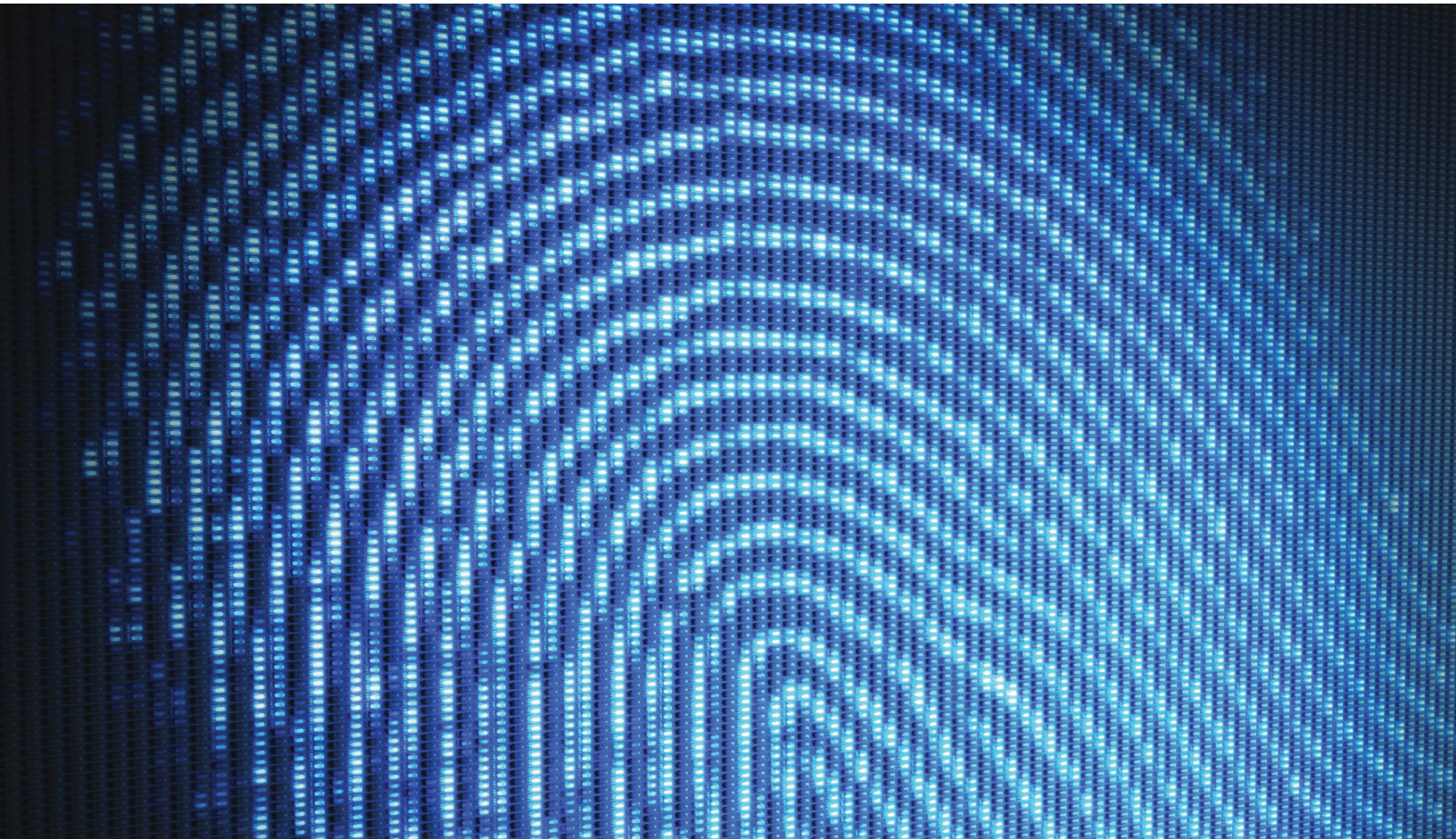
Crowe

Smart decisions. Lasting value.℠

April 2020

New Opportunities to Reinforce Personal Privacy Protections

An article by Pamela S. Hrubey, CCEP, CIPP/US, and Amanda M. Marderosian



In our digital age, consumers are exhausted by constant assaults on their personal privacy. Data breaches are commonplace even among reputable service providers. Users of many platforms have resigned themselves to the fact that their data will be harvested in exchange for service. The steps they need to take to protect their data from both legal and illegal exploitation seem futile. This phenomenon is known as "privacy fatigue."[1]

An expansive suite of legislation in Europe and, more recently, in the United States makes privacy a paramount concern for consumer-facing products and services. As a result, service providers must build privacy protection features into their offerings. To do so effectively, they must pay constant attention to the complexities of this evolving environment in order to maintain compliance.

A short history of privacy legislation

The European Union's General Data Protection Regulation (GDPR) came into effect on May 25, 2018,[2] replacing the 1995 Data Protection Directive. It has had major implications for all companies that collect and use the personal data of their customers. The GDPR is considered the most stringent set of regulations governing data use and protection ever implemented.

The GDPR is intended to shore up the protections afforded to consumer data and reinforce consumers' right to privacy. The European Commission defines personal data as "any information that relates to an identified or identifiable living individual."[3] This extremely broad definition is intended to capture the wide variety of means by which people are digitally identified, including not just names and addresses, but also numeric identifiers such as IP addresses and security features such as passwords.

Many interpret this legislation as a remedy for the ills of the digital age. That is certainly a valid assessment, but its roots date back to World War II. In the 1930s, Nazi Germany used the personal information collected by the census to locate and extort European Jews. Ultimately, the abuse of citizens' private data led to historic atrocities during the war. The liability of publicly available personal information thus became a major human rights concern and led Europe to become the leader in making sure that personal information remains private.[4]

