Strengthening international ties

Can support increased convergence of privacy regimes

The internet has become today's global trade route, and personal data is one of its major currencies.[1] The growth in the digital economy is impressive. One study found that economic activity taking place over the internet is growing at 10% per year within the G-20 group of nations.[2] In the United States alone, one estimate found that companies exported nearly $360 billion in digitally deliverable services in 2014.[3] The digital economy now drives countless aspects of the world economy.

Much of this economic activity depends on exchanges of personal information and that makes appropriate privacy and security protections essential. The need for extensive information exchanges also means that minimizing barriers to the transfer of information across borders is important to economic growth. Given the expected increase in the size and scope of the digital economy as well as changes in technology that make data collection, analysis and sharing practices easy and seamless, creating convergence and synergy between these two imperatives will become increasingly important.

As practitioners in this area in the U.S. and around the world, it is our job to be open and honest about our different nationally based approaches to privacy; to work together to create practical and executable solutions to support international data transfers such as the Privacy Shield; to find areas of commonality in what will continue to be a constantly changing field; and to look around the corner to anticipate the upcoming challenges, such as the Internet of Things and Big Data.

This article addresses these four topics. Section II provides a brief overview of how privacy enforcement works in the U.S. Section III focuses on the importance of transatlantic data flows and how Privacy Shield will have an important, positive effect on protecting Europeans' privacy. Section IV discusses the European Union's (EU) newly approved General Data Protection Regulation (GDPR) and some of the similarities between the GDPR and the U.S. approach to privacy regulation. Finally, Section V discusses the Internet of Things and Big Data, two innovations that will require new and hard thinking by privacy practitioners around the world.

U.S. privacy enforcement

To the frustration of many of my European colleagues, the U.S. does not have a single law that details the privacy protections provided to individuals. Instead, the U.S. has a variety of constitutional, federal and state laws that all play an important role in protecting the privacy and security of individuals' information. The U.S. Constitution provides protection against unwarranted government intrusion[4] and we have statutory restrictions on law enforcement access and intelligence surveillance. U.S. laws also are specifically designed to protect information about children,[5] financial information,[6] medical data,[7] student data,[8] and information used to make

decisions about consumers' credit, insurance, employment and housing.[9] Various federal agencies, including the Federal Trade Commission (FTC), have brought hundreds of enforcement actions under these specific laws. Layered on top of these specific laws – and filling many of the gaps between them – is the FTC's authority to enforce its broad and remedial statute that prohibits 'unfair or deceptive acts or practices in or affecting commerce.'[10] Under its 'unfair and deceptive practices' authority, the FTC has brought an additional 100 privacy and data security enforcement actions against companies for failing to meet consumer protection standards.[11]

The FTC generally targets privacy and data security practices that cause harm to consumers. But the Commission has a broad notion of harm. It includes financial harm, for sure, but it also includes, for instance, inappropriate collection of information on consumers' mobile devices,[12] unwarranted intrusions into private spaces,[13] the exposure of health and other sensitive information,[14] the exposure of previously confidential information about individuals' networks of friends and acquaintances and providing sensitive information to third parties who in turn victimize consumers.[15]

The FTC has taken action against some of the biggest names on the internet – including Facebook,[16] Google,[17] MySpace[18] and Twitter[19] – as well as many smaller players, for deceiving consumers about their data practices or using consumers' data in an unfair manner. Through its enforcement of privacy and data security law, the Commission has secured millions of dollars in penalties and restitution for consumers.[20] And the Commission has placed numerous companies under 20-year orders with robust injunctive provisions relating to their privacy and data security practices.

