STRESS TESTING THE US PRIVACY FRAMEWORK

Two major planks of US privacy regulation, including controversial new broadband rules, are discussed by **AARON BURSTEIN** and **JOSHUA BERCU**

Two of the major developments in privacy over the past year highlight the unique system of privacy laws in the United States (US). The first is the EU-US Privacy Shield framework that the European Commission (EC) and the US government finalised in July 2016. Privacy Shield offers a simplified mechanism for companies to transfer personal data of European Union (EU) citizens to the US in a manner that satisfies the requirements of EU privacy laws. The second is the emergence of the Federal Communications Commission (FCC) as a key regulator of privacy and data security, particularly through a set of new privacy and data security rules it imposed on broadband internet access service providers ('broadband providers').

Privacy Shield and the FCC's rules are independent developments, but they illustrate the challenges that the US faces as privacy becomes an increasingly important issue for governments, consumers and international trade relationships. Privacy Shield demonstrates that US privacy law – and the web of US government agencies that handle privacy issues – can change in relatively short order to produce a unified response that meets complex challenges. The FCC's rules, however, demonstrate that the force of the shared principles underlying existing US privacy laws has limits. The FCC determined that broadband providers have "unique access to consumer data"[1] and used this finding to justify creating a distinct privacy regime for broadband providers that does not apply to other online actors.

OVERVIEW OF US PRIVACY LAWS

For much of the recent past, privacy law in the US has been treated as a set of mostly separate domains: the commercial realm, law enforcement, national security, and civil government data collection and use. Within the commercial realm, the US lacks a comprehensive privacy law that is akin to the EU's Data Protection Directive of 1995 and the member state laws that implement it. The Obama administration has described the US privacy framework as "flexible and effectiv[e]", resting on "industry best practices, FTC [Federal Trade Commission] enforcement, and a network of chief privacy officers", as well as federal "data privacy statutes [that] apply only to specific sectors, such as healthcare, education, communications, and financial services..."[2] Proponents of this basic consumer privacy framework – FTC authority across broad swathes of the economy, in addition to sector-specific laws – have said it provides a good deal of flexibility and reserves more prescriptive rules only for personal data that is particularly sensitive (e.g. health and financial information), or settings in which the use of personal data could be particularly harmful to individuals (e.g. for determining creditworthiness).

Critics have argued that the current framework fails to provide clear rules of the road outside of the sector-specific laws. Others have argued that changes in technology and markets have eroded the lines that divide industries regulated by sector-specific privacy laws from the rest of the economy. For example, health apps and wearable health devices generate personal health information that generally is not covered by HIPAA, the federal health information privacy law, even though the information may be the same as what doctors – who are covered by HIPAA – collect. The result is a system

that is difficult for companies and government agencies themselves to navigate for purposes of enforcement, compliance and policymaking.

If anything, this may understate how much the privacy landscape is changing. The separation of privacy into commercial, law enforcement, intelligence, and civil government domains looks increasingly questionable in practice. High-profile policy issues, including electronic surveillance law reforms, law enforcement assistance requirements, and encryption policy, routinely produce complex privacy questions that require input from multiple governmental and private sector stakeholders to answer.

PRIVACY SHIELD: A SUCCESSFUL RESPONSE TO A SERIOUS PRIVACY CHALLENGE

The most severe test of the US privacy framework in recent years is the aftermath of former National Security Agency contractor Edward Snowden's 2013 revelations of US signals intelligence collection activities. A focal point for the reaction to Snowden in Europe was the US-EU Safe Harbor framework, a voluntary data transfer framework that had been in place since 2000. The challenge to Safe Harbor became a crisis in October 2015, when the Court of Justice for the European Union struck down the EC adequacy decision that underlay Safe Harbor. The US and the EC met this post-Snowden challenge by finalising Safe Harbor's successor, the EU-US Privacy Shield Framework, in July 2016.

On the US side, this achievement required an unprecedented whole-of-government approach to overcome the institutional and legal barriers that separate commercial, law enforcement, and national security privacy domains. Privacy Shield also accentuates the FTC's role at the apex of consumer privacy enforcement agencies.

