Privacy Regulations

Wednesday, 10 April 2019 | 8–9:30 a.m.

Skadden Conference Center
Costantino Room | Second Floor

CLE Course Materials
Table of Contents

1. Speaker Biographies

2. CLE Materials

Panel 1: Privacy Regulations

Accenture. *Data Privacy.* [View in document]

Serrato, Jeewon Kim; Rosenzweig, Daniel. *GDPR, CCPA and beyond: Changes in data privacy laws and enforcement risks to monitor in 2019.* [View in document]

Fordham Accenture Compliance Series
Privacy Regulations Speaker Bios

Matthew Coleman
Law Clerk
Orrick, Herrington & Sutcliffe
Matthew Coleman is a Law Clerk in Orrick’s Cyber, Privacy & Data Innovation practice group in New York. Matthew leverages years of experience in researching, auditing, counseling, and litigating complex, multi-jurisdictional issues surrounding privacy, cybersecurity and information governance. Matthew is a Certified Information Privacy Manager and a Certified Information Privacy Professional with a specialization in United States privacy law. Matthew focuses his legal practice on helping clients develop global privacy programs to meet the requirements of an incomplete patchwork of privacy and cybersecurity laws, both in the U.S. and abroad, including the GDPR, CCPA and its progeny, GLBA, COPPA, FCRA, TCPA, CAN-SPAM and state breach notification and cybersecurity laws.

Anne Fealey
Global Chief Privacy Officer
Citi
Anne Fealey joined Citi as its Global Chief Privacy Officer in November 2018. Prior to that, she spent almost five years as Prudential’s first global head of privacy, where she built and managed the firm’s global privacy program. Before joining Prudential, Anne spent almost a dozen years at American Express, the last seven of which she created and ran the privacy program for the global merchant and network businesses. Anne is a lawyer by training and is passionate about privacy and enabling the appropriate uses of personal data.

Anthony Gonzalez
Vice President, Divisional Information Security Officer
QBE North America
Tony Gonzalez joined QBE North America as Vice President, Divisional Information Security Officer in March, 2018. In his role Tony works closely with the North American IT and business organizations to drive and integrate global Cyber Security strategy throughout QBE’s North American businesses. He is also responsible for Cyber Security Compliance and Risk Management program development and implementation. Prior to joining QBE, Tony has spent the last 20+ years in various IT and IT Security and Risk Management divisional and global leadership roles with Prudential Financial, Chemtura Corporation, Pfizer and Glaxo.

Robert Hoffman
Executive Director, N.A. Government Relations
Accenture
As executive director of Accenture government relations in North America since March 2018, Robert Hoffman leads a team of advocacy professionals to advance Accenture’s public policy agenda in the United States and Canada, reporting to Chad Jerdee, Accenture’s general counsel and chief compliance officer. Robert brings to Accenture three decades of public-policy experience, including 18 years as a global government relations advocate for some of the world’s most innovative and dynamic companies and developing deep policy expertise on relevant topics that include cybersecurity, data privacy, encryption, telecommunications, internet governance, and high-skilled immigration.
DATA PRIVACY

A platform for building trust-based relationships in financial services
The global financial services industry is undergoing the most rapid change in its history. Large-scale migration to the public cloud and a hyper-focus on personalization are just two examples of a revolution in the financial services experience. In this new environment, privacy is more important than ever.
Our analysis indicates that there is a financial “cost” to eroded trust in the digital economy. Over the next five years, large private sector firms risk losing an estimated $5.2 trillion in value creation opportunities, which translates to 2.8 percent in lost revenue growth over the period. But our Accenture 2019 Compliance Risk Study research also shows that mitigating privacy risk—an essential building block for improving trust between the financial services institution and client—is the most challenging priority for compliance programs to manage in the next year.¹

Privacy concerns are not new, though they have evolved considerably from a more nationalistic focus around cross-border data flows, to an additional layer around information security standards from state-based regulators such as the New York Department of Financial Services (NYDFS), and now to a more holistic view touching on consumer rights. This latest development has elevated privacy from a purely regulatory-driven agenda to one impacting broader questions around trust and sustainable business growth.