Of course, the FTC does not do this work alone. Other federal regulators have an important role in privacy and data security with respect to health care providers and hospitals,[21] banks and depository institutions[22] and common carriers.[23] Recently, federal agencies regulating these institutions have adopted more aggressive enforcement and regulatory positions. The Federal Communication Commission's (FCC) draft privacy rule for internet service providers is the most recent – and perhaps interesting – example.[24]

Within the U.S., the state governments also play a vital and active role in advancing consumer privacy and data security. Last year, approximately 60 new privacy laws were passed at the state level in

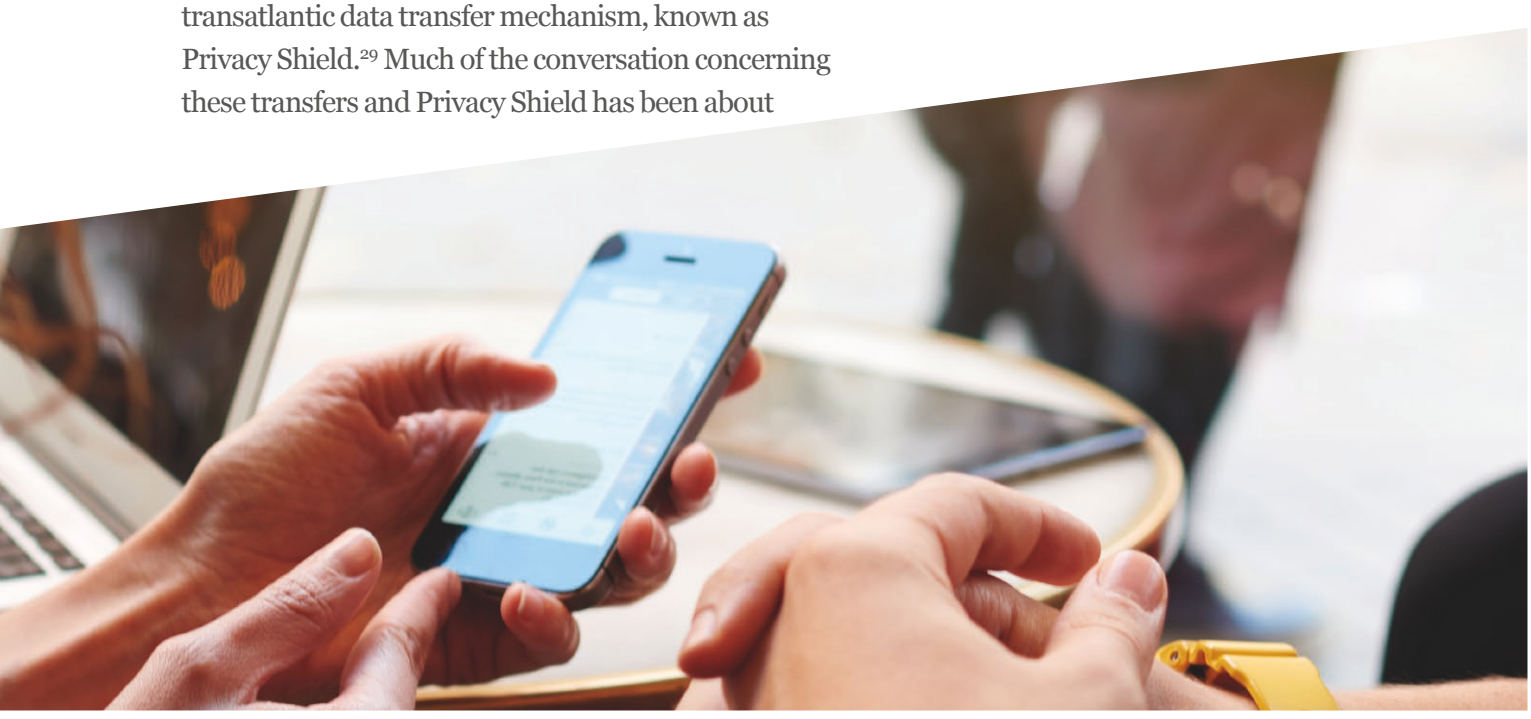
the U.S. State privacy laws range from limiting employers' ability to view their employees' social network accounts[25] and prohibiting employers and insurers from using information about certain medical conditions,[26] to requiring companies to notify consumers when they suffer a security breach involving personal information.[27] And the State Attorneys General are active enforcers of these laws.