FROM SAFE HARBOR TO PRIVACY SHIELD

To appreciate the significance of the US approach reflected in Privacy Shield, it helps to understand the origins and purpose of its predecessor, Safe Harbor. Safe Harbor provided a way for companies doing business across the Atlantic to comply with the 'adequacy' requirement of EU privacy law, which comes from the 1995 Data Protection Directive, and which generally prohibits personal data transfers from the EU to countries that have not been found by the EC to provide an 'adequate' level of data protection. The US did not seek an adequacy determination, and by 1999 it became clear that the lack of adequacy (and the limitations on other grounds for legally transferring data from the EU to the US) posed a threat to US and European economic interests.

Safe Harbor provided a way to transfer data to the US with the assurance of adequate data protections even in the absence of a general adequacy determination for the US. At its core, Safe Harbor consisted of a set of data protection principles that companies could commit to follow. These commitments were enforceable by the FTC (and, for air carriers, by the US Department of Transportation). In July 2000, the EC determined that the Safe Harbor principles, together with FTC enforcement and the US Department of Commerce's oversight of Safe Harbor registrations, made Safe Harbor an 'adequate' system of data protection. This finding allowed companies that participated in Safe Harbor to transfer personal data from the EU.

Although Safe Harbor had its critics, only after the Snowden revelations did their criticisms gain sustained traction. In November 2013, the European Commission (EC) issued a list of 13 demands to change the terms of Safe Harbor, including changes to US surveillance practices. These demands became the basis for negotiations between the EC and the US Department of Commerce.

In the meantime, a lawsuit filed in Ireland against Facebook was making its way to the Court of Justice for the European Union (CJEU). The plaintiff in this case, Max Schrems, alleged that government access to personal data transferred to the US under Safe Harbor was subject to mass and indiscriminate government surveillance and therefore inconsistent with the fundamental right of data protection as defined under EU law.

In October 2015, in Schrems vs Facebook, the CJEU found merit in these claims and effectively killed Safe Harbor. The Schrems court did not hold that the Safe Harbor principles were insufficient, nor did it pass judgment on US surveillance (or commercial) practices. Instead, the CJEU held that the EC's Safe Harbor adequacy decision did not assess government access to consumer information, including any governmental privacy intrusions, and thus could not guarantee that data transferred under Safe Harbor receives adequate protections.

Still, the Schrems judgment posed an immediate challenge to the transatlantic economy. About 4,400 companies had signed up for Safe Harbor and relied on it to transfer data from Europe to the US. Unless they had alternative arrangements in place, those companies faced the risk of enforcement actions by European data authorities and the possibility of the suspension of data transfers.

WHAT PRIVACY SHIELD SAYS ABOUT THE US PRIVACY FRAMEWORK

The looming shadow of this possibility had stimulated a US government-wide response to the EC's Safe Harbor demands in 2013. Part of this response led to consequences for companies, which must meet more stringent standards under Privacy Shield than under Safe Harbor. For example, Privacy Shield imposes stricter accountability requirements for 'onward transfers' from a Privacy Shield company to a third party.

The more remarkable differences between Privacy Shield and Safe Harbor lie in the roles that US government agencies play in the new framework. Although Safe Harbor and Privacy Shield both contain derogations for "national security, public interest, or law enforcement" purposes, Privacy Shield includes detailed statements about safeguards that apply in these contexts under US law and policy. Specifically, Privacy Shield includes a letter from the Office of the Director of National Intelligence that explains the privacy and civil liberties protections that apply to the US intelligence community's signals intelligence activities, a commitment from Secretary of State John Kerry to provide an ombudsperson to handle inquiries from EU national authorities about the handling of personal data transferred under Privacy Shield, and a letter from the Department of Justice describing the privacy and civil liberties protections that apply to US criminal investigations. This whole-of-government effort is a sharp contrast to the Safe Harbor framework, which had no statements from US officials on intelligence or law enforcement matters.