The European Union’s General Data Protection Regulation (GDPR) has been in force since May 2018 and has been instrumental in establishing a framework of specified rights for consumers with respect to their own data. Since implementation of GDPR, the California Consumer Privacy Act of 2018 (CCPA) that has been enacted is now in the formal rulemaking process, and could be subject to additional legislative changes before its effective date of January 1, 2020.² Unless a federal law is enacted that pre-empts multiple state laws like CCPA, we expect CCPA to be the de facto benchmark that sparks a wave of laws and regulations at the state level throughout the U.S., creating a patchwork of compliance requirements that could create new requirements and risk for financial institutions on top of those resulting from the federal Gramm-Leach Bliley Act (GLBA).

Industry groups—led by the Business Roundtable (BRT), a trade association representing 200+ CEOs from America’s leading companies—are seeking common ground at a national level regarding a framework for consumer rights and data privacy. In 2018, as Chair of the BRT’s Technology Committee and the Privacy Working Group, Accenture North America CEO Julie Sweet worked with CEOs across all major sectors, including financial services, to develop and put forward a framework in December 2018 for a national privacy law. While we believe a national privacy law is necessary and can eventually be achieved, in the interim, financial institutions should expect to face overlapping legal compliance requirements and potential litigation risk, each impacting their business strategy, risk management, and data and technology planning in an era of continued cost constraint.
Designing a Comprehensive Privacy Framework

Financial services institutions are investing in holistic activities, approaches and tools to address compliance needs related to emerging privacy regulations such as consumer rights.

Furthermore, financial institutions should take steps to understand how personal information enters their organization, how it remains in applications, and how unstructured data sources have generated a level of complexity over decades of organic and inorganic growth. Such monitoring, surveillance and reporting of data is also dependent on knowledge and close collaboration with a web of suppliers, who may be dependent on their own vendors, exposing the firm to potential and significant operational change.

Addressing this complexity in an efficient and effective manner that infuses innovation into current processes and technology can provide market differentiation for financial institutions, like increasing consumer loyalty in an era that places renewed premium on trust in client-financial institution relationships. Many institutions in the U.S. have put structures in place to respond to large-scale regulatory initiatives stretching back to GLBA and more recently NYDFS and GDPR. Many of these structures can be repurposed to proactively build stronger client relationship, with an emphasis on five core capabilities:

01 PRIVACY PROGRAM GOVERNANCE

Following the lead of the GDPR, many financial institutions are either establishing a position in the organization that is responsible and accountable for consumer rights and data privacy, like the data protection officer (DPO) or the chief privacy officer (CPO) role or raising the stature of these existing roles and conferring upon them the authority to highlight risks and make required changes across the organization. Such decisions should be taken in accordance with the organization’s privacy risk appetite.
The discovery, inventory and classification of personal information is a significant area of focus of any privacy program given the specific guidance of various regulations. Scanning should be automated and at scale with fit-for-purpose tools that can access unstructured data sources, leveraging existing technologies or supplementing with accelerators from the market. Implementation of data discovery and classification tools can be complex due to the multitude of architecture patterns and platforms on which data can reside. This often necessitates prioritizing the discovery of certain sources, while in parallel preparing for the discovery of more complex areas in subsequent sprints.

In addition to data discovery, capabilities should be leveraged to protect personal data across applications, workstations, servers, and the data supply chain in accordance with the overall privacy strategy. Identifying the remediation of legacy applications that may not support deletion, anonymization or other regulatory expectations is a key priority to support compliance, potentially requiring the adoption of more manual compensating controls in the short term, as a precursor to more strategic change.

Processes should be designed to manage all client requests related to privacy through to completion, such as access to information, opt out or erasure requests. Navigating the data supply chain across multiple third parties whose risk appetite, controls, and maturity may not match those of the financial institution is a key area of complexity, though persistence in closing out negotiations to update contract language and even to weigh the sustainability of certain relationships going forward is key.

Investments in technology cannot prevent major lapses and large fines if not accompanied by updates to policy and procedure, and the necessary training around such changes to build a culture of awareness and respect for consumer rights and data privacy. Training should take place at two levels: first, at the enterprise level, to build awareness; and, second, in the form of role-based guidance for front line staff handling consumer inquiries, such as consumer contact teams, social media specialists or those managing online platforms.
Establishing the Control Framework

The responsibility for establishing a culture of embedded privacy throughout the organization starts at the top, with the CEO and board of directors. Execution lays with senior managers establishing a control framework that can holistically address the dimensions of privacy risk.

