EXECUTIVE SUMMARY

The U.S. Securities and Exchange Commission requires most publicly traded companies to annually disclose in their Form 10-K submissions potential risk factors to investors. Beginning in 2017, the IAPP studied these disclosures to assess not just whether companies have been disclosing personal data processing practices and privacy regulations as a risk, but also increasingly what business harms the organizations faced for getting privacy wrong.

For the first several years of our study, we reviewed the risk disclosures of up to 150 of the largest publicly traded companies in the U.S., across industries, attempting to quantify their collective sense of privacy risk. This year, the IAPP’s Westin Research team took a different approach, focusing on six key industry sectors and reviewing the privacy risk disclosures published by a selection of five companies in each sector. The industry sectors we chose to focus on are business-to-consumer technology, business-to-business technology, pharmaceuticals and health services, banking and finance, brick-and-mortar retail, and health insurance.

We found that across industries, there is growing concern about the cost of compliance with a rapidly evolving privacy regulatory landscape. Even industries structured for regulatory compliance, such as the financial services and health/pharma industry sectors, see privacy law compliance as at least a short-term business risk due to the global variance in privacy laws, concerns about lawful international data transfers, and the interconnectedness of data storage and analytics services with multiple third parties.

Industry sectors relatively new to personal data-processing regulation — the B2C and B2B tech sectors, for instance — lead the pack on privacy risk disclosures because information privacy and security concerns feature prominently in their revenue streams. They, along with retail and banking sectors, also rely heavily on data analytics for predicting consumer behavior and anticipating external threats. They see restrictions on their use of personal data not just as regulatory compliance concerns, but also as foundational to their growth and prosperity.

We found that across industries, there is growing concern about the cost of compliance with a rapidly evolving privacy regulatory landscape.

It’s important to remember that the nature of a Form 10-K risk disclosure is to point out to potential investors what could go wrong. Nonetheless, some industries note that offering con-
Consumers trustworthy products and services is key to their market position. Failing to comply with privacy laws may very well signal to consumers that the enterprise may not be reliable; on the flip side, privacy regulatory compliance can be an opportunity to win consumer trust and fortify the brand. We observed both sides of the coin represented in the 2019 10-Ks.

This report is organized as follows: We attempt to extract and summarize (in our own words) the privacy risk disclosure essence for each selected industry sector, based on our reading of the five selected companies’ most recent Form 10-K risk factors. We then highlight the major disclosed privacy risks. In an attempt to rate risk perception per industry, we selected six privacy risk factor categories to compare across industry sectors: breach/cyberattack; sectoral privacy legal compliance; comprehensive privacy law compliance; payment card industry standards compliance; risk of private litigation or regulatory enforcement action; and risks to core revenue from consumer behavior tied to privacy, such as breach of trust or harm to brand. More information about these measures can be found in the key on this page.

Finally, for each industry sector, we illustrate the key points with selected quotes from certain risk disclosures and longer clips from those that were either standouts in their phrasing or illustrative of the industry’s view on privacy, generally. Throughout, we insert commentary from privacy thought leaders who work as in-house privacy professionals for industry-representative organizations.

Industry sectors relatively new to personal data-processing regulation ... lead the pack on privacy risk disclosures because information privacy and security concerns feature prominently in their revenue streams.

Privacy risk disclosures in 6 major industry sectors

We identify six privacy risk categories common across industries:

- **Breach/cyberattack** resulting in disclosure of personal data;
- **compliance with sectoral privacy laws** (e.g., the U.S. Health Insurance Portability and Accountability Act);
- **compliance with comprehensive privacy laws** (e.g., the EU General Data Protection Regulation and California Consumer Privacy Act);
- **compliance with the PCI standards**;
- **risk of private litigation or regulatory enforcement action** resulting in damages, fines or other sanctions; and
- **risk to core revenue based on consumer privacy preferences** (e.g., harm to reputation or brand, inability to use consumer data for analytics).
Major B2C tech platforms have for many years enjoyed the freedom to expand and innovate with little regulatory oversight. Now, however, with the growing impact of comprehensive privacy laws worldwide, including the GDPR, the CCPA as revised by the California Privacy Rights Act, and even Brazil’s newly enacted General Data Protection Law, global tech companies face unprecedented business risks due to their data practices.