On the commercial front, Privacy Shield spends much less space explaining the sector-specific privacy laws that govern commercial data practices in the US. Whereas online privacy enforcement was in its infancy when Safe Harbor was completed – the FTC's letter notes that the FTC brought its first online privacy case under FTC Act Section 5 in 1999 – the field has become far more mature. The FTC's letter in Privacy Shield states that the FTC brought nearly 40 Safe Harbor-related enforcement

actions and nearly 500 privacy-related cases in total,[3] engages in active order monitoring, and has obtained civil penalties from companies that apparently violated the FTC privacy or data security order issued against them.

Some important industry sectors are not eligible for Privacy Shield because they are exempt from FTC enforcement authority, including banks and telecoms common carriers.[4] But the picture that emerges from the FTC's submission to Privacy Shield is one of an agency that has broad authority, which it has used consistently and effectively to enforce consumer privacy rights.

HOW THE FCC'S ROLE AS A PRIVACY REGULATOR TESTS THE FRAMEWORK

While US government officials have touted the success of the FTC's approach to privacy abroad, a separate agency, the FCC, has emerged as a key and somewhat controversial regulator in the realm of US privacy and data security. Telecoms carriers, which now include broadband providers, are squarely under the FCC's regulatory authority, but 'edge' service providers – social networks, email services, and other online services – are not. The FCC approved new privacy and data security rules for broadband providers that are largely premised on the notion that broadband providers are uniquely situated compared with providers of other online services – a notion that the broadband industry has strenuously rejected.

FROM CPNI TO PII AND FROM TELECOMS TO BROADBAND

Privacy is not a new issue for the FCC – it has long imposed privacy and data security restrictions on telecoms carriers. In the Telecommunications Act of 1996, the US Congress set out a framework to cover carriers' protection and use of customer information, affording the most stringent protections to 'customer proprietary network information' or CPNI. This includes information related to a customer's use of a telecoms service such as the phone numbers called by a customer; the frequency, duration, timing and location of such calls; and any services purchased by the customer, such as call waiting. The FCC first implemented the statutory framework through rules in 1998. It since has amended the rules from time to time, with significant amendments in 2007 to address concerns about 'pretexting', which is the practice of pretending to be a particular customer or other authorised person to obtain access to the customer's call details or other private communications records.

Until recently, the FCC's privacy rules and enforcement activity focused on voice telephone service providers and their protection and use of CPNI. The FCC did not generally focus on other categories of customers' personal information (general, personally identifiable information, or PII). In the past two years, however, the FCC has expanded its privacy focus and role through two significant actions.

First, in October 2014, the FCC embraced new legal theories under which it can address carriers' practices involving information significantly broader than CPNI, including virtually any personal information about customers. Specifically, the FCC asserted that while the relevant statute imposed specific obligations for the protection and use of CPNI, the statute's reference to "a duty to protect the confidentiality of proprietary information of, and relating to ... customers"[5] indicated that the statute applies to a broader category of information – 'customer proprietary information'. The FCC deemed this class to include information that customers expect their carriers will keep private, including but not limited to CPNI and personally identifiable information.

The FCC also claimed that it could address data security practices, including misrepresentations about practices, through its authority to ensure that carriers' practices are "just and reasonable". It has since brought privacy and data security actions against major carriers and a cable company, and cited its new legal theories in other proceedings.

Second, in February 2015, the FCC altered the regulatory classification of broadband internet access services, placing such services within the statutory framework for telecoms carriers. Although the FCC's stated goal was to establish so-called open internet or net neutrality rules, the decision had implications for privacy by subjecting broadband to the CPNI framework.[6] The FCC's existing voice-centric CPNI rules, however, cannot be easily mapped onto broadband services. So the FCC began a proceeding to establish new privacy and data security rules for broadband providers.

FTC VS AT&T MOBILITY: CEMENTING THE FCC AS A PRIVACY REGULATOR?

A court decision in 2016 further complicates the US privacy framework, with significant implications for the FTC's and FCC's respective roles in regulating the privacy practices of telecoms service providers.