Supporting the CEO and board of directors, the chief risk officer (CRO), general counsel (GC), chief compliance officer (CCO) and chief privacy officer (CPO) are key stakeholders in establishing the appetite for privacy risk while engaging key partners within the organization, such as the chief information officer (CIO) and chief information security officer (CISO). Each function has a role to play, but all functions should be aligned in terms of business strategy and execution.

From a three lines of defense perspective, areas of focus can be summarized in Figure 1. It illustrates, dependent upon their vantage point, the key questions senior stakeholders and their teams are looking to address during the data privacy transformation journey.

<table>
<thead>
<tr>
<th>Line of Defense</th>
<th>Focus Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FIRST LINE OF DEFENSE</strong></td>
<td><strong>01</strong> Business and operational management can help keep the focus on the consumer while dealing with near-term priorities such as how the business can process data access requests.</td>
</tr>
<tr>
<td><strong>SECOND LINE OF DEFENSE</strong></td>
<td><strong>02</strong> Those directly responsible for risk management can coordinate privacy policies and associated controls related to data collection and information request procedures, while providing a sustainable and suitably high-touch advisory model for the business going forward.</td>
</tr>
<tr>
<td><strong>THIRD LINE OF DEFENSE</strong></td>
<td><strong>03</strong> Audit functions should broaden their focus on privacy to properly address the expanded scope of programs and controls going forward, and to prioritize the items for management attention.</td>
</tr>
</tbody>
</table>

**Figure 1** Key questions being asked today around data privacy
<table>
<thead>
<tr>
<th><strong>Front Office</strong></th>
<th>What new parameters are being placed on business initiatives (e.g., analytics, automated decisions, chatbots)?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Marketing</strong></td>
<td>How do these regulations impact my ability to meet business objectives and marketing goals?</td>
</tr>
<tr>
<td></td>
<td>How can we differentiate our brand while responding to regulations?</td>
</tr>
<tr>
<td><strong>Operations</strong></td>
<td>Do we know the additional volumes of inquiries we are likely to handle?</td>
</tr>
<tr>
<td></td>
<td>How can we manage early customer inquiries in line with regulations, even with job aids not yet complete?</td>
</tr>
<tr>
<td><strong>Information Security</strong></td>
<td>What updates are required to breach and crisis playbooks?</td>
</tr>
<tr>
<td></td>
<td>What can be accomplished around freeze windows, for example before 1 January 2020?</td>
</tr>
<tr>
<td><strong>Technology</strong></td>
<td>How capable are systems of supporting consumer rights (e.g., portability, erasure)?</td>
</tr>
<tr>
<td></td>
<td>What changes are required to the information security risk assessment?</td>
</tr>
<tr>
<td><strong>Human Resources</strong></td>
<td>How prepared is the organization to respond to employee inquiries (e.g., erasure)?</td>
</tr>
<tr>
<td></td>
<td>If an employee is also a customer, are their rights different?</td>
</tr>
<tr>
<td><strong>Data Office</strong></td>
<td>Does the organization have a view of its structured and unstructured sources of data?</td>
</tr>
<tr>
<td></td>
<td>How should data governance practices be updated to support increased accountability requirements?</td>
</tr>
<tr>
<td><strong>Regulatory Relations</strong></td>
<td>Should we seek to proactively engage our regulator(s) regarding our approach, or keep to regular meetings?</td>
</tr>
<tr>
<td></td>
<td>How can we leverage industry bodies (e.g., Business Roundtable) to inform the privacy agenda?</td>
</tr>
<tr>
<td><strong>Compliance</strong></td>
<td>What updates are required to policies and procedures?</td>
</tr>
<tr>
<td></td>
<td>How should revised expectations be trained across the organization?</td>
</tr>
<tr>
<td><strong>Privacy</strong></td>
<td>Does privacy have sufficient stature in the organization?</td>
</tr>
<tr>
<td></td>
<td>Where is privacy best aligned within the organization?</td>
</tr>
<tr>
<td><strong>Risk</strong></td>
<td>How can risk appetite inform our interpretation of each privacy regulation?</td>
</tr>
<tr>
<td></td>
<td>What KPIs and KRIs should be used to monitor the response?</td>
</tr>
<tr>
<td><strong>Procurement</strong></td>
<td>What changes are required to how we risk assess our suppliers?</td>
</tr>
<tr>
<td></td>
<td>What updates are required to supplier terms and conditions?</td>
</tr>
<tr>
<td><strong>Internal Audit</strong></td>
<td>How should a privacy audit be approached?</td>
</tr>
<tr>
<td><strong>External Audit</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Data Privacy**
Responding to the Emerging Privacy Policy Landscape

GDPR was the first to redefine the global thinking on privacy and consumer rights. However, new regulations may expand protections even further, such as the CCPA’s provision for right to equal service for consumers.