This change in the regulatory landscape has altered how these companies are conducting business — or at a minimum, the warnings they provide to investors. **While the possibility of a cyberattack or security breach still remains top of mind, regulatory compliance — and the cost of noncompliance — has gained prominence in the B2C tech industry’s overall risk outlook.**

Compliance costs in terms of privacy staffing, litigation expenses and the potential for regulatory fines are not their only concerns. Also disclosed was the potential for lost revenue due to changes in the regulation of consumer-behavior-tracking technologies and consumer consent requirements. Many B2C tech platforms profit from paid advertising, a business line made more profitable by their ability to target ads to consumers. **Privacy laws and regulations may dampen the success of these targeting technologies, placing stress on the industry’s revenue streams.**

Another key risk noted in this industry sector’s disclosures was confusion surrounding the legality of cross-border data transfers, as the most popular traditional method, standard contractual clauses, has been called into question. As well, increased regulatory scrutiny and litigation based on consumer privacy concerns, enforcement of competition and anti-trust laws, and the associated negative publicity are flagged for their potential to increase business costs and decrease consumer trust.

We rely on (data) transfer mechanisms permitted under these laws, including (SCCs). Such mechanisms have recently received heightened regulatory and judicial scrutiny. If we cannot rely on existing mechanisms for transferring personal data from the (European Economic Area), the United Kingdom or other jurisdictions, we may be unable to transfer personal data ... in those regions.
FACEBOOK

If people do not perceive our products to be useful, reliable and trustworthy, we may not be able to attract or retain users or otherwise maintain or increase the frequency and duration of their engagement. Factors that can negatively affect user retention, growth and engagement include decreased engagement with our products or failure to accept our terms of service as part of changes that we implemented in connection with the GDPR. …

Our advertising revenue is dependent on targeting and measurement tools that incorporate these signals, and any changes in our ability to use such signals will adversely affect our business. For example, legislative and regulatory changes, such as the GDPR and CCPA, have impacted, and we expect will continue to impact, our ability to use such signals in our ad products. In addition, mobile operating system and browser providers, such as Apple and Google, have announced product changes, as well as future plans to limit the ability of application developers to use these signals to target and measure advertising on their platforms. …

In addition, the other bases upon which Facebook relies to legitimize the transfer of such data, such as SCCs, have been subjected to regulatory and judicial scrutiny. … the Irish Data Protection Commissioner has challenged the legal grounds for transfers of user data to Facebook, and the Irish High Court has referred this challenge to the Court of Justice of the European Union for decision. …

Competition authorities in the United States, Europe and other jurisdictions have initiated formal and informal inquiries and investigations into many aspects of our business, including with respect to users and advertisers, as well as our industry. For example, in June 2019, we were informed by the (U.S. Federal Trade Commission) that it had opened an antitrust investigation of our company. In addition, beginning in the third quarter of 2019, we became the subject of antitrust inquiries and investigations by the U.S. Department of Justice, the U.S. House of Representatives and state attorneys general.
Unlike their B2C counterparts, B2B tech companies — the quintessential data processors — seem less concerned about the consequences of new privacy legislation and regulation. Their business customers have insisted upon security features — and increasingly, privacy by design, as well — for several years. As privacy laws demand that controllers put stronger privacy and security controls in their supply chain, including through contractual obligations that shift risk to data processors, B2B tech firms have found privacy and security of their hardware, software and cloud services to be market differentiators. Indeed, given their size and sophistication, players in this industry sector are already well staffed to comply with data privacy laws, such as the GDPR.

