STATEMENT OF JAY CLINE
TO THE UNITED STATES SENATE COMMITTEE
ON BANKING, HOUSING AND URBAN AFFAIRS
ON PRIVACY RIGHTS AND DATA COLLECTION IN A DIGITAL ECONOMY

May 7, 2019

Chairman Crapo, Ranking Member Brown, and distinguished members of the Committee, I appreciate the opportunity to appear today as the Committee considers privacy rights and data collection in a digital economy. I am currently a Principal and the US Privacy and Consumer Protection Leader at PricewaterhouseCoopers LLP (PwC). I am appearing on my own behalf and not on behalf of PwC or any client. The views I express are my own.

Lessons learned from US financial institutions' GDPR experience, 2016-2019

My testimony today will examine the experience of US financial institutions (FIs) with the European Union (EU) General Data Protection Regulation (GDPR). It is an experience marked by large-scale technical and organizational change to afford new privacy rights to EU residents in an evolving regulatory environment. It is my hope that my testimony will be useful to the Committee as it considers the collection, use, and protection of personally identifiable information by financial regulators and private companies.

GDPR caused many US FIs operating in Europe to undertake their largest-scale privacy program initiatives in two decades. Beginning after the ratification of the GDPR in April 2016 and generally accelerating a year later, these initiatives often rivaled the scale of US FIs' earlier mobilizations to prepare for the Privacy Rule of the Gramm-Leach-Bliley Act (GLBA) and other related US data privacy laws and regulations. As a result, US FIs generally used all of the GDPR's two-year grace period to prepare for the law's "go live" date in May 2018.

Impact of GDPR requirements on US FIs

The GDPR introduced several new obligations on US FIs.

- *New requirements on data-subject rights* most affected retail banks and direct insurers -- because of their direct exposure to fulfilling data-subject requests (DSRs) -- and least affected commercial banks, re-insurers, payment-card companies, and asset-management companies that generally had indirect exposure to DSRs.
- *New requirements on data privacy program accountability* by comparison most affected larger, diversified groups of companies that had to allocate more resources to accommodate their business variations and least affected more homogenous FIs.

The effects of the GDPR requirements included increases in headcount, changes in information systems, and alterations in products and services.

The GDPR also introduced several new organizing principles to US FIs. Concepts such as 'personal' data including data indirectly identifiable to individuals, 'sensitive' personal data, 'pseudonymized' data, 'high-risk' data processing, 'large-scale' data processing, 'original purpose' of data collection, 'cross-border' data transfer, 'data controller', and 'data processor' materially affected the policy regimes of all US FIs operating in the EU.

The GDPR also introduced a new enforcement environment for US FIs. This environment resulted in new and uncertain risk exposures. In the United States, for example, class-action lawsuits related to the Telephone Consumer Privacy Act (TCPA) are a significant driver of data privacy-related economic risk for US FIs. The private right of action for GDPR-related issues, however, is a new and untested citizen-led enforcement channel in the EU that could have broader impact than the TCPA because of the broader scope of covered data. Moreover, the new powers of EU data-protection authorities (DPAs) to impose fines of up to four percent of annual global revenues has expanded the potential risk exposure of the largest corporations into the billion-dollar range for the first time. Similarly, the EU DPAs' power to issue injunctions to stop data processing that runs counter to the GDPR could have the result of ending revenue-generating commercial activities that depend on that data processing. As the GDPR and its enforcement regime influence how other jurisdictions in the US and around the world take their next steps on data privacy law and enforcement, US FIs operating globally are re-evaluating their approaches to privacy-risk management.

Challenges, insights, and questions

The US FI experience with addressing the GDPR can be grouped into three categories: top challenges, implementation insights, and unanswered questions.