There are different approaches that can be applied by financial services institutions in responding to emerging privacy regulations, depending on their risk appetite as well as the level of pre-existing capability built up through prior compliance efforts. Figure 2 provides some examples of these for institutions considering their response to CCPA.

Regardless of the approach taken, our experience supporting financial institutions on their journey to GDPR compliance has provided valuable lessons in the areas of scope and implementation. Key examples include the importance of operating in a truly cross-functional manner across the organization, reflecting the scope of new requirements and the opportunity to capture competitive advantage during the response. Another learning is to use a consumer perspective and focus in the design of revised process and technology capabilities, rather than a more siloed application-by-application view that can take more time to identify and understand interdependencies.
### Figure 2  Responses to emerging privacy and consumer rights laws

<table>
<thead>
<tr>
<th>TACTICAL</th>
<th>STRATEGIC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>01</strong> Implement Regulation for in-scope data subjects alone</td>
<td><strong>02</strong> Enhance data privacy model for all data subjects to align with Regulation</td>
</tr>
</tbody>
</table>

**PROS**

<table>
<thead>
<tr>
<th>Implement Regulation for in-scope data subjects alone</th>
<th>Enhance data privacy model for all data subjects to align with Regulation</th>
<th>Address Regulation within a broader “Consumer Rights” Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Narrower scope, providing greater transparency to ROI</td>
<td>Opportunity to re-use prior enterprise capability development (e.g., NYDFS, GDPR, etc.)</td>
<td>Integrate efficiencies from “build once, solve for many” approach</td>
</tr>
<tr>
<td>May increase the chance of reaching compliance with the letter and spirit of the rule</td>
<td>Reduced complexity of capability development and deployment</td>
<td>Opportunity to develop capability ahead of legislation</td>
</tr>
</tbody>
</table>

**CONS**

<table>
<thead>
<tr>
<th>Implement Regulation for in-scope data subjects alone</th>
<th>Enhance data privacy model for all data subjects to align with Regulation</th>
<th>Address Regulation within a broader “Consumer Rights” Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less efficient as additional federal and state guidance comes onstream</td>
<td>May require re-work as federal and state guidance continue to change</td>
<td>Challenges defining “highest common denominator” across in-scope rules</td>
</tr>
<tr>
<td>Potential for an uncoordinated “patchwork” of compliance efforts without standardization</td>
<td>Potential resistance to performing compliance tasks that are not directly applicable</td>
<td>Gaining enterprise collaboration and alignment can impede agility</td>
</tr>
</tbody>
</table>

Source: Accenture, March 2019
Conclusion

Financial services institutions have been presented with an opportunity to create more transparent and trust-based relationships with their clients by taking a holistic approach that goes beyond mere compliance and security concerns and allows them to create differentiated outcomes.
About the Authors

Samantha Regan
Samantha is the Global Lead for the Regulatory Remediation and Compliance Transformation group within Accenture’s Finance & Risk practice. She has over 17 years of global experience working with C-suite executives and their businesses in compliance and regulatory initiatives.

Gracie Pereira
Gracie is a Managing Director in the Accenture Security Financial Services team with over 18 years of experience in the field of cybersecurity and privacy, technology risk, system and operational audit, and IT transformation. She has held executive level positions at large financial institutions, and has extensive experience leading the information technology and risk group, with an emphasis on information risk management and infrastructure engineering.

Ben Shorten
Ben is a Senior Manager with Accenture Finance & Risk. Based in New York, Ben serves as the Compliance Transformation Offering Lead for Accenture in North America. Ben has extensive experience working with investment banks, retail banks and insurance providers in North America, the UK, and continental Europe to define compliance strategy in response to regulatory and government mandates and ongoing changes in the financial services ecosystem.