That said, changes in the privacy and data protection regulatory environment still pose risk. Compliance with complex global privacy laws, such as the CCPA and GDPR, cross-border data transfer uncertainty, and meeting their B2B customers’ contractual demands all feature prominently in this industry’s risk disclosures. At least one company in this sector mentioned that they are expected to self-regulate through standards and private organizations. Another discussed how the insights gathered by consumer data helped them increase their efficiency and service quality to consumers and worried that privacy legal compliance could hinder these competitive assets.

“[T]he uncertain and shifting regulatory environment and trust climate may cause concerns regarding data privacy and may cause our customers or our customers’ customers to resist providing the data necessary to allow our customers to use our services effectively. Even the perception that the privacy and security of personal information are not satisfactorily protected or do not meet regulatory requirements could inhibit sales of our products or services and could limit adoption of our cloud-based solutions.”
MICROSOFT

As we continue to grow the number and scale of our cloud-based offerings, we store and process increasingly large amounts of personally identifiable information of our customers and users. The continued occurrence of high-profile data breaches provides evidence of an external environment increasingly hostile to information security. Despite our efforts to improve the security controls across our business groups and geographies, **it is possible our security controls over personal data, our training of employees and third parties on data security, and other practices we follow may not prevent the improper disclosure or misuse of customer or user data we or our vendors store and manage.** In addition, third parties (that) have limited access to our customer or user data may use this data in unauthorized ways. … Despite our efforts to protect customer and user data, perceptions that the collection, use and retention of personal information is not satisfactorily protected could inhibit sales of our products or services and could limit adoption of our cloud-based solutions by consumers, businesses and government entities. …

We are building (artificial intelligence) into many of our offerings and we expect this element of our business to grow. **We envision a future in which AI operating in our devices, applications and the cloud helps our customers be more productive in their work and personal lives.** As with many disruptive innovations, AI presents risks and challenges that could affect its adoption, and therefore, our business. AI algorithms may be flawed. Datasets may be insufficient or contain biased information. Inappropriate or controversial data practices by Microsoft or others could impair the acceptance of AI solutions. These deficiencies could undermine the decisions, predictions or analysis AI applications produce, subjecting us to competitive harm, legal liability, and brand or reputational harm. Some AI scenarios present ethical issues. **If we enable or offer AI solutions that are controversial because of their impact on human rights, privacy, employment or other social issues, we may experience brand or reputational harm.** …

In July 2020, the (CJEU) invalidated a framework called Privacy Shield for companies to transfer data from EU member states to the United States. This ruling has led to uncertainty about the legal requirements for data transfers from the EU under other legal mechanisms. Potential new rules and restrictions on the flow of data across borders could increase the cost and complexity of delivering our products and services in some markets.

The continued occurrence of high-profile data breaches provides evidence of an external environment increasingly hostile to information security.
The tech industry is closely watching how regulators approach privacy. It’s important to know how regulators are treating privacy because privacy can be a vehicle for regulators to be able to regulate other aspects of our business. ... Privacy is important to our consumers. If our consumers know they can trust us with their data and know what is being done with their data, then they are more willing to give us access to their data to be able to improve our products and enhance the value of our products.

Tech industry privacy officer
Accustomed to being regulated, the health and pharmaceutical industries, perhaps unsurprisingly, launched their data-related risk disclosures with concerns about privacy regulation. Compliance with major U.S. legislation — HIPAA and the Health Information Technology for Economic and Clinical Health Act — dominate the concerns, but increasingly these organizations also mention the GDPR, CCPA and Canada’s Personal Information Protection and Electronic Documents Act, as well as “other applicable privacy regulations,” among their top compliance risks. As one company noted, “There has been an increased attention to privacy and data protection issues in both developed and emerging markets with the potential to affect directly the company’s business.” These global firms also mentioned concerns about international transfers of personal data among the potential compliance risks.