Yet the FTC, with its broad authority under Section 5 of the Federal Trade Commission Act,[28] will be an increasingly important force as technology develops and as the silos that sector-specific laws are built around begin to crumble. The FTC's net of protection can capture problematic practices that fall through these cracks.

Privacy shield

Most recently, the U.S. approach to privacy has been the subject of significant debate in the context of discussions about the development of a new transatlantic data transfer mechanism, known as Privacy Shield.[29] Much of the conversation concerning these transfers and Privacy Shield has been about whether European courts, Member States, and data protection authorities will find the protections surrounding these data transfers to be adequate.

First, I would offer a bit of context. As discussed in the introduction, data is the life-blood of an ever-growing portion of the world the economy in and between the U.S. and Europe. We also are seeing significant data flows between countries, especially between the U.S. and EU. Transatlantic data flows between the U.S. and EU are the highest in the world, 50% higher than data flows between the U.S. and Asia, and almost double the data flows between the U.S. and Latin America.[30] Beginning in 2000, a framework known as the U.S.-EU Safe Harbor[31] provided a mechanism that allowed personal data from the EU to be transferred to the US. Although there were other ways to transfer data, Safe Harbor became the 'go to' solution. As of last year, 4,500 companies had voluntarily joined the program.[32]



All of this came crashing down with Edward Snowden's release of classified documents showing the extent of U.S. intelligence and law enforcement agencies' access to personal data in the hands of U.S. companies. Many European citizens and policymakers were furious, and the European Commission sharply questioned whether Safe Harbor was sufficient to protect European citizens. Thus began two years of negotiations over a new data transfer mechanism. These negotiations became even more urgent last October, when the European Court of Justice struck down Safe Harbor over concerns about intelligence surveillance.[33] Out of this complex and emotional web, Privacy Shield was born.

On national security issues, Privacy Shield is strong and clear about data protection in the U.S. and goes further than Safe Harbor. Privacy Shield explains how laws and Presidential Orders in the U.S. – including the newly adopted Judicial Redress Act,[34] the USA Freedom Act[35] and Presidential Policy Directive 28[36] – all set new limits on signals intelligence collection and give Europeans access to U.S. courts. Layered on top of these protections is a new ombudsperson within the State Department to whom data protection authorities can submit requests on behalf of individual European citizens about U.S. signals intelligence practices.[37] The ombudsperson will only receive requests from European citizens, and not from citizens of any other region or – perhaps most significantly – from U.S. citizens.[38]

Privacy Shield also goes further than Safe Harbor on the commercial side. As with Safe Harbor, companies that voluntarily agree to join Privacy Shield must obtain consent from Europeans before they share data with third parties, including affirmative express consent to share sensitive data such as health information, and they must allow Europeans to access, correct, or delete their transferred data.[39] In addition, Privacy Shield member companies will have to ensure through contracts that their business partners who receive information about Europeans can live up to all of these principles, too.[40] And Privacy Shield companies will have new, ongoing obligations to oversee the processing activities of their agents.

Privacy Shield also beefs up enforcement and consumer recourse. The Commission brought nearly 40 cases in the past five years against companies that violated Safe Harbor principles or misrepresented their participation in the program.[41] Under Privacy Shield, some of these violations might be detected and stopped before an enforcement action becomes necessary because the U.S. Department of Commerce will be required to closely monitor Privacy Shield registrations and participation.[42] At the same time, European citizens can choose to bring complaints about violations of the principles directly to the company, to the European data protection authorities, or to an independent entity designated to resolve disputes. If none of these entities satisfies the consumer, then she can choose to go to court or to arbitration, the results of which will be binding on the company.

For all of these reasons, I believe that Privacy Shield significantly strengthens Europeans' privacy rights, and should be deemed adequate by the EU Member States, the European Commission and the courts.

US-EU parallels under the general Data Protection regulation

With all that has been happening with Privacy Shield, I feel that the other significant development in transatlantic data flows has been a bit neglected, at least in many discussions in the U.S. Of course, I am referring to the GDPR,[43] which was recently adopted by the European Parliament.