<u>Seven GDPR implementation challenges for US FIs</u>

Financial institutions use personal data to provide most of their products and services. Whether to set up a bank or investment account, install a mobile application on a smartphone, underwrite an insurance policy, or process an insurance claim or payment-card transaction, data related to individuals are the linchpin for servicing these orders. As a result, the GDPR's impact on US FIs' handling of personal data was destined to have a widescale impact on operations. That impact tended to materialize in the following ways:

1. ***Completing a data inventory***. In order to comply with Article 30 of the GDPR requiring a 'record of processing' of all EU data, US FIs embarked on extensive projects to record details about hundreds and thousands of applications, databases, devices, and vendors that often operated in clusters independent of each other. Because no single technology on the market could do all of this automatically, these initiatives necessarily involved hundreds and thousands of labor hours answering data-inventory surveys and completing in-person interviews. To better automate this capability, many US FIs are exploring new technologies that rely to different degrees on 'machine learning' to scan and classify their data assets.

2. ***Operationalizing data-subject rights***. GDPR enhanced or created DSRs for EU residents to access, receive a copy of, correct, restrict processing of, or delete their data and to withdraw consent previously given to process their data. In the largest FIs, a single person's data could exist across dozens and even hundreds of systems often not synchronized with each other. Facing an uncertain volume of incoming DSRs after GDPR's effective date in May 2018 -- and lacking a single technology in the market to fully address this need -- US FIs developed predominantly manual processes to operationalize GDPR DSRs. To better automate this capability, many US FIs are exploring updating or enhancing workflow-software solutions.
3. ***Completing DPIAs***. GDPR introduced to US FIs a requirement to document a data-protection impact assessment (DPIA) of new technology change involving EU personal data and to remediate risks to the 'rights and freedoms' of individuals that are 'high' as defined and understood by EU DPAs.[1] Remediating risks could involve reducing the data collected or how long it was retained, for example. For large FIs, this could mean conducting dozens or even hundreds of these assessments and related remediation projects each year. To better automate this capability, many US FIs are exploring or enhancing workflow-software solutions.
4. ***Updating third-party contracts***. The GDPR required 'data controllers' to have contractual provisions holding their 'data processors' accountable to the relevant provisions of the GDPR. The newer DSRs and data-breach notification threshold were among the more important provisions many opted to add explicitly to their contract addendums and service-level agreements. For US FIs, the number of contracts needing updating could range from dozens to hundreds and even thousands. To better automate this capability, many US FIs are exploring workflow-software solutions that rely to different degrees on machine learning.
5. ***Appointing a DPO***. GDPR requires that organizations meeting certain conditions appoint a data protection officer (DPO), an 'independent' person with direct access to leadership. For large FIs, addressing this could involve a single, full-time position or multiple positions that were internal staff or an outsourced firm. The GDPR offers further practical advantages for placing these DPOs in the FI's 'main establishment' or main EU country of operations where they could more easily interact with their 'lead' local data protection authority (DPA). In the run-up to the May 2018 deadline for GDPR, demand for DPOs grew rapidly and the available supply of qualified candidates diminished, complicating US FIs' decisionmaking.
6. ***Preparing to notify breaches within 72 hours***. The GDPR echoed a requirement from a New York State Department of Financial Services cybersecurity regulation whereby companies that experienced a compromise of EU personal data must notify relevant regulators within 72 hours of becoming aware of it. For FIs headquartered in the United States but operating in Europe, this meant expanding their US breach-response capability into Europe -- including associated staff, technologies, and supporting vendor relationships. A further challenge was informational -- defining what could actually be known and reported

[1] See Article 29 Working Party WP247, *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, October 2017, for examples of these 'high-risk' criteria.

within a relatively short window of time during which forensics investigations would often still be in progress.

7. ***Engaging the "first line of defense."*** One of the most important, ongoing challenges for US FIs is to re-organize their data privacy organizations along the three 'lines of defense' in order to give scalable and sustainable effect to GDPR controls. Many implemented a model based on placing privacy representatives in the business operations of the first line; data privacy governance leaders in the second line; and an oversight role in the third line. Traditionally, privacy expertise in the FI sector had been concentrated in the second line of defense. Identifying and equipping privacy representatives in the first line, whose primary jobs and training had not historically been data privacy, remains a general challenge for all commercial sectors.

