from connected cars might help us 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 personal 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. I spend a lot of time talking with industry leaders from many sectors of the economy, and they understand this. Put simply, none of them wants their company to be in the headlines for failing to implement reasonable data security, deceiving consumers about the company's data practices, or collecting or using consumers' data unfairly.

But engendering consumer trust in the data-driven economy isn't as simple as companies' compliance with federal and state laws. Because data flows are now global, so are data privacy and security issues. Here in the U.S., protecting consumer privacy and data security are top priorities at the Federal Trade Commission and other state and federal agencies, and I am proud of the work we do along these lines. But I'll be honest with you: the U.S. privacy framework is different from those in Europe, Asia, and Latin America. While the United States embraces many of the same privacy principles as other countries, and we have developed ways to make our systems interoperable, the differences also create real challenges.

The first challenge is that some international thought leaders – within the government, business community and civil society of our trading partners – do not fully understand U.S. privacy law. Some of them believe that our system offers little or no privacy or security protections for data about individuals. Some say that the U.S. is the "Wild West" where data practices are concerned. Others think that privacy protections in the U.S. are voluntary, and the only way that a company can get into trouble is by making a promise about a product or service

The U.S. Consumer Privacy Framework: Different But Comprehensive

The notion that the United States doesn't have a privacy law stems primarily from the fact that we do not have a single, comprehensive law that governs the collection, use, and disclosure of personal information in the commercial sphere. Instead, here in the U.S. there are a variety of federal and state laws that play an important role in protecting the privacy and security of individuals' information. Some federal privacy laws apply to specific sectors, such as healthcare,[6] banking,[7] credit reporting,[8] and communications.[9] Other federal laws protect children's and students' privacy.[10] The states have many additional privacy laws that range from limiting employers' ability to view their employees social network accounts,[11] prohibiting employers and insurers from using information about certain medical conditions,[12] and requiring online services to allow minors to delete information they have posted[13] – to requiring companies to notify consumers when they suffer a security breach involving personal information.[14] In addition to these specific laws, Section 5 of the Federal Trade Commission Act[15] prohibits "unfair or deceptive acts or practices,"[16] and the FTC has used this authority to address a number of data security and privacy practices that fall through some of the gaps in more specific laws.

The FTC has been a cop on the privacy and data security beat since the rise of the commercial Internet. The FTC entered this arena because the potential for consumers to be harmed by losing control of personal information was clear. Over the past 15 years or so, we have brought nearly 100 actions protecting millions of consumers – in the United States, Europe, and elsewhere – from deceptive and unfair data practices. We have used this authority to bring enforcement actions against well-known companies like Google, Facebook, Twitter and

Snapchat.[17] We have also brought cases against companies that are not household names, but violated the law by spamming consumers,[18] installing spyware on their computers,[19] failing to secure consumers' personal information,[20] deceptively tracking consumers online,[21] violating children's privacy,[22] and inappropriately collecting information on consumers' mobile devices.[23] Most importantly, the broad reach and remedial

Things get more interesting when a company provides some information about their data collection and use practices to consumers, but leaves out material information about other practices. To take one example, in March 2014, the FTC brought an action against the vendor of an app that turned the LED on a mobile phone – most widely known for turning into a flash bulb for the phone's camera – into a flashlight. But we believed the flashlight app was collecting precise geolocation information, along with a number that uniquely identified consumers' phones. The company's privacy policy disclosed that the app collected

personal information,[29] including medical information,[30] pharmaceutical records,[31] and our social contacts.

But we also alleged that the app exposed consumers' mobile phone numbers,[37] and left consumers vulnerable to being impersonated by other Snapchat users.[38]

From time to time, I discuss these issues with my data protection colleagues in other countries – describing the scope and nuances of our privacy and data security laws in the U.S., as well as the breadth of our enforcement work. These conversations, and others like them, have helped increase the understanding abroad that, far from being the Wild West of data collection and use, the U.S. (and particularly the FTC) engages in robust and careful privacy enforcement, including against companies whose data practices cause substantial harm, even if the companies make no promises about how they collect, use, or share data.