On 29 August, a panel of the US Court of Appeals for the Ninth Circuit held that the common carrier exemption to the FTC's general authority applies to any entity that has common carrier status, rejecting the FTC's claims that the exemption is narrow and applies only to common carrier activities. The case, which arose from the FTC's challenge to certain contracting and advertising practices connected to AT&T's 'unlimited' mobile data plans, leaves the scope of the FTC's authority uncertain.

Under the decision, it is clear that an entity with common carrier status is categorically exempt from the FTC's enforcement authority, regardless of what non-common carrier services (e.g. home automation services) such entity is providing, at least in the states covered by the Ninth Circuit. But it is unclear whether separate but related corporate entities, such as a wholly-owned non-common carrier subsidiary, are also exempt.

Although the court's decision had no legal impact on the FCC's authority, it could affect how the FCC decides to assert its role as a privacy regulator in light of any perceived regulatory gaps. When the FCC reclassified broadband service, it was understood that this removed the FTC's authority over broadband services. But FTC vs AT&T Mobility raised the question of whether the FTC ever had authority over certain broadband providers – namely those that also provided a traditional common carrier service like voice telephony. Further, it indicates the FTC lacks authority over broadband providers' non-common carrier activities – authority which the FTC asserted it had retained even after the FCC's reclassification.

The FTC has petitioned for a rehearing of FTC vs AT&T Mobility by the full Ninth Circuit. Appeal to the Supreme Court remains an option, as does the possibility of a legislative fix.

WHAT THE BROADBAND PRIVACY RULES SAY ABOUT THE US PRIVACY FRAMEWORK

In early 2016, the FCC proposed new privacy requirements for broadband providers. The FCC's proposed rules combined the FCC's historical approach to the protection and use of CPNI with the agency's more recent legal theories regarding its authority to address information practices with respect to any customer information. The result was a prescriptive and restrictive privacy framework that contrasted sharply with the FTC's more flexible approach. For instance, the FCC's proposed rules would have required a broadband provider to obtain a customer's opt-in consent before using or sharing any of the customer's personal information or CPNI, except in certain limited circumstances.[7]

In contrast, the FTC generally requires opt-in approval before using or sharing sensitive personal information, a point that FTC staff made in comments to the FCC. According to the FTC staff, an approach that treats sensitive and non-sensitive data the same does not reflect consumers' expectations and, as a result, "could hamper beneficial uses of data that consumers may prefer, while failing to protect against practices that are more likely to be unwanted and potentially harmful".[8] Moreover, the FTC staff indicated that "impos[ing] a number of specific requirements on the provision of [broadband] services that would not generally apply to other services that collect and use significant amounts of consumer data" produces an "outcome [that] is not optimal".

Proponents of the FCC's proposal argued that broadband providers are 'gatekeepers' to the internet, and consumers have no choice but to share their information with them. They argued further that a broadband provider has no way of knowing whether information that traverses its network, such as what websites a customer visits, is sensitive. They claimed, therefore, that broadband providers must treat all information they can collect from and about customers as sensitive.

The broadband industry had argued that broadband providers lack unique or comprehensive visibility into customers' traffic and should be regulated the same way as other internet ecosystem players. This argument was based on the rise of encryption, virtual private networks, and consumers' reliance on multiple broadband providers (e.g. home, mobile, office, and public WiFi), all of which mean that other online services (e.g. social networks, email providers, and ad networks) have access to at least as much commercially valuable data as broadband providers; but these other services still would be subject to a less stringent regime. Broadband firms claimed further that restrictive privacy rules will inhibit their ability to compete in the online advertising market, where they are new entrants challenging dominant online providers. Industry also argued that the FCC's approach, including its application to information beyond CPNI, would exceed the agency's legal authority. Given their policy and legal concerns, broadband providers urged the FCC to adopt an approach consistent with that of the FTC.

Several groups have suggested Congress should extend the FCC's approach to all online services.

