

Ambassador Daniel A. Sepulveda
Remarks on the U.S. Privacy Framework and Signals Intelligence Reforms
November 3, 2015
Digital Europe
Brussels, Belgium

Thank you for the opportunity to join you here today.

At this important time in our relationship and dialogue, it is critical that we honestly and effectively exchange perspectives on the issues we are here to discuss today.

Let me assert that it is both simplistic and incorrect to argue that Europeans care more about their privacy than do Americans and it is equally as simplistic and incorrect to argue that Europeans care less about the health of the transatlantic digital economy than do Americans. That framing, which is all too common in the popular press, is both wrong and harmful to the prospects for joint problem solving.

I will assert and maintain as a matter of core conviction that existing privacy protections in U.S. law and practice are strong. They are built on a history of well enforced protections against improper collection, use, or distribution of personal information.

And while no body of law is perfect, and indeed U.S. officials continue to conduct efforts to examine and enhance civil liberties and privacy protections with respect to U.S. Signals Intelligence activities and privacy practices in commerce, the U.S. privacy legal and policy framework is both robust and consistent with our international human rights obligations.

Consumers of services originating in the United States, regardless of where those services are delivered, benefit from a combination of laws and active enforcement to protect data privacy. Legal protections barring deceptive or unfair business practices combined with robust enforcement by our consumer protection agencies, and binding contracts between companies that process data provide a strong foundation for consumer protection. In addition, market pressure from customers on firms, social pressure from privacy activists on those using information, and

vigilance by a free press all help ensure accountability for the way companies protect the data of the people they serve.

Beyond that, the American private sector, acting in their own self interest as well as in an effort to comply with law, are developing a culture of privacy protection. Leading American firms have chief privacy officers and other trained privacy professionals, as well as coordinated policies and practices, to ensure the trust and confidence of the people they serve. These professionals help ensure that American entities' privacy practices evolve to reflect ever-changing technologies and practices; they know it is in their interest to do so and many are competing against each other to drive the best privacy protection solutions for consumers.

Together, those forces create a holistic environment of protection for privacy that provides consumers with strong privacy protections and innovative digital services that is strong, as one noted privacy scholar has pointed out, not just on the books, but also on the ground.

Nonetheless, this Administration has explored how we can do better, both as a matter of law and practice. President Obama directed John Podesta to lead a scoping exercise to identify privacy challenges in the age of "Big Data"-an effort that resulted in multiple private and public sector reforms as well as the February release of a potential framework for a Consumer Privacy Bill of Rights. The draft law would provide greater specificity and certainty to consumers as to what they can expect from those who collect, use, and share their information.

In his release of the proposed framework for a Consumer Privacy Bill of Rights, President Obama states, "even though we live in a world where we share personal information more freely than in the past, we must reject the notion that privacy is an outdated value. It has been at the heart of our democracy since its inception, and we need it now more than ever."

The Consumer Privacy Bill of Rights calls on stakeholders, the U.S. Congress, and individuals to discuss and work toward a comprehensive framework for privacy protection that is flexible, understandable, and beneficial to consumers and industry alike.

The Consumer Privacy Bill of Rights applies to personal data, which means any data, including aggregations of data, that is linkable to a specific individual. Personal data may include data that is linked to a specific computer or other device. Even without legislation, the Administration will continue to convene multistakeholder processes that use this Bill of Rights as a template for codes of conduct that are enforceable by the Federal Trade Commission. These elements—the Consumer Privacy Bill of Rights, codes of conduct, and strong enforcement—will increase interoperability between the U.S. consumer data privacy framework and those of our international partners.

We are sometimes met with skepticism in Europe about our commitment to privacy in America because we lack an overarching law on commercial privacy. FTC Commissioner Julie Brill, a leading mind on these issues, has pushed back on that criticism in expert fashion, outlining the authorities of the FTC's power to protect consumers as well as the U.S. laws that protect privacy in specific business areas like health care and financial services.. In her recent speech in Amsterdam, Commissioner Brill detailed our privacy protections, summarizing, “When these different parts of the U.S. privacy framework are put together, the result is a system that is strong and comprehensive. But it is also maddeningly difficult to explain to my European colleagues.”