The GDPR and privacy

In addition to deploying several specific provisions intended to make data use safer and more transparent for consumers, the GDPR carries substantial enforcement powers. Companies found to be noncompliant with the new regulations face stiff financial and regulatory penalties. The legislation grants investigators broad powers to audit companies to make sure that they are compliant, and these powers apply to any company offering services in EU states.

Fines for noncompliance can run up to as much as 4% of annual revenue or €20 million.[5] Particularly egregious instances might even warrant a permanent ban on data processing in all 27 EU member states.[6]

For the most part, the law applies equally to large companies and smaller operations, including startups. Small- and medium-sized enterprises are relieved of some of the burden. Nonetheless, the standard for compliance is very high.

The GDPR has several notable provisions. Privacy must be built into all new products – a mandate known as privacy by design. Further, consumers, referred to as data subjects under the GDPR, must actively consent to the collection of their data with full knowledge of what it will be used for. They must also be able to withdraw consent at any time and obtain a copy of the data collected free of cost. Their data must be encrypted to prevent theft. They must be able to transfer this data to other service providers – it cannot be proprietary. And they have a right to erasure of that data upon request.

Companies harvesting data must also conduct regular audits to assess vulnerabilities, and they are required to notify customers of any significant breaches within 72 hours. If certain types of particularly sensitive data such as information on race, gender, religion, or genetics are collected, a data protection officer must be on staff.

Privacy legislation in the United States

In the United States, the California *Consumer Privacy Act of 2018* (CCPA) is the most significant state-level privacy legislation to date. It became effective Jan. 1, 2020. Similarly, thorough draft bills have been introduced in about 25 states, and Maine, Nevada, and Vermont have tightened up their privacy laws in recent years.[7] This legislation should serve as a bellwether to companies that handle personal data. More stringent regulations are coming, and preparation is essential.

