protiviti®

Face the Future with Confidence

Building a Comprehensive Data Privacy Program

Four actionable steps for technology companies

Internal Audit, Risk, Business & Technology Consulting

Introduction

Most technology companies today understand that ensuring data privacy and protection is an imperative for their business; however, few manage this process well or even invest enough resources in that effort. As governments and consumers around the world continue to raise their expectations of how technology businesses should handle and process private and sensitive data, the need to both formalize and improve data privacy practices will become increasingly critical. Global technology companies in particular should reevaluate their geographic footprint with an eye towards ensuring compliance with global privacy laws.

High-profile data breaches and concerns about poorly managed data-sharing practices with third-party vendors and service providers are helping fuel the concerns of regulators and consumers. They are also driving the development of more — and more — stringent regulations stipulating how companies should handle sensitive consumer data.

In December 2020, for example, the U.S. Federal Trade Commission (FTC) launched an inquiry into the privacy policies, procedures and practices of several major social media and video streaming service providers, including Amazon, Facebook, Twitter, WhatsApp, YouTube, TikTok, Snap and Reddit.[1]

In a joint statement on the inquiry, FTC Commissioners Rohit Chopra, Rebecca Slaughter and Christine Wilson decried that despite the central role of prominent online platforms in our daily lives, the decisions that they make regarding consumers and consumer data remain shrouded in secrecy. "Critical questions about business models, algorithms, and data collection and use have gone unanswered," the statement read. "Policymakers and the public are in the dark about

KEY STEPS FOR TECH COMPANIES	WHY IT MATTERS
Conduct a data privacy risk assessment	Helps organizations identify weaknesses in data privacy compliance and protection efforts
Establish a baseline	Allows firms to capture the totality of their privacy commitments, determine exactly what they've promised customers and whether or not they are honoring those commitments
Manage change	Ensures that data privacy is a strategic priority for the business and that a "culture of compliance" around data privacy is established
Enhance documentation	Enables organizations to maintain clearly verifiable and readily accessible documentation of data privacy plans and processes, thereby avoiding program management challenges