Across the industry sector, companies mentioned cybersecurity risks, generally after privacy regulation, as a potential threat to their business and operations. Most described the sophistication of their IT systems and their significant information security investments but were obliged to note that such systems are nonetheless always vulnerable to cyberattack and vendor mismanagement.

One leading medical supply/pharmaceutical firm identified risk around consumers lacking access to online services and their own data, given the reliance consumers now have on remote access to health information and the “timely delivery of medical care.”

“We are required to comply with increasingly complex and changing data privacy regulations both in the (U.S.) and beyond that regulate the collection, use, security, processing and transfer of personal data, including particularly the transfer of personal data between and among countries. Many of these regulations also grant rights to individuals.”
Privacy and data protection laws increase our compliance burden. We are subject to a variety of privacy and data protection laws that change frequently and have requirements that vary from jurisdiction to jurisdiction. For example, under HIPAA we must maintain administrative, physical and technological safeguards to protect individually identifiable health information and ensure the confidentiality, integrity and availability of electronic protected health information. We are subject to significant compliance obligations under privacy laws such as the GDPR, PIPEDA and CCPA. Some privacy laws prohibit the transfer of personal information to certain other jurisdictions. We are subject to privacy and data protection compliance audits or investigations by various government agencies. Failure to comply with these laws subjects us to potential regulatory enforcement activity, fines, private litigation, including class actions, and other costs. We also have contractual obligations to customers that might be breached if we fail to comply with privacy laws. Our efforts to comply with privacy laws complicates our operations and adds to our compliance costs. A significant privacy breach or failure to comply with privacy laws might have a materially adverse impact on our reputation, business operations and our financial position or results of operations.

We experience cybersecurity incidents and might experience significant computer system compromises or data breaches. We and our external service providers use sophisticated computer systems to perform our business operations, such as the secure electronic transmission, processing, storage and hosting of sensitive information, including protected health information and other types of personal information, confidential financial information, proprietary information, and other sensitive information relating to our customers, company and workforce. Many of these systems have experienced and are subject to cybersecurity incidents, despite physical, technical and administrative security measures. Cyber incidents include actual or attempted unauthorized access, tampering, malware insertion, ransomware attacks or other system integrity events. The risk of cyber incidents may be increased while many of our personnel are working remotely due to the COVID-19 pandemic. A cybersecurity incident might involve a material data breach or other material impact to the integrity and operations of these computer systems, which might result in litigation or regulatory action, loss of customers or revenue, increased expense, any of which might have a materially adverse impact on our business operations, reputation and our financial position or results of operations.

Many of these systems have experienced and are subject to cybersecurity incidents, despite physical, technical and administrative security measures. ... The risk of cyber incidents may be increased while many of our personnel are working remotely due to the COVID-19 pandemic.
Banks and financial services generally have evolved over the years to become heavily data-driven, partially to predict consumer behavior but as well to detect and prevent fraud. These goals, plus a rising financial technology marketplace forcing innovation and collaboration, result in a highly integrated and connected industry with multiple players, including independent data aggregators, storing, analyzing and sharing consumers’ personal data with and for each other. The 10-Ks demonstrate that financial institutions’ reliance on each other for sound privacy and security practices, as well as the increased risk to personal data created by the interconnected industry, creates significant risks for investors.

But perhaps more than other industries, financial services providers are aware that trust plays a major role in consumers’ willingness to give them their business and their money. Financial services make significant and growing use of AI and robotics, mobile applications, and remote connectivity solutions, all of which increase the amount of personal data collected about consumers. As mobile devices — and the telecommunication networks on which they rely — become a primary vector for conducting lending, investing, deposits and payment transactions, financial services players see significant increase in cybersecurity and data leakage risks.

Also accustomed to being regulated, including for their privacy and security practices, financial services companies tend to disclose privacy risk as one of many regulatory concerns. Risks disclosed include GDPR and CCPA compliance obligations, but also risk of additional compliance costs, litigation and regulatory fines from “new and evolving data privacy laws in the U.S. and abroad.” This risk is heightened by inconsistency in these laws.