Gregory Ross
Gregory is a Senior Manager in Accenture’s Finance & Risk practice, with responsibility for the Fraud Management Consulting area. Gregory brings his experience and knowledge in the areas of resiliency, regulatory and compliance, and operational risk management processes and technology solutions to help financial services organizations strategize and deliver robust and streamlined risk management capabilities. He also has deep experience driving strategy design and implementing risk management functions, as well as executing key risk management processes at-scale. Gregory also has significant experience organizing and running large-scale, regulatory-driven enhancement programs.

Timothy Lisko
Tim is a Security Principal Director in the Accenture Security practice. Tim focuses on assisting CxOs and boards on the journey to take control of their cyber security, privacy, and consumer rights programs, aligning them to the business goals and strategy, providing appropriate capabilities to the organization, and when possible creating market differentiation. Tim has been involved with the security and privacy industry for over 15 years.
ACKNOWLEDGMENT

The authors would like to thank the following Accenture employees for their important contribution to this document: Garrett Swanberg and Anwar Ali.

REFERENCES


ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world’s largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 469,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Its home page is www.accenture.com.

DISCLAIMER

This document is intended for general informational purposes only and does not take into account the reader’s specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.
With significant enforcement activity and new laws being enacted or proposed since the start of the year, regulators in the EU and the US, several US states, and the US Congress are showing they mean business in terms of data privacy.

To help companies best protect consumer data and remediate enforcement risks, we provide below an overview of the following:

1. two noteworthy recent EU and US regulator enforcement actions;
2. changes in the US state data privacy law landscape, including the proposal from the California Attorney General’s Office to expand enforcement authority and class action litigation under the California Consumer Privacy Act; and

EU and US regulators continue to increase the stakes for data privacy enforcement

On January 21, 2019, in one of the largest privacy fines announced globally, the French National Data Protection Commission (CNIL) imposed a €50 million penalty against a tech giant for violation of the General Data Protection Regulation (GDPR). This was followed by press reports in February that the US Federal Trade Commission (FTC) is currently negotiating a multi-billion dollar fine against a social media giant to settle the agency’s investigation into its privacy practices. To date, the largest fine the FTC had
imposed on a tech giant for breaking an agreement with the government to safeguard consumers’ data was a US$22.5 million penalty settlement in 2012.

Specifically, the CNIL’s enforcement action focused on the GDPR’s transparency and consent requirements and provides useful tips for companies that are looking for guidance on how to design privacy policies and consent tick boxes (click here for our earlier coverage of the multi-million Euro GDPR fine and key takeaways).

The FTC’s investigation started in the immediate aftermath of the Cambridge Analytica scandal, which focused on the controls a company must have on how its data is shared with and used by third parties. The complete scope of the investigation, however, has not been released yet but will likely include a broader review of the company’s data processing methods and practices, including how the company uses the data it collects from its members.

These CNIL and FTC actions signal that data privacy enforcement risk is now among one of the top risks a company must consider as part of its enterprise risk management framework.

The CCPA and CCPA-copycat laws in the US could bring higher scrutiny to privacy violations in the US

Several US states, following the GDPR’s passage last May, are proposing their own data protection laws that provide certain GDPR-like consumer rights. However, the US states’ approach has key differences noteworthy for businesses operating in the US.

The California Consumer Privacy Act (CCPA), passed in June 2018 in response to the Cambridge Analytica scandal, is slated to become the most comprehensive data privacy law in the US. The Act goes into effect on January 1, 2020 and like the GDPR, provides certain rights to consumers, including the “Right to Know,” “Right to Access,” “Right to Opt-Out” and “Right to Deletion.” Additionally, the CCPA greatly expands the definition of personal information so how these rights will be applied in practice requires significant changes to be made in how companies operate. The Act, unlike any other previously-enacted data protection law, also requires an opt-out link on the companies’ website, to allow consumers to opt out of data sharing to third parties. The Act permits a private right of action in the case of data breaches and allows for administrative penalties to be imposed by the California Attorney General of up to $7,500 per violation with no maximum cap (click here for coverage of the CCPA’s key requirements).