<u>Seven GDPR implementation insights for US FIs</u>

1. ***DSRs are not created equal****.* The GDPR provides for eight data-subject rights: to privacy notices, to data access, to data rectification, to objection to processing, to withdrawal of consent for processing, to objection to automated processing, to data erasure, and to data portability. For most US FIs, these were new requirements they were not previously subject to under US data privacy regulations such as the GLBA Privacy Rule. The DSRs in the latter Rule were limited to a right to opt out of marketing and a right to opt out of data sharing with affiliates. The implementation and exercise of these new GDPR rights varied:
    - The GDPR rights generally posing the most implementation challenges for US FIs were the rights to access and erasure. Fulfilling an access request could involve pulling information on an individual from dozens and even hundreds of structured databases and unstructured data stores -- but doing so in a timely manner would probably require configuring all of these systems to a single consumer-identity-management system. Fulfilling an erasure request could in turn require different erasure and redaction protocols for each of these systems.
    - When consumers exercised their GDPR rights after May 2018, those most exercised generally were the rights to access, erasure, and objection to use for marketing.
2. ***Erased doesn't mean forgotten***. The GDPR's right to erasure is parenthetically referred to in the regulation as the 'right to be forgotten', although in practice in the US financial industry, those two concepts may not be equivalent. The substantial number and scope of regulations and other obligations in the US financial industry requiring the collection and retention of personal data such as for fraud prevention, cybersecurity, anti-money laundering, terrorist watchlisting, and for other discovery or litigation-related purposes means that US FIs will limit or deny many requests for erasure. Moreover, for compliance purposes, US FIs tend to keep a log of completed erasure requests that retains basic contact information of the requestor.
3. ***DSRs benefit from strong authentication***. For individuals, the GDPR right of access could produce files containing many personal details. If these files were delivered to the wrong individual, their privacy would be exposed. To counter this risk of misdirected files, companies can and do ask for multiple pieces of personal information from DSR requesters

to first authenticate their identities before providing their requested files. A strong authentication process could also counter the risk of fraudulent DSR requests, which some US FIs experienced in the year since GDPR went into effect. A challenge for this approach, however, is fulfilling DSRs for individuals for whom companies do not keep enough information to authenticate at a strong level. For example, a name and an e-mail address may not be enough information to strongly authenticate.

4. ***The distinction between primary and secondary data controllers is important****.* The GDPR does not distinguish between 'primary' data controllers that maintain direct relationships with data subjects and 'secondary' data controllers that do not. But this distinction is useful in the insurance industry, for example, where direct insurers are positioned to provide privacy notices and data-breach notifications to data subjects and obtain consent and field DSRs from data subjects, whereby re-insurers are less well-positioned to do so.
5. ***Board visibility makes a difference***. The prospect of being exposed to a fine of four percent of global revenues motivated many companies to implement their GDPR programs by May 2018, but the lack of any enforcement action approaching that monetary level in the year since GDPR took effect has reduced the pressure for ongoing enhancement of privacy controls in some quarters. US FIs who routinized the reporting of their privacy program status to the Board or Audit Committee were more often successful in maintaining strong organizational support for GDPR during its first year of operation.
6. ***Data governance is critical for privacy's success***. The GDPR emphasizes the need to have strong controls for personal data throughout its lifecycle of collection, storage, use, disclosure, and deletion. Because personal data often moves horizontally across vertically structured financial institutions, there is a heightened need in the financial industry to formalize an approach to data governance. For this reason, some FIs have endowed data governance leaders with some data privacy responsibilities.
7. ***GDPR did not fully harmonize privacy regulation in Europe***. A benefit of the GDPR was to standardize many varying provisions in EU member states' data-protection laws, but substantial variations continue to exist. Accommodating regulatory variations generally increases the cost of compliance for FIs operating across multiple jurisdictions. To reduce their GDPR compliance and enforcement exposure, US FIs are finding it necessary to continue to track variations at the EU member-state level where DPAs take the lead on enforcement and where class-action lawsuits are adjudicated. Member states, for example, are taking different approaches to the derogations left to them in the GDPR, different interpretations of 'high risk' processing for DPIA purposes, and different enforcement priorities. The need to monitor these changes has tended to have a larger relative operational impact on smaller US FIs operating in Europe because of their generally smaller data privacy teams.