On 27 October 27 2016, by a 3-2 vote along party lines, the FCC approved broadband privacy rules that bear a closer resemblance to the FTC's framework than the FCC's initial proposal but that still depart from the FTC's framework in some significant ways. Specifically, similar to the FTC's approach, the final rules establish a customer approval regime that distinguishes between sensitive and non-sensitive customer information, generally requiring a customer's opt-in consent only for the use or disclosure of sensitive information.[9] But the FCC's rules categorise a broader range of information as 'sensitive' than the FTC does under its framework. Most notably, 'web browsing history' – including the domain names with which a customer communicates[10] – is deemed sensitive under the FCC's final rules but not under the FTC's framework.

Thus, the FCC's final rules permit broadband providers to engage in advertising and other activities based on web browsing information that they collect through the provision of broadband service, albeit pursuant to a customer's opt-in consent. In contrast, companies subject to the FTC's jurisdiction can continue to conduct similar activities without necessarily obtaining consumers' opt-in consent.

The exact implications of the FCC's departure from the FTC's approach remain to be seen. For broadband providers, in the opinion of dissenting Republican FCC commissioner Michael O'Rielly, the end result is "the lost opportunity and revenues for broadband providers precluded from competing against internet companies in the online advertising space[.]" For others in the internet ecosystem, the FCC's rules could set a new baseline that privacy advocates ask the FTC, Congress, and states to apply more broadly. In fact, several groups already have explicitly suggested Congress should now extend the FCC's approach to all online services.[11]

Ultimately, whether these developments will lead Congress, or an FCC led by an appointee of President-Elect Donald Trump, to consider seriously changing basic elements of the US consumer privacy framework – something it has long resisted doing – warrants close attention in the months ahead. For instance, a Republican-led FCC could revise or eliminate the new rules. One thing is clear: absent congressional action, the sector-specific privacy framework in the US will continue to face new challenges as evolving technologies and business models become more data-intensive and regulators jockey for a position in leading policy and law enforcement responses.

AARON BURSTEIN *and* ***JOSHUA BERCU*** *are attorneys at Wilkinson Barker Knauer, a Washington, DC law firm that focuses on telecoms, privacy, intellectual property and energy. This article does not constitute legal advice.*

REFERENCES **1** FCC (2016). Protecting the privacy of customers of broadband and other telecommunications services. Report and Order, WC Docket No. 16-106. fcc.us/1N6BNyI **2** White House (2012). Consumer data privacy in a networked world. bit.ly/1FQW1XF **3** This total appears to include FTC actions under Section 5, the Do Not Call Rule, the Fair Credit Reporting Act, and other specific privacy laws, and spans a timeframe that goes further into the past than Safe Harbor's beginning in 2000. **4** Privacy Shield annex at 61 (FTC letter). Whether the common carrier exemption to the FTC's enforcement authority restricts the FTC from addressing non-common carrier practices of a common carrier recently was addressed by a US appellate court. This significant decision is discussed in the panel on p20. **5** See: 47 US Code § 222 – Privacy of customer information. bit.ly/2gEyXqw **6** At the time, it was commonly understood that the FCC's decision removed broadband providers from the FTC's privacy and data security jurisdiction. The court case discussed on p20, however, indicates that at least certain broadband providers may never have been within the FTC's privacy and data security jurisdiction, irrespective of the FCC's reclassification decision. **7** The FCC's proposal also would have imposed certain transparency, data security, and breach notification requirements, which in many ways depart from the rules under which other entities are subject. **8** Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission to the Federal Communications Commission, In the matter of protecting the privacy of customers of broadband and other telecommunications services, WC Docket No. 16-106 (27 May 2016). **9** Privacy Report and Order, paras 177-195. The final rules permit providers to use non-sensitive information on an opt-out basis, and providers may also infer consent to use information or disclose information for a narrow set of purposes (e.g. providing service, protecting a carrier's rights or property, and limited first-party marketing). **10** Privacy Report and Order, paras 183-185. **11** See: Americans win significant broadband privacy rights in historic FCC decision. Center for Digital Democracy 27 October 2016. bit.ly/2hxEm75 / Consumer Watchdog welcomes FCC's new broadband privacy rules passed on 3-to-2 vote. Consumer Watchdog, 27 October 2016. bit.ly/2hoKuOJ