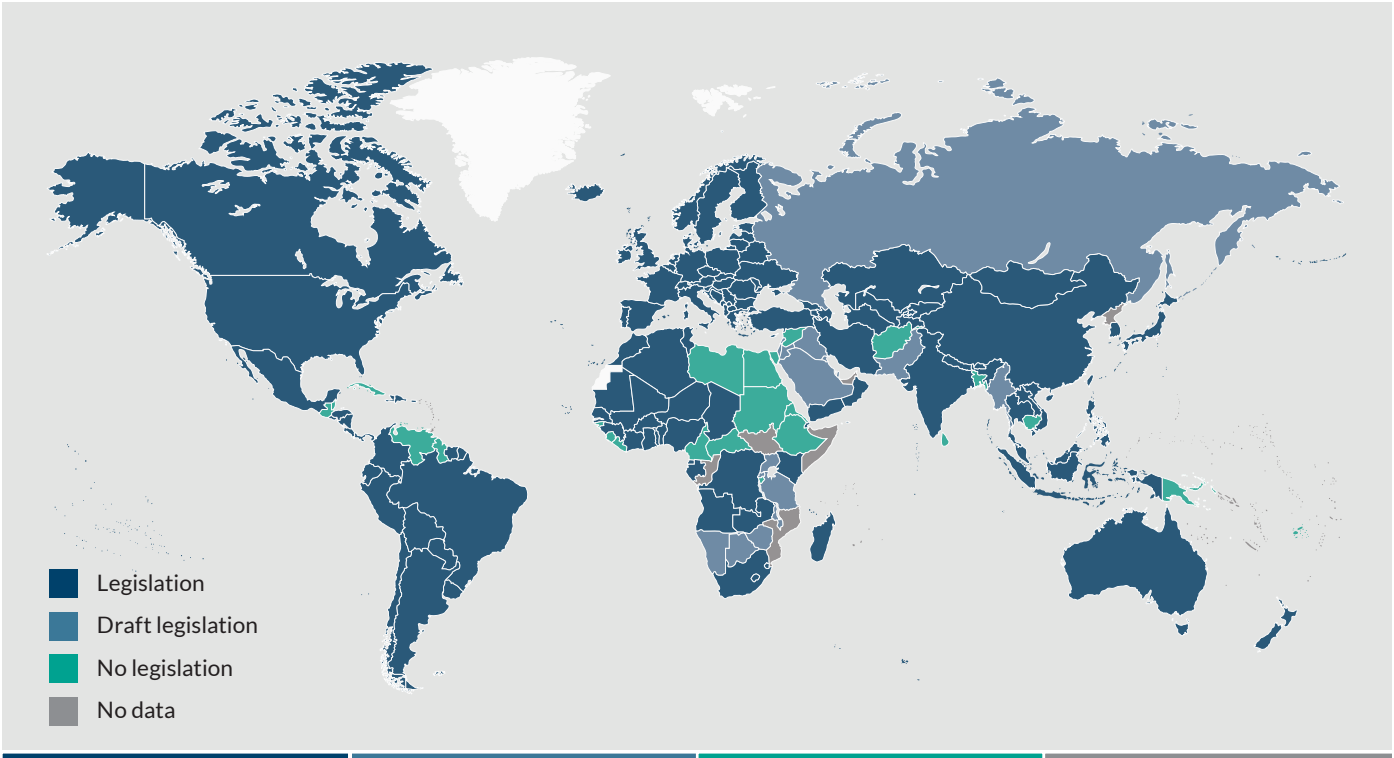
[1] "Resolution Directing Use of Compulsory Process to Collect Information Regarding Social Media and Video Streaming Service Providers' Privacy Practice," FTC, December 14, 2020: www.ftc.gov/system/files/documents/reports/6b-orders-file-special-reports-social-media-service-providers/6b_smvss_resolution.pdf.

what social media and video streaming services do to capture and sell users' data and attention. It is alarming that we still know so little about companies that know so much about us."[2]

Global efforts on privacy rules

Several countries – including Brazil, Canada and South Africa – have implemented comprehensive privacy regulations. In recent years, these efforts have been driven by the need to create stricter data privacy rules around new technological and market developments. Within the European Union, for example, Parliament is finalizing new rules governing the processing of information by electronic communications service providers. After more than four years of difficult negotiations, the European Council announced in February 2021 that member states have reached an agreement on the new ePrivacy regulations to replace the 20-year-old ePrivacy Directive.[3]

Data Protection and Privacy Legislation Worldwide



(as of January 2021)

[2] "Joint Statement of FTC Commissioners Chopra, Slaughter and Wilson," Federal Trade Commission, December 14, 2020: joint_statement_of_ftc_commissioners_chopra_slaughter_and_wilson_regarding_social_media_and_video.pdf.

[3] "Confidentiality of Electronic Communications: Council Agrees its Position on ePrivacy Rules," European Council, February 10, 2021: Confidentiality of electronic communications: Council agrees its position on ePrivacy rules - Consilium (europa.eu)

The ePrivacy regulations will cover electronic communications content transmitted using publicly available services and networks, and metadata related to the communication, as well as machine-to-machine data transmitted via a public network. In a statement, Pedro Nuno Santos, the president of the European Council, admitted the path to reaching an agreement has not been easy, but "we now have a mandate that strikes a good balance between solid protection of the private life of individuals and fostering the development of new technologies and innovation."