<u>Five unanswered questions for US FIs post GDPR</u>

As US FIs continue to absorb the GDPR into their daily operations and plan for the future, they tend to share five common questions they are in the process of answering:

1. ***Will the GDPR become the global data privacy standard?*** As US FIs operating internationally further automate their data privacy programs and capabilities, the cost of these enhancements is rising. Variances across jurisdictions regarding how these capabilities should be delivered to consumers -- such as the specific nature and scope of DSRs -- add to that cost. If GDPR DSRs will become the de facto global standard, it probably will make the most commercial sense for these multinationals to design their DSRs to be offered globally. If some GDPR DSRs won't become the global standard, however -- such as the GDPR's right to opt out of automated decisionmaking -- it would not make commercial sense to globalize those DSRs. Moreover, if GDPR's program accountability requirements become the global standard, it reduces the need and likelihood that the GLBA's right for customers to opt out of their non-public personal data being shared with affiliates of the FI will become a standard outside the United States. US FIs engaging in long-term, strategic planning for their data usage are needing to answer this question.
2. ***Will people increasingly exercise their privacy rights?*** Many US companies received under 100 GDPR DSRs in the year after GDPR went into effect, while some outliers fielded thousands of them. In some cases, US residents attempted to exercise GDPR rights. Companies receiving them had to decide whether to reject them on legal grounds or fulfill them in order to provide a positive consumer experience. Most US healthcare providers and insurers similarly receive fewer than 100 HIPAA DSRs each year. As the California Consumer Privacy Act (CCPA) brings to many US companies for the first time the rights to access and erasure and to opt out of selling data to third parties, questions many US privacy leaders are asking is whether their expected volume of DSRs will outstrip their generally manual processes for fulfilling DSRs, and whether residents outside California will attempt to exercise these rights in large numbers.
3. ***How can informed consent be facilitated in a blink?*** The sharp rise in the use of pop-up windows on mobile and stationary websites to capture user consent for cookies has slowed down the typical online customer experience to demonstrate compliance without offering an obvious material improvement in privacy protection. Corporate privacy leaders are looking for new models -- such as mobile apps that ask you if you want to enable that app tracking your device's geolocation or accessing your contacts -- that break down the privacy-consent process into quicker, more meaningful steps.
4. ***What pseudonymization protocol will stand the test of time?*** Effective pseudonymization can increase the ability to use and monetize data and create commercial innovation while also protecting individual privacy. Advances in data processing and artificial intelligence, however, are changing the threshold of what is identifiable data and how much has to be removed from a data set in order for it to be pseudonymized, anonymized, or de-identified. US privacy leaders are looking toward the 'statistical' method of de-identification described in the Health Insurance Portability and Accountability Act (HIPAA) as a potential answer to this question.
5. ***What is a high risk to privacy?*** Effectively functioning companies will allocate the most risk-management resources to address risks they determine are 'high' in their enterprise risk-management (ERM) programs. The concept of high risk embedded in the GDPR and interpreted in varying ways across EU member states diverges in many ways from the

concept of high risk provided for in different US data privacy laws. For example, the GDPR considers a person's status with regard to membership in a trade union as 'sensitive' data whose processing creates inherent high risk, while no US privacy law or regulation results in a similar determination. Conversely, US data-breach notification laws make the storage of Social Security Numbers an inherent high risk, but GDPR does not similarly classify the processing of EU social-insurance numbers. Similarly, EU DPAs have listed 'large-scale data processing' as a high-risk criterion that does not have an equivalent in US privacy regulations. Unless these concepts converge over time across jurisdictions, privacy risk management may need to be regionalized in several respects.

Looking ahead

The GDPR has caused US FIs to implement new ways for European residents to control their personal data. The GDPR's extraterritorial reach has in turn prompted other jurisdictions around the world to adopt its model that is centered on offering a set of data-subject rights and instituting programmatic controls. To plan for a future where consumers around the world may generally expect the core rights of access, deletion, and objection to marketing, many US FIs are redesigning their privacy organizational models and capabilities. Because of the relative newness of technologies designed to automate the fulfillment of privacy rights and the technical complexity of many FIs, a significant effort lies ahead of them in realizing these designs. A key factor in whether automation is needed or manual processes will continue to suffice is the degree to which consumers will increasingly demand these rights. As these factors converge, the highest level of privacy protection in the digital age will result when both companies and consumers exercise their roles to the fullest.