One of the focuses of the GDPR is 'setting global data protection standards.'[44] But what I find most interesting is the way in which some of the GDPR's requirements have found inspiration in the robust privacy laws and policies in the U.S.

Data security

Data security is one example. The standard that the FTC enforces in data security cases is reasonable security. Integral to the idea of reasonable security is that it must be a continuing process. Risk assessments, identifying and patching vulnerabilities, training employees to handle personal information appropriately, and employing reasonable technical security measures are all parts of this process.

The GDPR – like the Data Protection Directive before it – incorporates a risk-based data security requirement.[45] Importantly, the GDPR adds the word 'ongoing' to its requirements that data controllers and processors maintain the security of their personal data processing systems.[46]

This additional word suggests alignment with the FTC's view that data security must be a continuous process. In addition, the GDPR lists steps that companies should include in their 'technical and organizational' measures, including the use of encryption and de-identification, as well as testing their security measures and addressing vulnerabilities that such testing uncovers.[47] The FTC has recommended these steps, among others, as part of its recent guidance to companies, while also emphasizing that decisions about what is reasonable in a given case will be fact-specific.[48]

Security Breach Notifications

Closely related to data security provisions are security breach notifications. In the U.S., breach notification laws have become nearly ubiquitous since California passed the first general breach notification law in 2002. Before the GDPR, however, breach notification in Europe was required only in limited circumstance, such as when communications service providers suffered a breach.[49] That will now change. The GDPR, once implemented, will require a data controller to report a breach to the relevant data protection authority.

Also, the GDPR qualifies data controllers' duty to notify supervisory authorities with a risk-based standard. Specifically, notification is not necessary if the breach is 'unlikely to result in a risk to the rights of natural persons.'[50] Moreover, notification to individual data subjects is necessary only when there is a 'high risk' to individual rights and freedoms.[51] Many of the U.S. state laws also include similar risk-based triggers that limit the circumstances under which notification is needed, and many of them exempt encrypted data from the duty to notify.

However, the notice processes of the U.S. and EU regimes will not fully overlap. The notification timeline under the GDPR, for instance, is much more aggressive than it is under U.S. state laws. Rather than requiring expedient notice without unreasonable delay, which is the standard in many U.S. state laws, the GDPR requires notification to the data protection authorities generally within 72 hours.[52] That may be problematic, especially if law enforcement is trying to investigate a significant ongoing criminal hack.

There are numerous other parallels between the U.S. privacy regime and the GDPR, including protections for children, privacy by design, transparency requirements, and principles around de-identification of data. We should be encouraged that on these many substantive points, our two regimes are converging.

Right to be forgotten

But, in some instances, the provisions of U.S. and European law set up areas of conflict. This is the case with the right to be forgotten.

The GDPR enshrines the Right to be Forgotten (Right to Erasure) in Article 17.[53] According to the GDPR, a controller must erase personal data without undue delay under certain circumstances, such as when the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed. And, like other provisions in the GDPR, the scope of the right to be forgotten does not appear to be limited to European territory. Indeed, the Article 29 Working Party had already interpreted the Right to be Forgotten in the Google Spain[54] decision to require that takedowns have global effect, on the grounds that viewing information that an individual considers irrelevant is an infringement of her right to privacy, no matter where the information is viewed.[55] Such broad interpretations have raised questions about the balance between the right to be forgotten and the extent to which orders to comply with takedown requests are enforceable outside of the EU. I expect those questions to remain prominent under the GDPR and that they may run up against First Amendment safeguards in the U.S. that protect speech.

Looking around the corner to anticipate upcoming challenges

In addition to nationally based differences in existing privacy regimes, changes in technology that make data collection, analysis, and sharing practices easy and seamless, will increasingly put pressure on our regulatory and compliance mechanisms. The Internet of Things and Big Data will require new thinking and new approaches to privacy. How nations and privacy professionals respond to these technological changes – whether through legislation, legal challenges, or private contracts – ultimately may cause greater convergence or divergence in our privacy regimes, impacting the ability to transfer data across borders and the future interconnectedness of the digital economy.