Among these technologies, artificial intelligence is a growing area of focus. In March 2021, the Centre for Information Policy Leadership, a global data privacy and cybersecurity think tank, issued a white paper on how to implement a risk-based approach to AI regulation and compliance. With the intention of informing current EU discussions on the topic, the organization recommended, among other things, a regulatory framework focusing only on high-risk AI applications and a risk-based organizational accountability framework that calibrates AI requirements and compliance to the specific risks at hand.[4]

Heightened potential for federal data privacy legislation in the United States

Conditions for a federal privacy law in the United States are now likely to be more favorable under the Biden administration. The incoming team, including several members who worked in the Obama administration, have experience working on privacy issues. Also, federal privacy legislation would be in keeping with Vice President Kamala Harris' "track record and interest in privacy-related topics during her career as California attorney General and U.S. senator," as The National Law Review notes.[5]

As California's attorney general, Harris created the state's Privacy Enforcement and Protection Unit in 2012 to regulate the collection, retention, disclosure, and destruction of private or sensitive information by individuals, organizations and the government. Prior to that, she helped forge an industry agreement among the nation's leading mobile and social application platforms to increase privacy protections for consumers who use apps on their smartphones, tablets and other electronic devices. Apple, Amazon, Facebook, Google, Hewlett-Packard, Microsoft are among the platform companies that signed on to that agreement.[6]

There is also an expectation that the Biden administration can help smooth the path to negotiations with the European Commission over a new version of the EU-U.S. Privacy Shield. In 2020, the Court of Justice of the European Union declared the program invalid as a mechanism to comply with EU data protection requirements when transferring personal data from the EU to the United States.[7]

Any work toward creating federal data privacy legislation in the United States is likely to take a back seat in 2021 while the new administration addresses the COVID-19 pandemic, its economic and societal impacts, and other pressing issues for the country. Given these priorities, the administration is likelier to kick off its privacy agenda in 2022.

[4] "CIPL Recommendations on Adopting a Risk-Based Approach to Regulating Artificial Intelligence in the EU," Centre for Information Policy Leadership, March 22, 2021: cipl_risk-based_approach_to_regulating_ai__22_march_2021_.pdf (informationpolicycentre.com)

[5] "Election 2020: Looking Forward to What a Biden Presidency May Mean for Data Privacy and Data Privacy Litigation," National Law Review, November 12, 2020: www.natlawreview.com/article/election-2020-looking-forward-to-what-biden-presidency-may-mean-data-privacy-and.

[6] "Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit," Office of the Attorney General, July 19, 2012: oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-privacy-enforcement-and-protection.

[7] "FAQs — EU-U.S. Privacy Shield Program Update," Privacy Shield Framework, updated August 20, 2020: www.privacyshield.gov/article?id=EU-U-S-Privacy-Shield-Program-Update.

INTERNATIONAL	U.S.-SPECIFIC STATE LAWS
• Australia Privacy Act • Canada Personal Information Protection and Electronic Documents Act (PIPEDA) • Dubai Privacy Law • EU Data Governance Act (proposed) • EU Digital Services Act (proposed) • EU ePrivacy Regulation (proposed) • EU General Data Protection Regulation (GDPR) • India Privacy Act (proposed) • LGPD – Brazil's Privacy Law • South Africa – Protection of Personal Information Act (POPI) • U.S. Children's Online Privacy Protection Act (COPPA) • United States Consumer Data Privacy Act (proposed) • U.S. Consumer Online Privacy Rights Act (proposed)	• California Consumer Privacy Act (CCPA) • California IoT Security Law • California Privacy Rights Act (CPRA) • Illinois Biometric Information Privacy Act (BIPA) • Maine Act to Protect the Privacy of Online Consumer Information • Nevada Senate Bill 220 Online Privacy Law • New York Biometric Information Privacy Bill • New York Privacy Act (NYPA) & New York State Senate Bill S567 (proposed) • Texas Biometric Privacy Act • Virginia Consumer Data Protection Act (CDPA) • Washington Biometric Privacy Act

(as of January 2021)

Meanwhile, states including Virginia, Maine, Massachusetts and Nevada have recently joined California in enacting their own privacy, data security, cybersecurity and data breach notification laws. California is preparing to create a new consumer data privacy agency following approval by its voters of the California Privacy Rights Act (CPRA) last November.[8] Despite strong opposition from technology, media and telecommunications firms to state-based privacy rules, the fragmentation in U.S. privacy laws is expected to continue until a federal privacy law is in place.

