Two-Way Street: U.S.-EU Parallels Under the General Data Protection Regulation
Ghostery/Hogan Lovells Data Privacy Day
U.S. Federal Trade Commissioner Julie Brill
January 21, 2016

Good afternoon. Thank you, Todd, for your warm introduction. And thank you to Ghostery and Hogan Lovells for the invitation to speak with all of you today to mark Data Privacy Day. With all that is going on in privacy right now in the U.S. and Europe, Data Privacy Week might have been more appropriate. Todd asked me to address two issues from my perspective as a Federal Trade Commissioner: the General Data Protection Regulation (GDPR)[1] and a transatlantic data transfer mechanism to replace Safe Harbor.

I would like to begin with the GDPR. With all that has been happening with data transfer mechanisms in the wake of the Schrems decision last October,[2] I feel like the GDPR has been a little neglected, at least in the discussions taking place in Washington. But as Eduardo Ustaran pointed out recently, it would be a "huge mistake" to wait two years between the finalization of the Regulation and its effective date before figuring out what it means.[3] That goes for companies as well as enforcement agencies like the Federal Trade Commission (FTC).

The GDPR will have far-reaching effects on all of us. Setting a global standard has been part of the European privacy project for a long time. The Data Protection Directive's adequacy requirement[4] has encouraged countries outside the EU to adopt EU-style data protection laws.[5] As the European Commission began to develop the General Data Protection Regulation, at least one European Commissioner explicitly said that part of its goal was to set a global standard.[6] More recently, after the EU institutions reached a political agreement on the final form of the GDPR, the European Commission's own press release stated that a focus of the Regulation is

[1] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (Dec. 15, 2015) ["GDPR"].

[2] Schrems v. Data Protection Comm'r, CJEU Case C-362/14 (Oct. 6, 2015), available at http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=en&type=TXT&ancre=.

[3] Eduardo Ustaran, GDPR – A Game Changer for the Digital Economy, Hogan Lovells Chronicle of Data Protection (Jan. 4, 2016), available at http://www.hldataprotection.com/2016/01/articles/international-eu-privacy/gdpr-a-game-changer-for-the-digital-economy/.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L281/31, Digital World (Jur

"setting global data protection standards."[7] As a result, it has become natural to think of European privacy policy as projecting only outward from Europe towards the United States and elsewhere, radiating its requirements in one direction.

But the GDPR is not a purely European document. Some of the key substantive provisions of the GDPR have roots in U.S. privacy law and policy. And some of the big questions left open in the GDPR that the Europeans will have to grapple with over the coming years are questions that we have been grappling with here in the U.S. for some time. So I think it is more helpful – for both European and U.S. stakeholders – to recognize that the transatlantic discussion about privacy policy that the GDPR has engendered is a bustling two way street. The traffic in ideas about privacy protections travels in both directions, allowing both sides to learn from each other's experiences. Recognition of this dynamic will allow us to find common ground where it exists as the GDPR is put into practice, and to engage in rich and robust discussions about how to find solutions to common problems.

Of course, there are important differences between the U.S. framework and the framework envisioned by the GDPR. We would be foolish to not discuss those differences just as honestly.

Elements of a Two-Way Exchange of Privacy and Data Protection Ideas

Let me begin with some of the clearest examples of the ways in which principles of the US privacy framework have found a home within the GDPR.

Data Security

I rarely discuss consumer privacy without bringing data security into the picture. Put simply, there is no privacy without data security. If companies cannot protect consumer data from unauthorized disclosures or uses, privacy is pretty hopeless. Recent FTC cases like Snapchat[8] and TRENDnet[9] illustrate this close connection between privacy and data security. 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.[10]

Many of our state laws include risk-based triggers that limit the circumstances under which notification is needed, and many of them exempt encrypted data from the duty to notify. My guess is that the GDPR's "high risk" trigger is something that many companies in the U.S. will be familiar with, and will welcome. Conversely, only some states require notification to be sent to state attorneys general or other law enforcement officials. Requiring notification to the responsible authorities across a broader portion of the United States would, in my view, serve consumers and companies well by giving all of us a better understanding of specific breaches as well as broader trends.