We are connecting nearly everything these days to the internet – from cars and buildings to clothing and light bulbs. The pace and scale of these changes is breathtaking. Cisco reports that there are 25 billion networked devices in the world today and predicts that there will be 50 billion by 2020.[56] Sensors in these devices, along with our smartphones, tablets, and computers, generate twice as much data today as they did two years ago, and this trend is expected to continue.

The Internet of Things,[57] promises not only to make our lives more convenient and efficient, but also to offer insights that could help U.S. solve some of society's most pressing problems. This is due not only to connected devices themselves, but also to the data that they generate. Data from wearable fitness devices could help each of U.S. get motivated to eat better or exercise more, while also providing important information to health researchers. Data from connected cars might help U.S. find a quicker route to our destination, and shed light on how traffic engineers should design highways to minimize traffic delays. And when teachers use tablets and apps in their classrooms, they can expose their students to challenges and experiences that are individually tailored while, at the same time, giving educators and researchers greater insight into what works – and doesn't work – in education.

So a great deal rides on data – and not just any kind of data, but personal data. This means that a great deal also rides on how we protect this data. Protecting individual privacy and keeping data secure are integral to the success of the data-driven economy because they are essential to earning and keeping consumers' trust.

Protecting consumers' privacy within the borders of one country, with its own legal framework and traditions, is a vast undertaking, particularly when technologies and business models are rapidly changing. Providing effective consumer protections in a world of global services and personal data flows is even more challenging – but also essential to our growing global economy.

While we likely won't see complete convergence in the various privacy regimes around the globe, we are beginning to see some evidence of it. The Judicial Redress Act demonstrates that U.S. policymakers are responsive to EU citizens' concerns about access

to U.S. courts. Privacy Shield recognizes that there are significant areas of overlap between the U.S. and EU approaches, and creates a bridge over other key gaps. The GDPR demonstrates that EU policymakers want stronger and more cohesive privacy protections through Europe, and they were inspired in some areas by the best ideas in the U.S.

This is not to say that differences do not exist between our two approaches. They clearly do. But moving forward we should not look for ways to prevent data transfers. That will likely just harm the individuals we are trying to protect. Instead, it will be important for us, as we grapple with the Internet of Things and Big Data, to recognize the importance of transatlantic data flows, acknowledge similarities in our approaches to protecting that data, and continue to look to find more ways to create common ground between our privacy systems.

Julie Brill
Partner, Washington, D.C.
T +1 202 637 5623
julie.brill@hoganlovells.com

1 William E Kennard, U.S. Ambassador to the EU, Remarks Before the AmCham EU Transatlantic Conference, 'Winning the Future Through Innovation' (3 March 2011) <http://useu.usmission.gov/kennard_amchameu_030311.html> accessed 10 May 2016.

2 World Economic Forum, 'Delivering Digital Infrastructure: Advancing the Internet Economy' (April 2014), 7 <http://www3.weforum.org/docs/WEF_TC_DeliveringDigitalInfrastructure_InternetEconomy_Report_2014.pdf> accessed 10 May 2016.

3 Economics and Statistics Administration, U.S. Department of Commerce, 'Digital Economy and Cross-Border Trade: The Value of Digitally-Deliverable Services' (January 2014), 2 <http://www.esa.doc.gov/reports/digital-economy-and-cross-border-trade-value-digitally-deliverable-services> accessed 11 May 2016.

4 See U.S. Constitutional amendment IV.

5 See Children's Online Privacy Protection Act of 1998, Pub L No 105-277, 112 Stat. 2681-728 (15 USC. § 6501 et sqq).

6 See 15 USC §§ 6801-6809.

7 Health Insurance Portability and Accountability Act of 1996, Pub L No 104-191, 110 Stat. 1936 (codified in scattered sections of 18, 26, 29 and 42 USC.).

8 See 20 USC § 1232g.

9 See, eg, 15 USC § 1681 et sqq.

10 5 USC § 45(a).