Strengthening the U.S. Privacy and Data Security Framework

While Section 5 and sector-specific data privacy laws create good protections for consumers and their data, I believe our consumer privacy and data security framework can and should be improved. As more and more sensitive information flows throughout the commercial marketplace, I think it is important to ensure that the data are appropriately protected. For example, health and personal financial information are at the center of many new apps, services, and devices – and many of them are operated by companies that are not covered by our sector specific laws governing health and financial information. Yet the information is just as sensitive and deserving of protection.

The growth of the Internet of Things, while exciting, will increase the need to adapt our data security laws. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion.[39] A recent study by Hewlett-Packard found that 90 percent of connected devices are collecting personal information, and 70 percent of them are transmitting this data without encryption.[40] And the data security concerns raised by connected devices involve not only unauthorized access to personal information, but also involve security threats to device functionality itself. If a device like a pacemaker[41] or a car[42] is hacked, very sensitive information could be compromised and the person using the device could be seriously harmed.

---

[37] *Id.* at ¶¶ 30-33.

[38] *Id.* at ¶¶ 34-45.

[39] DAVE EVANS, CISCO INTERNET BUS. SOLUTE7.89 -SJ10.02 0 0 10.02 225.694.601 TguY7.98 252.6 213.3 oncrease t00e a.3(kP13.3 Tm( )Tj10.02 3co

provides for strong remedies that protect consumers and improve how companies handle data. This framework is effective, and it is uniquely American.

Handling Differences: Interoperability in a Post-Snowden World

Other countries handle privacy differently. Most countries with industrialized economies have a baseline law that governs data practices in the commercial sphere. This is certainly the case in Europe, as well as Canada, Mexico, Israel, and Japan, to name a few. Some privacy regimes present unique challenges, including the emergence of data localization laws.[48] Yet for the FTC and other parts of the U.S. government, as well as companies that do business globally, Europe presents some of the most urgent questions about privacy frameworks and global data flows, so that's where I'll focus my attention today.

One of the major differences between the U.S. and EU privacy frameworks is that, in Europe, privacy is a fundamental right. The Charter of Fundamental Rights establishes rights to the protection of private life and of pers,srd ofr.

industrial revolution driven by digital data, computation and automation,"[54] and concluded that fully developing this potential requires ensuring that "[u]sers have sufficient trust in the technology, the behaviors of providers, and the rules governing them" and that appropriate data protection laws are ways to build this trust.[55] Similarly, the Article 29 Working Party, which consists of data protection authorities from EU Member States, also noted last September that the Internet of Things holds "significant prospects of growth for a great number of innovating and creative EU companies" but also stated that "these expected benefits must also respect the many privacy and security challenges."[56] These efforts in Europe to tie together the promise of the data-driven economy with the need to appropriately address privacy and security are similar in many ways to the discussions underway here in the U.S., driven by policy recommendations from the White House and from the FTC.

Moreover, just as we have done in the United States, European policy makers have identified gaps and other problems in their ow

There are, however, mechanisms that allow personal data to legally flow from the EU to the United States. From the time that the Directive went into force, the EU and the U.S. recognized that prohibiting such data flows would be harmful to the economies on both sides of the Atlantic. As the initial Safe Harbor negotiations approached their conclusion in 2000, the White House noted that the arrangement would protect privacy in accordance with EU law while "prevent[ing] the potential disruption of approximately $120 billion in U.S.-EU trade."[60] The amount at stake has only increased since then.[61] This mutual interest in transatlantic data flows led to the U.S.-EU Safe Harbor Framework, which allows specific companies to certify that they provide adequate protections for personal data.

There are two main pieces to Safe Harbor. First, the Framework spells out seven privacy principles that companies must follow, such as notice, choice, access, and security.[62] Second, the Framework says that companies that want to be in Safe Harbor must certify and publicly declare that they follow the Safe Harbor principles in their own data practices.

The FTC plays an essential role in the Safe Harbor Framework, because it is the agency that enforces companies' Safe Harbor commitments.