Enthusiasm for more privacy rules remains high among state legislators, many of whom are closely watching their counterparts in states like California iron out the details of their law before setting their own policies.

More evidence that tech firms should bolster data privacy efforts

Changes in the regulatory environment aside, there are other reasons technology companies should prioritize building a comprehensive data privacy program. Consumer sentiment is one.

[8] "CPRA Explained: New California Privacy Law Ramps Up Restrictions on Data Use," by Maria Korolov, CSO, December 21, 2020: www.csoonline.com/article/3601123/cpra-explained-new-california-privacy-law-ramps-up-restrictions-on-data-use.html.

Recent data shows that 64% of consumers in the United States consider a company's data privacy policies very important.[9] In a recent survey of more than 1,000 North American consumers, over half of the respondents said they are likelier to trust a company that asks only for information relevant to its products or that limits the amount of personal information requested — a signal, perhaps, that these consumers perceive the company as taking a thoughtful approach to data management.[10]

In the post pandemic recovery period, technology companies will want to ensure that they are well-positioned to use customer data for innovation and deliver new products and services. Transparent and easy-to-understand policies and practices for data privacy and protection will help businesses earn users' trust — along with their willingness to permit the company to collect and use their data to create new and more personalized customer experiences.

Also, as the responsible investment trend continues to expand, a growing number of investors are giving a more critical eye to how technology companies protect their customers' personal data. Current trends suggest data privacy practices are becoming more important to environmental, social and governance (ESG) reporting. As an example, S&P Global has added several cybersecurity data and privacy questions to its Corporate Sustainability Assessment which it issues to companies.[11] Some leading tech companies are already detailing data privacy policies and practices in their corporate social responsibility reports and other public-facing outlets, including their websites.

The opportunity to tackle a top risk head on

Many technology companies have invested significantly in data privacy and protection efforts in recent years, though those investments have often fallen short. In many cases, revenue maximization has trumped privacy, and as companies have grown larger and more complex, tracking data usage and ensuring compliance with laws and commitments has become a much more difficult activity. This is underscored by the fact that the issue of ensuring data privacy and protection consistently ranks among the top risks for technology companies in Protiviti's annual global risk survey.[12]

What's at Stake?

A strong privacy program can help your organization avoid:

- Major fines
- Loss of customers (and trust)
- Diminished investor confidence
- Decline in market share
- Damage to brand reputation

Legal and compliance teams at technology companies understand that building a comprehensive data privacy program can no longer be a back-burner initiative. There's simply too much at stake, whether it's the potential for major fines for noncompliance or losing customers, investor confidence and market share. These teams know data privacy challenges are

[9] "U.S. Online Consumer Concerns About Brands and Data Privacy 2019," Statista, August 28, 2020: www.statista.com/statistics/308707/company-transparency-regarding-consumer-data-usage.

[10] "The Consumer-Data Opportunity and the Privacy Imperative," by Venky Anant, Lisa Donchak, James Kaplan and Henning Soller, McKinsey, April 27, 2020: www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative.

[11] "Pandemic Prompts Companies to Ramp Up Forthcoming ESG Initiatives," S&P Global, December 17, 2020: www.spglobal.com/en/research-insights/articles/pandemic-prompts-companies-to-ramp-up-forthcoming-esg-initiatives.

