Privacy in our Digital Lives: Protecting Individuals and Promoting Innovation

January 2017

THE WHITE HOUSE
WASHINGTON

THE WHITE HOUSE

WASHINGTON

January 17, 2017

Trust is a bedrock of our society, our economy, and our Nation — and respect for our privacy is one of the cornerstones of that public trust. Yet in a world where a private opinion expressed online can ricochet among millions in an instant, privacy has never been more at risk. Nor has there been a time in history in which the global flow of data, products, and services have made shared norms of privacy protection so imperative.

Privacy is more than just, as Justice Brandeis famously proclaimed, the "right to be let alone." It is the right to have our most personal information be kept safe by others we trust. It is the right to communicate freely and to do so without fear. It is the right to associate freely with others, regardless of the medium. In an age where so many of our thoughts, words, and movements are digitally recorded, privacy cannot simply be an abstract concept in our lives; privacy must be an embedded value.

When our privacy is safeguarded, it helps improve our lives, promote innovation, strengthen trade relationships, building trust between companies and consumers, and ensure that governments are accountable to citizens. This is the work I've sought to promote as President these past 8 years, and this report highlights our accomplishments in key areas.

Many of today's national security threats know no borders; they can affect dozens of States simultaneously and often travel through the very digital networks that enable so much our global economy. That is why we put into place the world's clearest limitations and most public descriptions of our signals intelligence practices to ensure we protect privacy alongside our national security, sacrificing neither.

Likewise, with so much of our daily lives occurring online and through technology — whether consumers, workers, or among family and friends — data collection and transmission can seem omnipresent, and to some, omniscient. That is why we put forward groundbreaking policies, brokered new industry consensus, developed new tools of enforcement, and put into place new global privacy norms.

All this work reflects my Administration's broader commitment to ensure that the tools of progress do not become instruments of dehumanization, blackmail, exploitation, or persecution. As my Presidency draws to a close, there remains much to be done to keep this priority at the forefront of national policymaking, and to ensure that the freedoms we cherish as Americans are preserved for future generations.

Table of Contents

I.
Continuing the U.S. Legacy of Privacy Protections through Technological and Economic Change

Data is more deeply woven into the fabric of our lives than ever before. In the last eight years, the cars that once got us to and from home became equipped with navigation cameras and now some models have the ability to operate on their own. Many children who used to do their homework with pen and paper at the kitchen table now have the ability to complete interactive and tailored homework assignments on school tablets or laptops. A network of technologies from personal computers to cell phones, from smart televisions to home speakers, from connected cars to wearable devices now offer consumers simple solutions to the questions people ask every day, such as "Where is the closest cup of coffee?" These solutions are fueled by the data that consumers give to companies or that is shared among machines in the growing Internet of Things.

This extraordinary interconnection creates enormous opportunities and some significant risks for the Nation, our economy, and for individual families. Unprecedented computational power and sophistication, most of which is not visible or available to the average consumer, also has the ability to create an asymmetry of power between those who hold the data and those who intentionally or inadvertently supply it. This Administration has asked not only how new technology will benefit our quality of life, but also whether there are appropriate safeguards to protect the fundamental freedoms of privacy and other civil liberties that Americans and all persons around the world hold dear.

In order to adapt the old physical world protections to the new online environment, we first need to better understand what the expectations of consumers are for their privacy and security in the digital ecosystem. While the executive branch of the Federal Government is made up of agencies that generally have authority over specific sectors of society and the economy the Internet is not a sector – it is a method of driving efficiencies across all parts of our economy. To this end, the Administration has championed a comprehensive approach to digital privacy guided by consumer expectations and the context of data collection and use.

This paper is a reflection on how people's interaction with technology has changed, and how we as a government have adapted our policies, our regulations, and our strategy for economic prosperity and national security while protecting privacy. While this document is not exhaustive of all the privacy protections in the United States, we hope that it can serve as a guide for Americans and our international partners as they engage with ever-evolving technologies. In some places, we have identified areas where individuals may encounter unique issues of privacy and where the next Administration may wish to begin addressing these policy challenges.