Companies now have less than a year to put compliance programs in place for the CCPA, and yet the California legislature is continuing with its efforts to amend the law, adding to increased uncertainty for businesses. On February 22, California Attorney General Xavier Becerra and Senator Hannah-Beth Jackson introduced legislation to strengthen and clarify the CCPA. Among other things, the bill would: (1) no longer require the Office of the Attorney General to provide businesses and private parties individual CCPA-compliance advice; (2) remove language that would have previously allowed companies to cure CCPA violations prior to the AG bringing an enforcement action; and (3) provide consumers a private right of action to seek remedies for any violations of their CCPA rights, not just limited to data breaches. If this proposal were to be adopted, it would further expand the AG’s ability to bring enforcement actions and significantly increase class action litigation in California.

Not to be outdone by California, eleven (11) states—including Maryland, New Jersey and Washington—have recently introduced similar legislation. Among other things, the bills include their own versions of opt-out rights and require new disclosure requirements that are slightly different than the GDPR and CCPA. If enacted, these laws would result in significant costs for businesses as they try to understand and put in place
a privacy framework that would comply with this patchwork of US and non-US laws that often have overlapping and conflicting requirements. In fact, the level of complexity and uncertainty posed by these various changes in the legal landscape is leading businesses to call on the US Congress to step in and implement national comprehensive data privacy legislation.

The US Congress’s response to regulator and state data privacy activity

In response to increased enforcement action and US state activity, the 116th US Congress has introduced several data privacy bills to implement a federal data privacy standard in the US. For example, the American Data Dissemination Act (S. 142) would “impose privacy requirements on providers of internet services similar to the requirements imposed on Federal agencies under the Privacy Act of 1974”. The Social Media Privacy Protection and Consumer Rights Act of 2019 (S. 189), among other things, would require covered entities to “(1) offer a user a copy of the personal data of the user that the operator has processed, free of charge, and in an electronic format; and (2) notify a user within 72 hours of becoming aware that the user’s data has been transmitted in violation of the security platform.”

Indeed, even the US Government Accountability Office – a federal legislative agency that provides the Congress auditing, evaluation, and investigative services – recommends that the US Congress pass federal data privacy legislation, stating that “[r]ecent developments regarding Internet privacy suggest that this is an appropriate time for Congress to consider comprehensive Internet privacy legislation.”[1]

If the US Congress passes federal data privacy legislation, it would represent a first-ever federal privacy standard, with the promise of uniformity and consistency in what would otherwise be a patchwork of state laws and regulatory standards.

This week, the House Energy and Commerce Committee and the Senate Commerce Committee are holding hearings on what key issues the federal privacy legislation should seek to address. We will provide an update covering the two committee hearings here.

Our take

Recent enforcement actions by the EU and US regulators and active legislative changes at the state and federal level in the US mean data privacy risks should be one of the top risks managed by companies as part of the enterprise risk management framework. Because the GDPR, CCPA, and other state and US legislative proposals each introduce new and different requirements on the collecting, processing, sharing, and maintaining of personal data, companies should conduct gap assessments at least annually to identify any business activities that are in non-compliance or pose a high risk to the company.

As a result of specific requirements under the CCPA, for example, businesses that have either employees or customers in California should consider adding the following to their compliance project plans for 2019:

- review and revise their Website Privacy Policy to meet new data disclosure, consent and opt-out requirements;
- review, revise, and deliver training for a new Employee Privacy Notice that complies with the CCPA;
- draft and roll out new processes and train key internal teams that would intake and respond to privacy inquiries and complaints;
- review and test incident response plans that prepare the organization to respond effectively in the case of a data breach; and
• review and roll out Master Service Agreements with restrictions for data use by service providers that are required under the CCPA.

Reforming the U.S. Approach to Data Protection and Privacy

Rather than a comprehensive legal protection for personal data, the United States has only a patchwork of sector-specific laws that fail to adequately protect data. Congress should create a single legislative data-protection mandate to protect individuals’ privacy.