But perhaps more than other industries, financial services providers are aware that trust plays a major role in consumers’ willingness to give them their business and their money. Accordingly, reading carefully, it’s clear the role of data privacy and security failures as a brand risk is as strong with the financial services disclosures as with any other industry sector.

Similar to the retail sector, discussed below, financial services industries are heavily driven by customer behavior data. Interconnectivity and mobile banking have generated vast amounts of consumer data from which banks can gain insights. In their risk disclosures, some banks discussed the potential for privacy regulation to restrict their data analytics practices, which creates a risk to their operations.
JPMORGAN CHASE

As JPMorgan Chase’s interconnectivity with clients, customers and other external parties expands, JPMorgan Chase increasingly faces the risk of operational failure with respect to the systems of those parties. Security breaches affecting JPMorgan Chase’s clients or customers, system breakdowns or failures, security breaches or human error, or misconduct affecting other external parties, may require JPMorgan Chase to take steps to protect the integrity of its own operational systems or to safeguard confidential information, including restricting the access of customers to their accounts. These actions can increase JPMorgan Chase’s operational costs and potentially diminish customer satisfaction and confidence in JPMorgan Chase.

Furthermore, the widespread and expanding interconnectivity among financial institutions, central agents, CCPs, payment processors, securities exchanges, clearing houses and other financial market infrastructures increases the risk that an operational failure at one institution or entity may cause an industrywide operational failure that could materially affect JPMorgan Chase’s ability to conduct business.

In recent years, well-publicized allegations involving the misuse or inappropriate sharing of personal information have led to expanded governmental scrutiny of practices relating to the safeguarding of personal information and the use or sharing of personal data by companies in the U.S. and other countries. That scrutiny has, in some cases, resulted in and could, in the future, lead to the adoption of stricter laws and regulations relating to the use and sharing of personal information. These types of laws and regulations could prohibit or significantly restrict financial services firms such as JPMorgan Chase from sharing information among affiliates or with third parties, such as vendors, and thereby increase compliance costs or could restrict JPMorgan Chase’s use of personal data when developing or offering products or services to customers. These restrictions could also inhibit JPMorgan Chase’s development or marketing of certain products or services, or increase the costs of offering them to customers.
We rely on data to aggregate and assess our various risk exposures and business activities, and any issues with the quality or effectiveness of our data, including our aggregation, management and validation procedures could result in ineffective risk management practices, business decisions or customer service, inefficient use of resources, or inaccurate regulatory or other risk reporting.

We also use AI to help further inform our business decisions and risk management practices, but there is no assurance that artificial intelligence will appropriately or sufficiently replicate certain outcomes or accurately predict future events or exposures.

Wells Fargo
The top retail enterprises in the U.S. are principally domestic in their operations and are less accustomed to being regulated for their personal data practices than the financial and health services industries. Retailers are far less likely than companies in the other sectors we studied to mention the risk of international privacy regulatory compliance. Instead, their principal disclosed data risks relate to payment data, including the risk of reporting data breaches and compliance with PCI contracts and security standards.

The rise of comprehensive privacy laws, like the CCPA, is catching their attention, however. Some retailers disclosed the importance of personal data analysis to their business operations, particularly as retailers are increasingly forced to develop their internet presence and compete with other retailers online. Privacy laws pose a new risk to this industry sector, through regulatory enforcement actions, litigation in the wake of a data breach involving payment data or other PII, and customers choosing not to share or to delete their data. As one company noted, privacy regulations potentially create a risk to their ability to “obtain accurate and relevant data on guest preferences,” thereby posing a risk to their “pricing, promotion, inventory and other business strategies which are based on having sound data about consumer behavior and preferences.”