11 FTC, 'Privacy & Data Security Update (2015)' (2016 January) <https://www.ftc.gov/reports/privacy-data-security-update-2015#data> accessed 10 May 2016.

12 See, In re Goldenshores Techs. LLC, No C-4466 (FTC 31 March 2014) (decision and order) <https://www.ftc.gov/system/files/documents/cases/140409goldenshoresdo.pdf> accessed 10 May 2016.

13 See FTC, Press Release, Aaron's Rent-To-Own Chain Settles FTC Charges That It Enabled Computer Spying by Franchisees (22 October 2013) <https://www.ftc.gov/news-events/press-releases/2013/10/aarons-rent-own-chain-settles-ftc-charges-it-enabled-computer> accessed 11 May 2016.

14 See FTC, Press Release, Dental Practice Software Provider Settles FTC Charges It Misled Customers About Encryption of Patient Data (5 January 2016) <https://www.ftc.gov/news-events/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled> accessed 11 May 2016.

15 FTC v Sitesearch Corp., dba LeapLab, No CV-14-02750-PHX-NVW (D. Az. 22 December 2014) (complaint) <https://www.ftc.gov/system/files/documents/cases/141223leaplabcmpt.pdf> accessed 11 May 2016.

16 In re Facebook, Inc., No C-4365 (FTC 27 July 2012) (decision and order) <https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf> accessed 11 May 2016.

17 In re Google, Inc., No C-4336 (FTC 13 October 2011) (decision and order) <https://www.ftc.gov/sites/default/files/documents/cases/2011/10/111024googlebuzzdo.pdf> accessed 11 May 2016.

18 In re MySpace LLC, No C-4369 (FTC 30 August 2012) (decision and order) <https://www.ftc.gov/sites/default/files/documents/cases/2012/09/120911myspacedo.pdf> accessed 11 May 2016.

19 In re Twitter, Inc., No C-4316 (FTC 2 March 2011) (decision and order) <https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110311twitterdo.pdf> accessed 11 May 2016.

20 See, eg, FTC, Press Release, 'Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser' (9 August 2012) <https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented> accessed 11 May 2016; FTC, Press Release, 'LifeLock Will Pay $12 Million to Settle Charges by the FTC and 35 States That Identity Theft Prevention and Data Security Claims Were False' (9 March 2010) <https://www.ftc.gov/news-events/press-releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states> accessed 11 May 2016.

21 See U.S. Department of Health & Human Servs., 'HIPAA Compliance and Enforcement' <http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html> accessed 11 May 2016.

22 See Federal Deposit Insurance Corporation, 'Privacy Choices' (28 July 2014) <https://www.fdic.gov/consumers/assistance/protection/privacy/privacychoices/> accessed 11 May 2016 (describing roles of different agencies with responsibilities for enforcing privacy laws against banks and other financial institutions).

23 See FCC, 'Customer Privacy' <https://www.fcc.gov/general/customer-privacy> accessed 11 May 2016 (describing FCC's role in enforcing privacy protections under the Telecommunications Act of 1996, Pub L No 104-104, 110 Stat 56 and FCC rules).

24 Notice of Proposed Rulemaking, In re Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, No 16-106 (FCC 1 April 2016) <https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1.pdf> accessed 12 May 2016.

25 See National Conference of State Legislatures, 'Employer Access to Social Media Usernames and Passwords' (31 December 2014) <http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords.aspx> accessed 11 May 2016 (noting that in 2014, at least 28 States had introduced social media and employment legislation or had such legislation pending).

26 See, eg, Privacy Rights Clearinghouse, 'California Medical Privacy Fact Sheet C5: Employment and Your Medical Privacy' (2012 July) <https://www.privacyrights.org/content/employment-and-your-medical-privacy> accessed 11 May 2016.

27 See National Conference of State Legislatures, 'Security Breach Notification Laws' (4 January 2016) <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx> accessed 11 May 2016.

28 See Federal Trade Commission Act, ch 311, § 5, 38 Stat 717 (15 USC § 45).

29 See U.S. Department of Commerce, 'EU-US Privacy Shield' <https://www.commerce.gov/privacyshield> accessed 11 May 2016.