January 30, 2018

Introduction

Half of all Americans believe their personal information is less secure now than it was five years ago, and a sobering study from the Pew Research Center reveals how little faith the public has in organizations, whether governmental or private-sector, to protect their data—and with good reason. In 2017, there was a disastrous breach at Equifax. Yahoo’s admission that...
Yet record-shattering data breaches and inadequate data-protection practices have produced only piecemeal legislative responses at the federal level, competing state laws, and a myriad of enforcement regimes. Most Western countries have already adopted comprehensive legal protections for personal data, but the United States—home to some of the most advanced, and largest, technology and data companies in the world—continues to lumber forward with a patchwork of sector-specific laws and regulations that fail to adequately protect data. U.S. citizens and companies suffer from this uneven approach—citizens because their data is not adequately protected, and companies because they are saddled with contradictory and sometimes competing requirements. It is past time for Congress to create a single legislative data-protection mandate to protect individuals’ privacy and reconcile the differences between state and federal requirements.

A Patchwork of Existing Protections

The United States lacks a single, comprehensive federal law that regulates the collection and use of personal information. Instead, the government has approached privacy and security by regulating only certain sectors and types of sensitive information (e.g., health and financial), creating overlapping and contradictory protections.

The rules that govern health information illustrate this problem. The Health Insurance Portability and Accountability Act (HIPAA), the United States’ primary health privacy and security law, only applies to “covered entities” holding “protected health information.” Federal regulators acknowledge [PDF] that most Americans have no grasp of when their health information is protected by the law and when it is not—or what security standards apply in either case. Separate privacy laws govern specific areas of the U.S. health-care system [PDF]:

THIS SITE USES COOKIES TO IMPROVE YOUR USER EXPERIENCE. CLICK HERE TO LEARN MORE.
records existed in physical file cabinets and not digital clouds. FERPA, in turn, intersects with and sometimes conflicts with the Children’s Online Privacy Protection Act (COPPA), which does protect data, but only of children under the age of thirteen.

Widespread collection of personal information puts [people's] privacy and security at risk.

State laws add to this patchwork, particularly with respect to data breaches. Many states recognize that widespread collection of personal information [PDF] puts their residents’ privacy and security at risk. Starting with California, which enacted the first data-breach notification law in 2003, forty-eight states have passed laws that require individuals to be notified if their information is compromised. These laws have different and sometimes incompatible provisions regarding what categories and types of personal information warrant protection, which entities are covered, and even what constitutes a breach. Notification requirements also vary: New Jersey requires that the state police cybercrime unit be notified, while Maryland requires that the state attorney general be notified before any affected individual is.

Enforcement of these laws is also complicated. While state attorneys general have an important role to play, the Federal Trade Commission (FTC) considers itself the “top cop on the privacy beat.” The FTC has the general power to prohibit “unfair and deceptive trade practices” under Section 5 of the FTC Act, and has attempted to establish a data-security baseline through over sixty different enforcement actions. However, companies have begun to aggressively push back against the FTC’s legal authority to police data-security practices, and the FTC has limited jurisdiction over banks, insurance companies, nonprofit entities, and even some internet service providers.
The Challenge of Preventing and Responding to Data Breaches

Experienced security professionals advise even the most sophisticated organizations that they will eventually experience a breach. Even organizations with multiple layers of digital and physical security are vulnerable to the persistent threats of commercial and governmental intrusion, as well as inept or intentionally malicious insiders. Perfect security is impossible, and the informational injuries that can result from the collection and (mis)use of data are constantly evolving.

As a result, many lawmakers sought to respond to the Equifax breach and similar breaches by reassessing data-breach notification rules. Members of Congress are reintroducing data-breach protection proposals, and industry voices have suggested that the United States could have finally reached the “tipping point” that will lead to the creation of a single national data-breach notification standard.

“Breach-notification laws . . . place the burden on the individuals whose information has been compromised.”

This is a common refrain after every headline-making breach, but enacting data-breach
some of which could occur years after the initial incident. Eliminating conflicting state notice provisions at the federal level, while simplifying the experience for both consumer and institution, does nothing to address this problem.

Companies need clearer rules, and individuals need to be able to incentivize companies to secure data. Most data breaches, even with the costs of disclosure and response and the attendant reputational harm, do not result in significant financial harm to companies. Even when regulators such as the FTC get involved, the likelihood of any monetary fine is small. A more comprehensive legal framework is needed: one that offers a mix of incentives for better security practices, disclosures, and individual protections.

**Toward a Baseline Privacy and Security Proposal**

The twenty-first-century economy will be fueled by personal data. But it is not yet clear what rules will govern this information, with whom information will be shared, and what protections will be put in place. A baseline data-protection law would provide a legal framework for answering these questions.