I share both her conviction and her pain.

But we are not here to argue that the status quo requires no new work. The President understands, and we believe industry does as well, that we all have to work together to create a continually improving environment of respect for people's personal information in order to support the trust necessary to encourage use of services and promote the continued growth of the digital economy.

At the Federal Trade Commission earlier this year, President Obama presented his comprehensive approach to enhancing that trust by improving consumers' security, tackling identity theft, and bolstering privacy online and in the classroom. Among his proposals, the President has put forward a new legislative proposal to help bring peace of mind to the tens of millions of consumers whose personal and financial information has been compromised in a data breach. This proposal clarifies and strengthens the obligations companies have to notify customers when

their personal information has been exposed, including establishing a 30-day notification requirement from the discovery of a breach, while providing companies with the certainty of a single, national standard. The proposal also criminalizes illicit overseas trade in stolen identities.

To further address identity theft, the President has sought to give consumers access to one of the best early indicators of identity theft, as well as an opportunity to improve their credit health. A growing list of firms will make credit scores available for free to their customers. Through this effort more than half of all adults in the U.S. with credit scores will now have access to this tool to help spot identity theft.

To protect students, the President has released a legislative proposal designed to ensure that data collected in the educational context is used only for educational purposes. This bill, modeled on a landmark California statute and building on the recommendations of the White House Big Data review released earlier this year, would prevent companies from selling student data to third parties for purposes unrelated to educational missions and from targeting advertising to students based on data collected in school. The bill would, however, still permit important research initiatives to improve student learning outcomes as well as efforts by companies to continuously improve the effectiveness of their learning technology products.

Not wanting to wait for passage of a law, the President won new commitments from the private sector to help enhance students' privacy on the day he announced the legislative proposal. Seventy-five companies have committed to the cause, signing a pledge to provide kids, parents, and teachers with important protections against misuse of their data.

As you know, at the same time as we proposed changes to our laws and practices, our Department of Commerce has engaged with EU officials on updating the Safe Harbor Framework for commercial data transfers. The Safe Harbor's 4,000 plus membership is as deep and broad as the U.S.-EU relationship itself. Safe Harbor companies come from almost every sector of the economy and include both U.S.-headquartered companies and the U.S. subsidiaries and affiliates of EU-headquartered companies. In addition to the thousands of companies in the Safe

Harbor, countless EU-based companies have relied on the Framework to conduct business with their U.S.-based partners and clients.

In the process, U.S. and EU companies have built one of the most robust cross-border data networks in the world. Safe Harbor has strengthened and facilitated this network, which is a critical pillar of our competitiveness and the economic well being of our people. The Safe Harbor privacy principles have also provided vital privacy protections to the benefit of EU citizens, most importantly through the strong enforcement of the U.S. Federal Trade Commission.

In the wake of the European Court of Justice's decision invalidating the European Commission's 2000 decision on Safe Harbor, it is now more imperative than ever that the U.S. and EU expeditiously conclude an updated Framework that provides EU citizens with privacy safeguards that meet EU requirements and provides a clear path for U.S. and EU companies to continue transferring data.

The ECJ decision makes FTC enforcement of companies' transatlantic privacy commitments much more difficult because, in the absence of Safe Harbor, companies have little incentive to make representations about their adherence to European privacy standards. Further, it has eliminated the transparency that comes from knowing who is participating in the program and the conditions under which they have agreed to treat transatlantic personal data.

America's willingness to update the Safe Harbor as the EU's partner will ensure that the Framework lives up to our shared values. The U.S. Congress, as well as our Administration, is working hard to address EU concerns because we respect and value this relationship.

