comply?

7. Under what terms is your vendor required to notify you if your vendor is breached?

8. Is your vendor subject to your privacy, cybersecurity, and data retention policies?

9. Does your privacy policy allow your company to share your data with a vendor?

10. After the termination or expiration of the vendor agreement, under what terms is your vendor required to return your data?

11. What right does your vendor have to withhold access to your data or terminate your service?

12. What rights do you have to audit your vendor's operational practices?

13. Is your vendor required to self-audit?

14. Have your vendor's past audits exposed any vulnerabilities, or has your vendor been breached in the past?

15. Will your vendor be required to maintain certain levels of insurance during the term of the vendor agreement?

59. Wire Transfer Fraud

Businesses are increasingly falling victim to wire fraud scams – sometimes referred to as "man-in-the-email" or "business email compromise" scams. Although there are multiple variants, a common situation involves an attacker gaining access to the email system of a company, or the company's vendor, and monitoring email traffic about an upcoming transaction. When it comes time to submit an invoice or a payment, the attacker impersonates one of the parties and sends wire instructions asking that payment be sent to the attacker's bank account.

Wire fraud scams often victimize two businesses – the business that expected to receive payment, and the business that thought that they had made payment. The scam can cause significant contractual disputes between the victims as to who should bear the loss. Wire fraud scams also target businesses of all sizes across sectors. There is no single industry that is targeted more than another. [245]

[245] Federal Bureau of Investigation, Alert No. I-050417-PSA (May 4, 2017), https://www.ic3.gov/media/2017/170504.aspx.

40,203	$5.3 Billion	2370%
The number of businesses victimized by wire transfer fraud.[246]	The amount of domestic and international exposed dollar loss from October 2013 to December 2016 due to wire transfer fraud.[247]	Increase in identified victims and exposed loss from January 2015 to December 2016.[248]

Steps to help avoid wire fraud scams:

1. Avoid free web-based email systems to transact business.

2. Enable multi-factor authentication to log into all email systems.

3. Require employees to select unique and strong passwords or pass phrases.

4. Require employees to change email passwords frequently.

5. Require multi-factor authentication (e.g., email and telephone call) when receiving initial payment information.

6. Require multi-factor authentication when receiving a request to change payment information.

7. Send a confirmatory letter or email (not using the "reply" feature in email) concerning any request to change payment information.

8. Delay payment in connection with any request to change payment accounts or a request to make payment to a foreign bank account.

9. Review any request received by email to change payment accounts for signs that the email may be from a third party.

10. Provide clear instructions to business partners concerning how payment information should be communicated.

If you are victimized by wire fraud, consider:

1. Notifying the receiving bank and request that a freeze be placed on any remaining funds.

2. Notifying law enforcement.

3. Investigating whether your email system may have been compromised.

4. Asking business partners to investigate whether their email systems may have been compromised.

[246] *Id.*

[247] *Id.*

[248] *Id.*

5. Determining whether your organization has a crime-fraud insurance or cyber insurance policy and, if so, whether it extends to wire transfer fraud.

60. Written Information Security Policies

Although federal law only requires that financial institutions and health care providers maintain a written information security policy or "WISP," approximately thirty four states have enacted legislation that require organizations in other industries to take steps to keep certain forms of personal information safe. These statutes are broadly referred to as "safeguards" legislation. In some states safeguards legislation requires that organizations adopt certain security-oriented practices such as encrypting highly sensitive personal information or irrevocably destroying sensitive documents. In other states safeguards legislation requires the adoption of a comprehensive written information security policy.

5	4	8
Number of states that require that some, or all, of the security program be memorialized in writing.[249]	Number of states that require that an employee be designated to maintain the security program.[250]	Number of states that require that a security provision be included in contracts with service providers.[251]
$100 - $500,000 Range of Sate Safeguard Law Penalties.[252]		

The following are the most popular types of personal information protected by state statutes:[253]

91%	Social Security Numbers
74%	Financial Account Number
72%	Driver's License Number
31%	Health records
15%	Federal, State, or Local Tax Returns
12.5%	Biometric data

The top 10 sections typically included in a WISP are as follows:

1. Designated employee responsible for overseeing security program.

2. Procedure for appropriately destroying documents with sensitive information.

3. Encryption standards for mobile devices.

4. Encryption standards for transmitting sensitive information.

[249] Bryan Cave LLP, Survey of State Safeguards Laws, (2015).

[250] *Id.*

[251] *Id.*

[252] *Id.*

[253] *Id.*

5. Employee training.
6. Data breach incident response.
7. Vendor management.
8. Process for provisioning user access.
9. Process for de-provisioning user access.
10. Disciplinary measures for security violations.

GLOSSARY

The following is a quick-reference to defined terms or acronyms that are used in this handbook:

AMP	Administrative Monetary Penalties under CASL
BCP/DR	Business Continuity Planning / Disaster Recovery Plan
BCR	Binding Corporate Rules
BYOD	Bring your own device
CalOPPA	The California Online Privacy Protection Act, Cal. Bus. & Prof. Code 22575, *et seq.*
CAN-SPAM Act	Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003
CASL	Canadian Anti-Spam Law
CEM	Commercial Electronic Message under CASL
Consumer Sentinel	A collection of databases maintained by the FTC that tracks complaints submitted by consumers concerning data privacy, data security, advertising, and marketing practices of organizations.
COPPA	The Children's Online Privacy Protection Act
CPO	Chief Privacy Officer
CRTC	Canadian Radio Television and Telecommunications Commission
DAA	Digital Advertising Alliance
Directive	The EU Data Protection Directive 95/46/EC.
DOPAA	Delaware Online Privacy and Protection Act
DPI	The FTC's Division of Planning and Information.
DPIP	The FTC's Division of Privacy and Identity Protection.
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FTC	Federal Trade Commission
FTCA	Federal Trade Commission Act
HHS	The Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
Interagency Guidelines	Interagency Guidelines Establishing Information Security Standards pursuant to the Gramm-Leach-Bliley Act
NAI	Network Advertising Initiative
OCR	The Office of Civil Rights within the Department of Health and Human Services

PCI	Payment Card Industry
PFI	A forensic investigator certified by the PCI Council
PHI	Protected Health Information
RA	Resolution Agreement entered with the Department of Health and Human Services
ROSCA	The Restore Online Shoppers' Confidence Act
Safe Harbor	The US-EU Safe Harbor certification process.
SSN	Social Security Number
WISP	A written information security program.

CONTRIBUTORS

Chris Achatz, Associate (Boulder, Colorado)

Jenna Baranko (Privacy Intern)

Stephanie Bradshaw, Associate (Kansas City, Missouri)

John Bush, Associate (Atlanta, Georgia)

Jason Haislmaier, Partner (Boulder, Colorado)

Joshua James, Associate (Washington DC)

Jena Valdetero, Partner (Chicago, California)

David Zetoony, Partner (Washington DC / Boulder, Colorado)