The viability of the Safe Harbor was seriously threatened starting in June 2013, when information provided by Edward Snowden began to detail some of the data collection activities of the National Security Agency and other intelligence and law enforcement agencies. Many European officials, advocates, and citizens reacted to these revelations with outrage over what was reported.[63] The European Parliament recommending suspending Safe Harbor.[64] The European Commission took a different approach. It issued a report indicating that the Safe Harbor Framework should be retained, but demanding 13 changes.[65]

---

[59] European Commission, Commission Decisions on the Adequacy of the Protection of Data in Third Countries (last updated Dec. 15, 2014), *available at* http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

[60] White House, Fact Sheet: Data Privacy Accord with EU (Safe Harbor) (May 31, 2000), *available at* http://clinton4.nara.gov/WH/New/Europe-0005/

For more than a year, the Department of Commerce and the European Commission have been negotiating these changes. Many of the items on the European Commission's list are reforms that make good sense and would improve Safe Harbor from a consumer protection standpoint. These changes include eliminating the fees that some EU consumers have to pay to have Safe Harbor-related disputes resolved, increasing transparency in the administration of the Safe Harbor program, and increasing accountability within companies that are in Safe Harbor.[66] Two of the EC's recommendations for improving Safe Harbor concern national security issues.[67] The current Safe Harbor Framework,[68] as well as other mechanisms governing data transfers in the commercial sphere (such as binding corporate rules), and even the EU Data Protection Directive itself, all include exceptions for national security and law enforcement.

The Snowden revelations began a robust conversation on both sides of the Atlantic about whether we have struck the right balance in the law enforcement and national security arenas. The Charlie Hebdo and Jewish market attacks have added some important new perspectives to this discussion in Europe.[69] The conversation on both sides of the Atlantic is critically important, but in my view it should be distinct from the issues surrounding companies' collection and use of consumer data.

In the context of companies' collection and use of consumer data, I believe that Safe Harbor gives the FTC an effective tool to protect the privacy of consumers in the EU and the U.S. As such, Safe Harbor is a solution, not a problem. The FTC has settled 24 actions against companies that allegedly either falsely stated that they were in Safe Harbor but actually were not, or claimed to meet Safe Harbor's substantive requirements but did not.[70] In addition, in November, the FTC announced a settlement with TRUSTe, which maintains a Safe Harbor certification program, over its alleged misrepresentations about the extent to which it conducted annual recertifications for Safe Harbor and other privacy programs.[71]

---

[66] *See* Julie Brill, At the Crossroads 7-8 (Dec. 11, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/crossroads-keynote-address-iapp-europe-data-protection-congress/131211iappkeynote.pdf.

[67] *See* European Commission, Restoring Trust in EU-US Data Flows – Frequently Asked Questions (Nov. 27, 2013), *available at* http://europa.eu/rapid/press-release_MEMO-13-1059_en.htm.

[68] *See* Safe Harbor Principles, *supra* note 62 ("Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; . . .").

[69] *See, e.g.*, Kevin Johnson, *Security vs. Privacy: France Trying to "Find the Line"*, USA TODAY (Feb. 9, 2015 6:54 PM), *available at* http://www.usatoday.com/story/news/nation/2015/02/09/france-terror-surveillance/23118939/.

[70] *See* FTC, Privacy & Security Update (2014), *available at* http://www.ftc.gov/reports/privacy-data-security-update-2014 (noting that "[s]ince 2009 the FTC has used Section 5 to bring 24 Safe Harbor cases").

[71] True Ultimate Standards Everywhere (TRUSTe), FTC Matter No. 1323219, Complaint at ¶¶ 11-16 (Nov. 17, 2014), *available at* http://www.ftc.gov/system/files/documents/cases/141117trustecmpt.pdf. Under the FTC's proposed order, TRUSTe is prohibited from making such representations and would be subject to civil penalties if it fails to abide by these terms. *See* TRUSTe, FTC Matter No. 1323219 at § I (consent order), *available at*

* * * *

Where do things go from here? As business leaders and business students, you should probably think about this question the same way you think about mid-February in New Hampshire: we've put a lot behind us, but there's still a long way to go. In terms of the discussions with our European colleagues, I am optimistic about resolving the tensions that have understandably arisen since June 2013. Part of my optimism goes back to the common privacy principles that we share, and the efforts underway on both sides of the Atlantic to examine whether our different privacy frameworks are able to sufficiently protect consumers in an era of big data and the Internet of Things.

Going forward, the appropriate measure of progress should not be which system "wins" [as I was recently asked during a talk in Brussels]. Instead, the appropriate measure is whether the United States and Europe develop practical, effective, and interoperable frameworks that will allow data to be adequately protected and to flow between our economies. Neither the U.S. nor Europe will succeed without getting privacy and data security right, as they are key elements to engendering consumer trust. Consumers – and businesses – need and deserve nothing less.

Thank you.