It is important to note that as a result of significant effort on the part of multiple parties, the Judicial Redress Act was passed by the U.S. House of Representatives on October 20 and is currently being considered by the U.S. Senate. The passage of this bill would give citizens of designated countries the same judicial redress rights available to Americans under the Privacy Act with regard to information shared with U.S. law enforcement authorities, including the ability to seek access and amendment of their personal data, as well as to bring a lawsuit for the intentional or willful disclosure of personal information.

I would also like to address the review of the U.S. signals intelligence programs in 2013. These reviews were conducted by a Presidentially- appointed, independent Review Group on Intelligence and Communications Technology as well as the Privacy and Civil Liberties Oversight Board, otherwise known as the PCLOB, which is an independent entity within the Executive Branch established by Congress as a privacy watch-dog in the area of counter-terrorism.

Both of these entities were given full access to classified intelligence security materials in order to facilitate their reviews. That kind of access and review of signals intelligence programs by independent actors is the equal of any in the world.

The Review Group issued a report in December 2013 that contained 46 recommended changes to law, procedure and practices. The PCLOB has issued two reports regarding Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act, or FISA. Based on the recommendations of these independent groups, the Obama Administration and U.S Congress have taken many concrete steps that have resulted in strengthened privacy and civil liberties protections for people around the world. These changes reflect the United States' longstanding conviction that signals intelligence collection should target national security threats and not be used to surveil either legitimate exercises of free expression or domestic political debate.

On January 17, 2014, President Obama delivered a speech to announce key signals intelligence reforms, saying “we have to make some important decisions about how to protect ourselves and sustain our leadership in the world, while upholding the civil liberties and privacy protections that our ideals and our Constitution require. We need to do so not only because it is right, but because the challenges posed by threats like terrorism and proliferation, and cyber-attacks are not going away any time soon.”

On that day the President issued Presidential Policy Directive 28 implementing substantial changes to the collection of all signals intelligence. The President directed that U.S. signals intelligence activities must include appropriate safeguards for personal information of all individuals regardless of nationality, and that, where feasible, protective policies and procedures be applied equally,

regardless of nationality, to govern the retention and dissemination of such information. PPD-28 also makes clear that the United States does not collect intelligence to suppress criticism or dissent. We do not collect intelligence to disadvantage people based on their ethnicity, race, gender, sexual orientation, or religion. And we do not collect intelligence to provide a competitive advantage to U.S. companies, or U.S. commercial sectors.

In terms of our bulk collection, we will only use data to meet specific security requirements such as counter-intelligence; counter-terrorism; counter-proliferation; cyber-security; force protection for our troops and allies; and combating transnational crime, including sanctions evasion. The bottom line is people around the world – regardless of their nationality – should know that the United States is not spying on ordinary people who do not threaten our national security and takes their privacy concerns into account.

Other significant reforms were contained in the USA FREEDOM Act that the U.S. Congress enacted into law on June 2, 2015. It prohibits the U.S. government from using FISA to acquire metadata in bulk.

The Act also enacted meaningful reforms to the Foreign Intelligence Surveillance Court, for instance by allowing cleared attorneys to specifically represent privacy and civil liberties interests before the Court, and also provides for the public release of significant decisions, orders, and opinions. It also furthered the United States' commitment to transparency by authorizing U.S. companies to reveal information about government requests for data, and by requiring the government to release aggregate numbers about such requests.

I was encouraged to hear Commissioner Vera Jourova recognize the significant advancements the U.S has made in protecting individuals' privacy and enacting reforms to our signals intelligence programs during her speech last week to the Committee on Civil Liberties, Justice and Home Affairs.

As I have tried to convey and ask you to consider on the merits, the United States places the highest importance on our partnership with the European Union. We know that it is built on shared interests and shared values. We will continue to cooperate with our EU partners to address their concerns and endeavor to

continually improve the privacy safeguards of both U.S. and EU citizens. We will emerge from this having jointly tackled the challenge and stronger for it.

We look forward to working with you and I appreciate your time.