Companies are subject to the CCPA if they make more than $25 million in revenue, if they maintain data from more than 50,000 people, or if they make more than 50% of their revenue from sales of personal information. A maximum fine of $7,500 can be assessed for each intentional violation and a maximum of $2,500 can be assessed for each unintentional violation.[8]

Comparing the GDPR and the CCPA

The CCPA is broadly similar in scope to the GDPR. However, there are several noteworthy differences. For example, the CCPA defines personal information in a way that includes information that does not relate directly to a single individual (information associated with a household), whereas the GDPR restricts its definition to data on an "identifiable natural person." Under the CCPA, the timeline for addressing requests from data subjects is slightly more generous, at 45 days, while the GDPR only allows companies one month to comply with such requests.

The GDPR covers the data of all EU residents. The CCPA does not cover publicly available data, and it defers to regulations such as the *Health Information Privacy and Portability Act* and other federal financial regulations to cover primary uses of sensitive information such as medical or genetic data.

Dozens of minute differences exist between these two bodies of legislation as well, and complexities arising from differences in regulatory requirements will only increase as more states adopt their own versions of privacy laws. While there is typically a fair degree of overlap, the contradictions in these laws will make compliance in local markets an ever-more complicated task.

Identifying the similarities and differences in privacy and data protection-related laws as they apply to day-to-day activities is time-consuming and expensive. Until overarching federal legislation on the issue is in place, companies will need to factor the disentanglement of these conflicting statutes into their privacy models.

As consumers realize the risk that data exposure creates, they will almost certainly increase pressure on both service providers and legislators to strengthen protections. Their perspectives will play an important role in determining the privacy landscape going forward.

The importance of data mapping

Data mapping is a foundational process in supporting compliance with emerging privacy legislation. In this process, related sets of data are located and linked. Several steps must be completed to make sure that all data is accounted for and properly organized.

- First, processing activities must be identified. What data is being collected and how?
- Second, the owners of these activities need to be located. Which departments are collecting this data? How are they doing so?
- Finally, it is imperative to discern where this data is being stored and how vulnerable to misuse or exploitation it might be.

External consultants play a valuable role in this process. By conducting surveys of the involved parties, these questions can be answered in a centralized fashion. This process often involves the use of proprietary software. Consulting firms likely are more familiar with the efficient use of these programs.

Once this information has been analyzed, communication between siloed departments can be increased. In doing so, redundant data processing activities can be eliminated, and storage procedures can be centralized and standardized. If gaps are identified, new procedures can be implemented on a holistic level, and staffing needs can be reassessed. These processes can lay the foundation for a cohesive and forward-thinking privacy program that identifies points of weakness and corrects them before they become a true risk. Ultimately, these types of analysis can improve overall business efficiency.

Another reason why data mapping is critical is that several data practices can pose institutional risk. Failing to institute a data retention schedule can result in keeping data longer than is necessary or never removing it at all. Data that is past its useful life or no longer current ought to be disposed of. The suggestion of scrubbing unnecessary data can be a major disappointment to teams that have devised elegant means of collecting large volumes of data. But if there is no pressing need, and the protection of that data would involve costly processes, it might be best to simply purge it.

Data maps are living documents, and they must be regularly updated. The initial investment of time and resources can establish a baseline for the types of data collected and how it ought to be organized. Data mapping is incredibly time-consuming, detail-focused work, but to achieve full compliance with privacy legislation, data mapping needs to be a continual process.

Reconciling old and new

With the principles outlined by new legislation like the GDPR and CCPA in mind, it becomes easier to bake privacy compliance into developing systems. Additionally, future liabilities can be anticipated and planned for. Addressing weak points in existing systems is trickier. However, thorough data mapping can provide an accurate portrait of a data catalog and its liabilities.

The assessment of existing data and the production of new products that collect data can be complementary processes. The lessons learned from mapping existing data and the resulting understanding of its associated problems can then be applied to the design of new products that use this data or collect new information.