II.
Privacy as a Catalyst for Social and Economic Growth in the United States

Privacy gives us space to develop who we are and how we interact with others. We are students and parents. We are individuals and members of a community. We are travelers, foreigners, and citizens. We are homeowners and participants in online worlds. In each context, privacy is what allows us to develop as individuals and to act freely. It is what Warren and Brandeis called our "right to be let alone," which, in turn, gives us the space to realize our "spiritual nature" or our "inviolate personality" free from intrusions by others.

Never has privacy been more important than today, in the age of the Internet, social networks, and smart phones. In just the last decade, the Internet has enabled a renewal of direct political engagement by citizens around the globe and an explosion of commerce and innovation creating jobs for the future. Much of this innovation is enabled by novel uses of personal information. Every day, 2.5 quintillion bytes of data are created related to every aspect of life.[1] This is what technology *can* do; the Obama Administration has laid out guidelines and policies for what technology *should* do, so that your privacy is better protected today.

The policies that this Administration has put in place have built off of the legacy of individual protections put forward since our founding. The right to choose who you associate with, to be secure in your own home, and to be secure in your own thoughts without being compelled to disclose them are all rooted in privacy. Privacy is about much more than just solitude or secrecy, but the feeling of being protected and free to engage in commerce, to participate in the political process, or to seek needed health care. This is why we have laws that protect financial privacy and health privacy and that protect consumers against unfair and deceptive uses of their information. This is why the Supreme Court has protected anonymous political speech, the same right exercised by the pamphleteers of the early Republic and today's bloggers.

Beyond this Administration's privacy achievements, there is more work to be done to secure consumers' private information. In 2015, the Administration released draft legislation to secure consumers' privacy through comprehensive standards and to create a level playing field across technology sectors.[2] If passed, this legislation would serve as a powerful tool to establish expectations and protections for privacy. In the absence of new legislation, some technology

[1] *See* IBM, *What Is Big Data?*, https://www-01.ibm.com/software/data/bigdata/what-is-big-data.html (last visited Dec. 29, 2016).

[2] The White House, Administration Discussion Draft, Consumer Privacy Bill of Rights Act of 2015, *available* at https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

companies and consumer groups have come together to create best practices and codes of conduct for certain industries using the high-level principles and framework the Administration proposed in the Consumer Privacy Bill of Rights.

> *The Consumer Privacy Bill of Rights offers a blueprint to protect individual privacy rights and give users more transparency and control over how their information is handled. It provides organizations with flexible implementation mechanisms, built around a respect for context, to ensure privacy rules keep up with ever-changing technologies. The framework modernizes traditional privacy regulation and practices by introducing seven consumer "Bill of Rights" principles for the digital age: individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability.*[3]

We expect that both the framework and the draft legislation will continue to serve as a guide in the coming years for companies who want to do right by their consumers and for consumers themselves who want to be confident their privacy expectations are met.

Privacy Protections for Individuals

Financial Information Privacy

You now have more control over the privacy of your financial information because of a series of steps brought about by this Administration. Millions of Americans suffer from credit card fraud and identity theft every year. To tackle these problems, in 2014 the President announced the BuySecure Initiative to improve the security of Americans' financial information by encouraging the deployment of new security technologies for payments made in the United States.[4] The Administration has led by example, upgrading all of the Federal Government's consumer payment terminals to accept more secure chip-and-PIN cards, as well as deploying over 3 million of these cards for Federal accounts. Alongside the work of this Administration, credit card companies and banks began deploying at scale more secure chip technology for all charge cards – now making the United States the most robust user of this security technology in the world. Many banks have also partnered with the FICO Alliance to make credit scores more readily available on over 150 million online accounts so that consumers can better monitor their activity for fraud. Further, as part of the BuySecure initiative, the Federal Trade Commission (FTC) has also redesigned IdentityTheft.gov to be the premier resource for victims of identity theft that

[3] The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and promoting Innovation in the Global Digital Economy*, Feb. 2012, *available* at https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[4] President Barack Obama, Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, Oct. 17, 2014, *available* at https://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions.

streamlines the reporting and remediation process with credit bureaus. Together, these steps provide Americans with more understanding of and control over their financial data.