30 Joshua P Meltzer, 'The Importance of the Internet and Transatlantic Data Flows For U.S. and EU Trade and Investment' (October 2014) <http://www.brookings.edu/~/media/research/files/papers/2014/10/internet-transatlantic-data-flows-meltzer/internet-transatlantic-data-flows-version-2.pdf> accessed 19 June 2016.

31 FTC, 'Guidance: Information for EU Residents Regarding the U.S. – EU Safe Harbor Program' (February 2015) <https://www.ftc.gov/tips-advice/business-center/guidance/information-eu-residents-regarding-us-eu-safe-harbor-program> accessed 11 May 2016.

32 Martin A Weiss and Kristin Archick, CRS, 'US-EU Data Privacy: From Safe Harbor to Privacy Shield' (12 February 2016), 6 <https://www.fas.org/sgp/crs/misc/R44257.pdf> accessed 11 May 2016.

33 See Case C-362/14 Schrems v Data Protection Commissioner (CJEU, 6 October 2015) ECLI:EU:C:2015:650.

34 Judicial Redress Act of 2015, Pub L No 114-126, 130 Stat 282.

35 Uniting and Strengthening America By Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub L No 114-23, 129 Stat 268.

36 The White House, Press Release, 'Presidential Policy Directive/PPD-28 — Signals Intelligence Activities' (17 January 2014) <https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities> accessed 11 May 2016.

37 Memorandum from John F Kerry, Secretary of State, U.S. Department of State, to Vera Jourova, Commissioner, European Commission (22 February 2016) <http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-3_en.pdf> accessed 11 May 2016.

38 See EU-US Privacy Shield Ombudsperson Mechanism Annex A (n 29) 2-3.

39 EU-US Privacy Shield Principles (n 29) 5.

40 idem 20-21 (n 37) 20-21.

41 FTC, 'Legal Resources' <https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field_consumer_protection_topics_tid=251> accessed 11 May 2016.

42 European Commission, Press Release, 'EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield' (2 February 2016) <http://europa.eu/rapid/press-release_IP-16-216_en.htm> accessed 11 May 2016.

43 General Regulation Data Protection (adopted 14 April 2016) <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf> accessed 11 May 2016.

44 European Commission, Press Release, 'Questions and Answers – Data Protection Reform' (21 December 2015) <http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm> accessed 11 May 2016.

45 See GDPR (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/51, art 32(1) (requiring data controllers and processors to 'implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk'); Council Directive (EC) 95/46, art 17 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31, 43.

46 GDPR (n 44) art 32(1)(b).

47 See idem art 32.

48 See FTC, 'Statement Marking the FTC's 50th Data Security Settlement' (31 January 2014), 1 <https://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf> accessed 11 May 2016 (stating that 'there is no one-size-fits-all data security program').

49 See Commission Regulation (EU) 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and the Council on privacy and electronic communications [2013] OJ L173/2.

50 GDPR (n 44) art 33(1).

51 idem art 34.

52 idem art 33(1) (A controller may offer a reason justification to the relevant supervisory authority for failing to meet this deadline).

53 idem art 17.

54 See Case C-131/12 Google Spain SL v Agencia Española de Protección de Datos (CJEU, 13 May 2014) ECLI:EU:C:2014:317.

55 See European Commission, 'Article 29 Data Protection Working Party: Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja Gonzáles" C-131/12' (26 November 2014), 3 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf > accessed 11 May 2016 ('In order to give full effect to the data subject's rights as defined in the Court's ruling, de-listing decisions must be implemented in such a way that they guarantee the effective and complete protection of data subjects' rights and that EU law cannot be circumvented. ... In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com.').

56 Dave Evans, White Paper, 'The Internet of Things: How the Next Evolution of the Internet Is Changing Everything' (April 2011) <http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf> accessed 11 May 2016. These estimates include all types of connected devices, not just those aimed at the consumer market.

57 ibid.