Compliance thus becomes a smoother process. It is impossible to comply with the increasingly specific provisions of privacy legislation if the types and locations of data collected are unknown. Consumers might want their data deleted, transferred to another company, or summarized per their rights under the new laws. As they become more aware of the possibilities for increased privacy under new legislation in other regions, they will almost certainly increase demands for such protections in jurisdictions that do not yet have such protections in place.

If companies are unable to comply with requests for this type of data service within the legally specified time frames, they might become the subject of complaints to regulatory bodies and subsequent investigations, which can be financially consequential.

Companies that elect an ethical approach to data collection, supported by ongoing data mapping, might recognize a positive impact to their brand. A survey of consumers conducted in 2019 by Cisco identified a group of individuals willing to switch service providers because of their privacy-related convictions. About 32% of respondents stated that they cared about privacy, were willing to act to protect their data, and had already taken action to protect it by switching companies.[9]

Risk and consequences for noncompliance

Aside from the punitive financial consequences of noncompliance, which can be substantial, there are reputational risks to consider. Data breaches are a regular feature of the news cycle. Many consumers have been burned and are now more cautious about disclosing certain information. Once a company has experienced a publicized data breach due to gaps in its cybersecurity system, consumers are likely to be more wary of doing business with that company for fear of falling victim to the same vulnerabilities.

One of the most infamous data breaches occurred in November 2013 when the retailer Target allowed sensitive data belonging to 41 million consumers to be exploited by malware using credentials belonging to a third-party vendor. Identifying information and credit card numbers were included in the breach. Many were forced to cancel cards and verify that their identities had not been stolen.

The breach also exposed 60 million customers to risk by exposing their contact information, including addresses. In May 2017, the company settled a multistate suit for $18.5 million.[10] An additional consumer class-action settlement amounting to $10 million, a settlement with banks for $39.4 million, and a settlement with Visa for $67 million were compounded by about $290 million in expenses related to the case.[11]

The home improvement retailer Home Depot experienced a similar breach in September 2014, with cards held by 56 million consumers compromised.[12] The exposure cost the company at least $179 million, plus legal fees.[13]

Data breaches at Yahoo in 2013 and 2014, not acknowledged until 2016, affected more than 3 billion people. The company settled a $117.5 million class-action suit in October 2019.[14] As a result of the breaches, Yahoo also lost $350 million on its 2017 sale to Verizon.[15]

In 2019, the data of more than half a billion users of the social media giant Facebook was exposed.[16] The company now faces numerous lawsuits and a record $5 billion fine from the Federal Trade Commission.[17]

While large companies might be able to rebound from incidents like these, smaller enterprises will find coping with financial and reputational repercussions more difficult. Without the name recognition and investor support commanded by these well-known businesses, small- and medium-sized businesses could be decimated by similar breaches.

Business integrity and consumer protection

These cautionary tales illustrate in dramatic fashion the necessity of developing and maintaining proper privacy programs. However, the risk posed by data breaches is only the tip of the iceberg. Forward-thinking companies should emphasize security concerns as a matter of business integrity. The financial risk posed by privacy liabilities is considerable, but the responsibility of protecting vulnerable consumers is perhaps a greater burden.

Companies have a fiduciary duty to make sure that consumers who entrust their data to them are adequately shielded from the myriad assaults on privacy that define the digital age. Consumers are fatigued and have resigned themselves to the fact that true privacy is nearly impossible. However, that realization does not give companies an excuse to expose their consumers' vulnerable personal information to risk.

Planning ahead

If consumers are suffering privacy fatigue at the moment, this phenomenon might be short-lived. As data breaches and abuses of personal information increase in frequency, and victims deal with ever-more dire consequences, a critical mass could be reached. American consumers likely will begin to demand more sweeping legislative solutions as they have in California and the EU. Federal legislation has been proposed, though nothing of substance has yet been passed. The *Consumer Privacy Protection Act of 2015* stalled in Congress,[18] but in 2019, Congress again raised the issue.[19]

Like many challenges, the growing ubiquity of data privacy laws also presents a major opportunity. Data privacy legislation provides an objective framework by which to measure any data privacy program. While the processes necessary to protect data privacy might seem burdensome, they can help facilitate more efficient interdepartmental communication and the standardization of data practices.