Encryption

Let me turn to encryption. As I mentioned a moment ago, the FTC encourages companies to encrypt personal data. This message is especially important with respect to the Internet of Things, where some research indicates that the use of encryption is way behind where it ought to be. The FTC has brought enforcement actions against companies whose failure to use encryption to protect sensitive personal information was one element of a systemic data security problem within the company.[20] We have also brought cases against companies that misrepresented how much protection their encryption methods would offer to consumers' data.[21]

The GDPR lines up rather well with the FTC's call for more extensive use of encryption. In addition to making encryption a possible means to avoid individual notification of a breach and a consideration in the "appropriate" level of security for personal data, the GDPR makes encryption one consideration among several others in determining whether secondary uses of personal data are lawful – perhaps on the theory that strong data security safeguards are integral to reducing the risk that data kept longer than needed to serve its original purpose will interfere with individuals' privacy rights.[22]

The GDPR does not settle or even address explicitly hot-button questions about encryption, such as whether companies should provide "back doors" to allow governments to obtain access to the plain text of encrypted communications under an appropriate court order.

---

[20] See, e.g., Accretive Health, No. C-4432 (F.T.C. Feb. 5, 2014), available at https://www.ftc.gov/enforcement/cases-proceedings/122-3077/accretive-health-inc-matter.

[21] See, e.g., FTC, Press Release, Dental Practice Software Provider Settles FTC Charges It Misled Customers About Encryption of Patient Data (Jan. 5, 2016), available at https://www.ftc.gov/news-events/press-releases/2016/01/dental-practice-software-provider-settles-ftc-charges-it-misled. See also Credit Karma, No. C-4480 (F.T.C. Aug. 13, 2014), Complaint ¶ 22, available at https://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc ("As a result of these failures, attackers could, in connection with attacks that redirect and intercept network traffic, decrypt, monitor, or alter any of the information transmitted from or to the application, including Social Security numbers, dates of birth, 'out of wallet' information, and credit report information.");

Such questions remain unsettled in the United States, too. A further exchange of ideas in this issue may be fruitful.

Deidentification

To stay with technical data protection measures for another minute, let me discuss deidentification and anonymization. For several years there has been a lively debate in the United States about what constitutes deidentified data, how robust technical deidentification measures are, and whether deidentification is useful as a standalone data protection measure.[23]

pseudonymization as part of fulfilling the GDPR's privacy by design and security mandates.[27] Only when personal data is transformed to be "anonymous information" – meaning that data subjects cannot be identified – is data considered to be outside the scope of the substantive requirements of the GDPR.[28]

Privacy by Design

Although the FTC was not the first to use the term "privacy by design," we have recommended privacy and security by design for a long time.[29] The GDPR also discusses privacy and security by design, and calls out data minimization as a specific step that companies should take as part of data protection by design.[30] The FTC made the same recommendation in its 2012 privacy report. Indeed, data minimization is a foundational privacy principle that I have continued to encourage companies to embrace, rather than kick to the side as a relic of the antiquated times soon to be known as "BBD" – "before big data".

Children's Privacy

Still more evidence of the dynamic dialogue between the privacy principles on both sides of the Atlantic is the mutual focus on heightened protections for data about children. In the United States, these protections take the form of the Children's Online Privacy Protection Act (COPPA), which protects children under the age of 13 and has been the law of the land since 1998.[31] One of COPPA's requirements is that websites directed toward children, or whose operators know that they are collecting personal data from children, must obtain verifiable parental consent before doing so.[32]

Like COPPA, the GDPR recognizes that children's data is sensitive, [33] In another similarity to COPPA, the GDPR requires operators of online services under some circumstances to obtain verifiable parental consent to process children's data.[34] However, the GDPR departs from COPPA in one significant way. The GDPR's parental consent provisions apply to individuals up to 16 years of age, though Member States can lower this age to 13. Those three years are pretty important in children's lives. Some scholars believe that allowing young teenagers – even those younger than 13 – to navigate the shoals of social media is an important

---

[27] GDPR arts. 23 and 30.