SURVEY SPOTLIGHT

TARGET

Our business has evolved from an in-store experience to interaction with guests across multiple channels (in-store, online, mobile, social media, voice assistant, and smart home devices, among others). Our guests are using those channels to shop with us and provide feedback and public commentary about our business. … We … need to collect accurate, relevant and usable guest data to personalize our offerings. …

A large part of our business is dependent on our ability to make trend-right decisions and effectively manage our inventory in a broad range of merchandise categories …. If we do not obtain accurate and relevant data on guest preferences, predict changing consumer tastes, preferences, spending patterns and other lifestyle decisions, emphasize the correct categories, implement competitive and effective pricing and promotion strategies, or personalize our offerings to our guests, we may experience lost sales, spoilage and increased inventory markdowns, which could adversely affect our results of operations by reducing our profitability. …

Complying with new data protection requirements, such as those imposed by the recently effective California privacy laws, may cause us to incur substantial costs, require changes to our business practices, limit our ability to obtain data used to provide differentiated guest experiences, and expose us to future litigation and regulatory risks, each of which could adversely affect our results of operations.
We accept payments using a variety of methods, including cash, checks, credit and debit cards, and our private label credit cards and gift cards, and we may offer new payment options over time, which may have information security risk implications. As a retailer accepting debit and credit cards for payment, we are subject to various industry data protection standards and protocols, such as payment network security operating guidelines and the PCI data security standards. … In certain circumstances, our contracts with payment card processors and payment card networks … generally require us to adhere to payment card network rules that could make us liable to payment card issuers and others if information in connection with payment cards and payment card transactions that we process is compromised, while liabilities could be substantial.

Walmart
One word for the insurance industry’s relation to privacy is “stable.” Similar to the health and financial services sectors, the insurance sector is familiar with being regulated for their data practices. Accordingly, companies in this sector appear less concerned about complying with new regulations because they perceive themselves as well structured to manage data privacy.

However, this industry is still concerned about cyberattacks and security breaches and what that could mean for their businesses, both in loss of reputation and in cost. Many companies in this sector mentioned the risk of fees, judgments or penalties stemming from a data breach. Some large, multinational corporations are concerned about the availability of cross-border transfers, but because this industry is largely a domestic industry, international privacy law compliance was not a commonly disclosed risk.

Compliance with new privacy and security laws, regulations and requirements may result in increased operating costs, and may constrain or require us to alter our business model or operations.

**SURVEY SPOTLIGHT**

**UNITED HEALTH**

Noncompliance or findings of noncompliance with applicable laws, regulations or requirements, or the occurrence of any privacy or security breach involving the misappropriation, loss or other unauthorized disclosure of protected personal information, whether by us or by one of our third-party service providers, could have a material adverse effect on our reputation and business and, among other consequences, could subject us to mandatory disclosure to the media, loss of existing or new customers, significant increases in the cost of managing and remediating privacy or security incidents and material fines, penalties and litigation awards.

Breaches of our security measures and the unauthorized dissemination of sensitive personal information, proprietary information or confidential information about us or our customers or other third parties, could expose our customers’ private information and our customers to the risk of financial or medical identity theft, or expose us or other third parties to a risk of loss or misuse of this information, result in litigation and potential liability, including regulatory penalties, for us, damage our brand and reputation, or otherwise harm our business.
There is a culture of compliance in the (health care) industry. They are used to being regulated and this makes for a relatively stable industry as compared to other, newer industries that are just now starting to be regulated. ... The insurance industry is slowly undergoing a transformation when it comes to data. They are starting to use data to help make more informed decisions when it comes to evaluating risk, and this could lead to a change in how the industry will view data privacy as risk.

*Insurance industry privacy counsel*
Public Companies Likely to Disclose Privacy as a Risk Factor

The IAPP and FTI Consulting’s 2020 “Privacy Governance Report” revealed at least half of publicly traded companies surveyed mention privacy-related risks in financial notices, disclosures, shareholder communications or annual reports. In these disclosures, 58% of respondents noted that both privacy law compliance and data breach risks are disclosed.