Data privacy and protection laws also serve as a harbinger of things to come. The changes signified by new legislation will compel forward-thinking companies to plan ahead and structure their data in ways that anticipate new security threats.

Learn more

Pam Hrubey
Managing Director
+1 317 208 1904
pam.hrubey@crowe.com

Amanda Marderosian
+1 646 356 4448
amanda.marderosian@crowe.com

---

[1] Hanbyul Choi, Jonghwa Park, and Yoonhyuk Jung, "The Role of Privacy Fatigue in Online Privacy Behavior," Computers in Human Behavior, April 2018, https://www.sciencedirect.com/science/article/pii/S0747563217306817

[2] Data Protection in the EU, European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en#legislation

[3] "What Is Personal Data?," European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

[4] Olivia B. Waxman, "The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History," Time, May 24, 2018, https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/

[5] "What Are the GDPR Fines?," European Commission, https://gdpr.eu/fines/

[6] "What if My Company/Organisation Fails to Comply With the Data Protection Rules?," European Commission, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-company-organisation-fails-comply-data-protection-rules_en

[7] "2019 Consumer Data Privacy Legislation," National Conference of State Legislatures, Jan. 3, 2020, https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx

[8] *California Consumer Privacy Act of 2018*, California Legislative Information, http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=

[9] "Consumer Privacy Survey: The Growing Imperative of Getting Data Privacy Right," Cisco, November 2019, https://www.cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html

[10] Kevin McCoy, "Target to Pay $18.5M for 2013 Data Breach That Affected 41 Million Consumers," USA Today, May 23, 2017, https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/

[11] Jonathan Stempel and Nandita Bose, "Target in $39.4 Million Settlement With Banks Over Data Breach," Reuters, Dec. 2, 2015, https://www.reuters.com/article/us-target-breach-settlement-idUSKBN0TL20Y20151203

[12] Eliana Dockterman, "Home Depot Breach Exposed 56 Million Credit Cards," Time, Sept. 18, 2014, https://time.com/3399822/home-depot-breach-exposed-56-million-credit-cards/

[13] Jeff John Roberts, "Home Depot to Pay Banks $25 Million in Data Breach Settlement," Fortune, March 9, 2017, https://fortune.com/2017/03/09/home-depot-data-breach-banks/

[14] Gina Martinez, "Yahoo Could Owe You Up to $358 for Data Breaches. Here's How to File Your Claim," Time, Oct. 15, 2019, https://time.com/5700738/yahoo-settlement-how-to-file-claim/

[15] Anjali Athavaley and David Shepardson, "Verizon, Yahoo Agree to Lowered $4.48 Billion Deal Following Cyber Attacks," Feb. 21, 2017, Reuters, https://www.reuters.com/article/us-yahoo-m-a-verizon/verizon-yahoo-agree-to-lowered-4-48-billion-deal-following-cyber-attacks-idUSKBN1601EK

[16] April Glaser, "Another 540 Million Facebook Users' Data Has Been Exposed," Slate, April 3, 2019, https://slate.com/technology/2019/04/facebook-data-breach-540-million-users-privacy.html

[17] Lesley Fair, "FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making," Federal Trade Commission Business Blog, July 24, 2019, https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history

[18] *Consumer Privacy Protection Act of 2015*, Library of Congress, April 30, 2015, https://www.congress.gov/bill/114th-congress/senate-bill/1158

[19] David McCabe, "Congress and Trump Agreed They Want a National Privacy Law. It Is Nowhere in Sight," New York Times, Oct. 1, 2019, https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html

crowe.com

CC20133-002A