Such a proposal is not new. The FTC has continually called on [PDF] Congress to enact flexible and technologically neutral privacy and security laws, and nearly six years ago the Barack Obama administration put forward a blueprint for its Consumer Privacy Bill of Rights, based on Fair Information Practice Principles (FIPPs). The FIPPs are generally thought of as processes and procedures that organizations should implement; the Privacy Bill of Rights recognized that individual Americans have an ongoing interest in how information about them is collected, used, and shared by companies and government entities alike.
the industry craft its own rules, and a draft legislative bill was quietly put forward only three years after the initial proposal. Since then, data practices across all industry sectors have continued to fall short of individual privacy and security expectations.

“
Lawmakers’ failure to provide users with a set of privacy rights has made the United States a global outlier.
”

The Donald J. Trump administration appears to have little appetite for technology policy or legal regulation in general, and lawmakers’ continuing failure to provide users with a set of privacy rights has also made the United States a global outlier. While the U.S. legal framework on personal data has not meaningfully changed in several decades, the European Union has enacted multiple data-protection directives. With the revised General Data Protection Regulation (GDPR), the European Union has become the focal point of the global dialogue on individual data privacy. In contrast to U.S. law, EU law protects all personal data, regardless of who collects it or how it is processed. Other advanced economies, such as Canada, Israel, and Japan, have pivoted toward creating privacy regimes that are compatible with the EU’s GDPR rather than with the patchwork approach of the United States. This puts U.S. companies at a disadvantage globally as emerging economies adopt simpler, and often more EU-style, comprehensive approaches.
rights and responsibilities. This would not only simplify compliance for U.S. companies, but would also strengthen and bring the United States in line with emerging data-protection norms. Congress could implement an effective baseline privacy regime with at least the following four qualities.

First, the law should cover all institutions, not just tech companies, credit-rating agencies, and other narrow sectors of the economy. Data protection is not only part of corporate social responsibility in a digital age, it is also both an institutional risk and an essential compliance function for any organization that collects, uses, or shares personal information or other potentially sensitive consumer data.

Second, the law should harmonize the inconsistencies and fill the gaps created by the existing sectoral approach. Health information is sensitive regardless of whether it is input into a consumer application, generated by a wearable device, or conveyed to a medical professional. A baseline privacy law could polish away the inconsistent consent requirements, access rights, and security protections around health information that exist in between and outside of HIPAA, FERPA, and COPPA, for example.

“Incentives for companies to protect data should skew toward prevention, rather than self-flagellating disclosures.”
should offer easy-to-use individual access, correction, and deletion mechanisms for users’ data, and documented risk assessments and other compliance requirements, which leave a paper trail. When these mechanisms are backed by the force of law, companies are put on notice that they need to prioritize data security, which in turn gives privacy and security professionals and consumer advocates more leverage to push for better industry practice. If the United States adopted the significant fines for noncompliance seen in the European Union’s GDPR, corporate practice could be reshaped—for not just major technology firms but also small and medium-sized enterprises and nonprofit entities.

Fourth, the U.S. legal framework should recognize and provide mechanisms to address the harms that result from privacy violations. Lawmakers and courts recognize the harm of breaches, but the definition of a “privacy harm” should be expanded. Identity theft is one such harm, but so too are the inconveniences suffered by affected individuals and their gnawing sense that they lack control over their “digital selves.” These less quantifiable harms that result from the exposure of bits and bytes of individuals’ personal lives should be recognized by law: as the depths of these harms are plumbed and addressed over time, individuals should be afforded a private right of action to hold companies accountable, and regulators should have the ability to penalize entities that flout their duty to be responsible stewards of personal information. Jack Balkin, the director of Yale Law School’s Information Society Project, has suggested that companies be thought of as “information fiduciaries” and proposed a grand bargain that would extend a duty of care for personal information in exchange for legal certainty and safe harbors for industry.

A simpler and more comprehensive approach to individual digital dignity is warranted, especially after this past year of increasing magnitude of breaches and digital stewardship
This Cyber Brief is part of the Digital and Cyberspace Policy program. The Council on Foreign Relations takes no institutional positions on policy issues and has no affiliation with the U.S. government. All views expressed in its publications and on its website are the sole responsibility of the author or authors.

Nuala O’Connor