[12] To download the latest annual top risks survey data, including results by industry group, from Protiviti and the ERM Initiative at North Carolina State University's Poole College of Management, visit www.protiviti.com/US-en/2020-top-risks.

emerging and evolving, and the actions the company takes now to identify and manage these issues require improvement. To identify these issues, these teams should consider the following questions:

- Is the company moving and growing so fast that privacy is always an afterthought?
- How is the tone at the top influencing data privacy practices? Is leadership emphasizing the importance of data privacy, or communicating messages effectively, so that the company can build a culture of compliance?
- Is the company inadvertently violating its data privacy policies and commitments when different business units and teams take a siloed approach to launching new initiatives and don't consider how those efforts may impact current policies and commitments?
- Are our engineering and product development teams standing in the way of the business implementing a data privacy program because they worry it will have a negative impact on their work? (And is business leadership knowingly allowing them to resist change because they also worry about stifling innovation?)
- Is the business doing only the minimum when it comes to ensuring data privacy and protection, and thus creating risk by not doing enough?
- Does the company approach compliance with data privacy and protection mandates like one-and-done projects and not an ongoing program?

It is fair to assume that most technology companies will answer in the affirmative to some, if not all, of the above questions as these are common problems that many are struggling to address effectively. But it also means technology companies have an opportunity to meet this key risk for their business head on — and manage it far better than they likely are doing today.

> *"Having driven the expansion of the digital age, technology companies are under increased scrutiny globally by regulators and legislatures, and many find themselves playing defense regarding the protection of personal data, maintaining privacy protections, and accusations of anticompetitive behaviors. Forward-thinking tech companies are addressing these challenges head on by bolstering their compliance capabilities, refreshing their privacy program, and identifying and mitigating increased areas of risk brought on by process or system changes, business acquisitions, third-party vendor involvement, and other business model changes."*
>
> — Gordon Tucker, Managing Director & Global Leader, TMT

Steps to make data privacy and protection an embedded process

Positive change comes from treating data privacy and protection efforts like a formal compliance initiative. That will help to ensure that the business, at all levels, starts to look at everything it does through a privacy lens. How does every new partnership, marketing strategy, product or service rollout, or other change potentially impact data privacy and protection commitments that the company has made, or the compliance mandates it needs to meet?

It takes time, focus and resources to transition to this way of thinking and make data privacy and protection an embedded process. Based on Protiviti's experience working with leading technology companies, the following four steps are fundamental to laying the groundwork for a comprehensive data privacy program that can help the business preserve customer confidence and meet evolving — and intensifying — regulatory expectations:

01 Conduct a data privacy risk assessment

This assessment is essential for identifying weaknesses in data privacy compliance and protection efforts. The objective of a typical risk assessment is to identify:

- The data collected, stored and processed by the organization
- The privacy risks to that data (e.g., confidentiality, security)
- Controls in place at the organization to address those risks
- Residual risks not addressed by those controls (i.e., the gaps)

Ultimately, the assessment can help leadership better understand which data privacy and protection regulations are most critical to the business and determine compliance obligations.

02 Establish a baseline

Baselining involves capturing the totality of an organization's privacy commitments; determining exactly what the company has promised its customers regarding how the business collects, processes, stores and transfers their data; and, most important, whether or not the company is honoring those commitments. In the absence of a federal privacy law and the prevalence of disparate state laws, it is critical that organizations adopt a baseline to control the framework they are building. Organizations should consider extending these commitments to contracts, third-party vendor relationships and training.

03 Manage change

Organizations must continually assess how new privacy decisions, changes to services and products, or changes to how consumer data shared with third parties can impact data privacy commitments and compliance requirements. Traditionally this has been a major challenge for organizations, particularly large technology companies, where changes happen at a code or data level literally every minute. Building a sustainable change-management program that can manage this change is critical. For leaders, this means ensuring that data privacy is a strategic priority for the business and that a "culture of compliance" around data privacy is established. Effectively managing change ensures that privacy commitments to customers are honored and trust is maintained.