[28] *See* GDPR R. 23 ("The principles of data protection should therefore not apply to anonymous information, that is information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable. This Regulation therefore does not concern the processing of such anonymous information, including for statistical and research purposes.").

[29] *See* 2012 PRIVACY REPORT, *supra* note 24, at 22-30.

[30] *See* GDPR art. 23(1).

[31] 15 U.S.C. §§ 6501-6506.

[32] 15 U.S.C. § 6502(b)(1)(A).

[33] GDPR R. 29 ("Children deserve specific protection of their personal data, as they may be less aware of risks, consequences, safeguards and their rights in relation to the processing of personal data.").

[34] GDPR art. 8(1a).

part of the maturation process.[35] I wonder whether European tweens who are looking forward to joining their peers on social networks will end up provoking a backlash against a requirement that they must wait another three years. I also wonder how this requirement to keep them off social media and other online services without parental consent can be enforced. I guess we shall see.

Right to Be Forgotten

In some instances, the parallels that one

I am concerned that the GDPR may reverse this trend by limiting the FTC's ability to cooperate with Member State DPAs. Article 43a appears to prohibit companies from disclosing data covered by the GDPR in response to "any judgment of a court or tribunal and any decision of an administrative authority" unless the request is made pursuant to an "international agreement" or MLAT. Whether this provision could limit the FTC's ability to further its investigations by obtaining information from companies in Europe is something that the FTC is currently examining. It would be a loss for consumers in the U.S. and EU if this provision of the GDPR ends up turning enforcement cooperation into dead end.

The Ongoing Need for a Transatlantic Data Transfer Framework

Now to the ongoing negotiations over a transatlantic data protection framework to replace Safe Harbor. Those negotiations are at a delicate stage, so I cannot get into too much detail. Instead, I would like to spend a moment reemphasizing my support for such a framework.

Many advocates and DPAs hailed the *Schrems* decision as a victory for the fundamental right of privacy, but some of the losses are now becoming apparent. The first loss is transparency. When a company joined Safe Harbor, consumers knew it, advocates knew it, and the entire enforcement community knew it. The principles and operating procedures for Safe Harbor were also well known and uniform. The same cannot be said for other data transfer mechanisms, such as binding corporate rules and model contractual clauses.

The second loss is FTC enforcement. Simply put, the absence of Safe Harbor may limit the FTC's ability to take action against companies if they misrepresent how they follow European privacy standards. And, in the absence of Safe Harbor, there is little reason for companies to make those representations in the first place. Before *Schrems*, The FTC had brought 39 enforcement actions against companies for alleged Safe Harbor violations, as well as an action against TRUSTe for allegedly misrepresenting the extent of its Safe Harbor assessments.

Finally, small and medium enterprises – which made up around 60 percent of Safe Harbor membership[43] – stand to lose the most from the *Schrems* decision. Like the biggest companies that are often discussed in public debates in Europe, these SMEs depend on the free flow of information to sell goods and services globally, build global workforces, and take advantage of low-cost cloud computing resources. Unlike the big companies, however, these SMEs do not have the resources to get BCRs approved or put model contractual clauses in place.

---

https://www.congress.gov/bill/109th-congress/senate-bill/1608/text?overview=closed (codified in scattered sections of 15 U.S.C.).

[43] Testimony of Edward M. Dean, Deputy Assistant Secretary International Trade Administration,0008 Tcnnd take on Tw[(s.6.368

I hope to see a new transatlantic data protection framework in place very soon. This will be to the benefit of consumers and companies on both sides of the Atlantic. Agreeing on a framework would also allow everyone involved to start focusing on the many other challenges that the U.S. and Europe should try to address together. The GDPR itself is one of them. The Internet of Things, big data analytics, and all of their associated privacy and security challenges are also on this list. If we are going to bring appropriate data protections to these new technologies, and help them reach their full potential, we need to start addressing these challenges together, and we need to start right now.

Thank you.