04 Documentation

There are two critical documentation approaches that are essential to building a successful data privacy program. First, it's important to document the privacy procedures, processes, risks and/or controls. This is a deficiency for many technology companies because it takes time, effort and investment to do it in a comprehensive way. Second, the processes within

the business that deal with customer information (or covered information) also require documentation because they generate the risks that firms need to understand and carefully manage. Having a proper understanding of the existing processes requires capturing how changes to those processes would impact privacy risk. Inevitably, organizations that do not maintain clearly verifiable and readily accessible documentation of plans and processes tend to encounter challenges managing their program. As such, an employee dedicated to managing document security and compliance, as well as ensuring that all records are complete and updated, is highly recommended.

> *Beyond publishing applicable policies, organizations must know precisely how data is used to ensure they're following their own policies – not just at the application and data level, but across the entire organization.*
>
> — Jeff Sanchez, Managing Director, Security & Privacy

How Protiviti can help

Technology companies are facing unprecedented change in the data privacy landscape. Numerous new and evolving regulations worldwide are forcing business, technical and legal operational changes on an almost weekly basis. These changes often overlap, creating complex legal and regulatory scenarios for businesses.

Additionally, technology firms are under intense pressure to meet heightened expectations about data privacy from their customers, investors and many other stakeholders, including their employees. The ability to manage data and privacy issues effectively, and demonstrate that strength to the marketplace, may prove to be a competitive differentiator for many technology companies.

Protiviti helps technology businesses establish comprehensive data privacy and protection programs that cross legal, technical, business and compliance groups. Our approach helps ensure that the programs that tech firms create meet or exceed legal data privacy obligations efficiently and cost-effectively.

ABOUT PROTIVITI

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, governance, risk and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60 percent of *Fortune* 1000 and 35 percent of *Fortune* Global 500 companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

CONTACTS

Gordon Tucker
Managing Director and Global Leader,
Technology, Media & Telecommunications
+1.415.402.3670
gordon.tucker@protiviti.com

Terry Jost
Managing Director and Global Leader,
Security & Privacy
+1.469.965.6574
terry.jost@protiviti.com

Jeffrey Sanchez
Managing Director,
Security & Privacy
+1.213.327.1433
jeffrey.sanchez@protiviti.com

Daniel Hansen
Managing Director,
Security & Privacy
+1.415.402.3697
daniel.hansen@protiviti.com

Kaitlin Curry
Director,
Risk & Compliance
+1.206.262.8385
kaitlin.curry@protiviti.com

THE AMERICAS

UNITED STATES
Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Denver
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*
Buenos Aires

BRAZIL*
Belo Horizonte
Rio de Janeiro
Sao Paulo

CANADA
Kitchener-Waterloo
Toronto

CHILE*
Santiago

COLOMBIA*
Bogota

MEXICO*
Mexico City

PERU*
Lima

VENEZUELA*
Caracas

EUROPE, MIDDLE EAST & AFRICA

FRANCE
Paris

GERMANY
Berlin
Dusseldorf
Frankfurt
Munich

ITALY
Milan
Rome
Turin

THE NETHERLANDS
Amsterdam

SWITZERLAND
Zurich

UNITED KINGDOM
Birmingham
Bristol
Leeds
London
Manchester
Milton Keynes
Swindon

BAHRAIN*
Manama

KUWAIT*
Kuwait City

OMAN*
Muscat

QATAR*
Doha

SAUDI ARABIA*
Riyadh

UNITED ARAB EMIRATES*
Abu Dhabi
Dubai

EGYPT*
Cairo

SOUTH AFRICA *
Durban
Johannesburg

ASIA-PACIFIC

AUSTRALIA
Brisbane
Canberra
Melbourne
Sydney

CHINA
Beijing
Hong Kong
Shanghai
Shenzhen

INDIA*
Bengaluru
Hyderabad
Kolkata
Mumbai
New Delhi

JAPAN
Osaka
Tokyo

SINGAPORE
Singapore

*MEMBER FIRM

protiviti®