Broadband Privacy

If you are a broadband Internet subscriber, you have more control over your privacy today because of new rules approved by the Federal Communications Commission (FCC) that require broadband providers to get your consent before using and sharing the sensitive information they collect about you over their networks with advertisers or other third parties. In October 2016, the FCC approved new rules that give consumers more control over how Internet Service Providers (ISPs) use their data.[5] Specifically, consumers' privacy is now better protected through rules that require ISPs to affirmatively receive consumer consent to use and share sensitive information, such as web browsing or app usage history. The new rules also require ISPs to give their customers the opportunity to opt-out of the use and sharing of non-sensitive information. Consumers should not have to trade their privacy for the ability to connect to the Internet, and the FCC's rules ensure that consumers will continue to have protections as they increasingly engage online to access the benefits of broadband.

The FCC's broadband privacy rules build on the precedent set by the Open Internet Order. Until 2015, broadband privacy had been enforced primarily by the Federal Trade Commission (FTC). When the FCC reclassified broadband as a Title II "common carrier" service during the Open Internet Order, jurisdiction over broadband privacy shifted from the FTC to the FCC. The new rules combine the FCC's decades of experience protecting consumers' privacy regarding their telephone service with guidance proposed by the FTC for protecting privacy in the digital ecosystem.

Drone Privacy

If you are a U.S. homeowner, your family's privacy is better protected from drones overhead because of the good work done by the National Telecommunications and Information Administration (NTIA), the Federal Aviation Administration (FAA), and six other Federal agencies. In 2015, President Obama issued a Presidential Memorandum on "Promoting Economic Competitiveness while Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems," which directed NTIA to establish a multistakeholder engagement process for developing and communicating best practices with regard to privacy, transparency, and accountability.[6] Heeding the President's call, a diverse

[5] FCC, Report and Order, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, adopted Nov. 2, 2016, *available* at https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-148A1.pdf.

[6] President Barack Obama, Presidential Memorandum, *Promoting Economic Competitiveness while Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems*,

group of stakeholders including drone manufacturers, software developers, technology companies, consumer protection groups, academia, and industries interested in the use of Unmanned Aircraft Systems (UAS) came together to develop a set of best practices for the use of commercial and private UAS. These best practices are being implemented through innovative software on UAS devices and notices to consumers, as well as through education spearheaded by the Federal Aviation Administration.

In addition, with respect to government-operated drones, six Federal entities – the Departments of Defense, Homeland Security, the Interior, Justice, and Transportation, and the National Aeronautics and Space Administration – have put in place privacy policies for their use of UAS. The Department of Homeland Security has also published best practices to provide Federal, state, local, and tribal unmanned aircraft system operators with privacy, civil rights, and civil liberties practices they can consider before initiating an unmanned aircraft program, including increasing transparency around the use of UAS.[7] These guidelines mean that with the proliferation of UAS and the information they will be able to collect, your privacy will be better protected.

Children's Privacy

If you are a parent or guardian, your child's privacy is more strongly protected today because of updates to the Children's Online Privacy Protection Act (COPPA) and strong enforcement actions by the Federal Trade Commission (FTC).[8] Enacted in 1998, COPPA requires the FTC to issue and enforce regulations regarding the online privacy of children under the age of 13, including, among other conditions, by requiring that online services obtain affirmative parental consent for the collection and use of certain kinds of information; provide clear and comprehensive online privacy policies; and protect the confidentiality, security, and integrity of information they collect from children. Children should have the freedom to go online without being coerced into sharing personal information and the freedom to make mistakes without leaving a permanent record. The FTC's enforcement of COPPA ensures that children have the privacy protections necessary to grow and explore the world.

To increase COPPA's power to protect children's privacy, the FTC modernized the COPPA regulations in 2012 to address changes in technology, updated its COPPA FAQs so that both parents and companies have a clear understanding of how COPPA protects children's privacy,

---

Feb. 15, 2015, *available* at https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

[7] DHS, *Best Practices for Protecting Privacy, Civil Rights, and Civil Liberties in Unmanned Aircraft Systems Programs*, Dec. 18, 2015, *available* at https://www.dhs.gov/sites/default/files/publications/UAS%20Best%20Practices.pdf.

[8] *See* Children's Online Privacy Protection Act, Pub. L. 105-277 (codified at 15 U.S.C. §§ 6501-6506) *and* FTC, Children's Online Protection Rule, 16 C.F.R. Part 312.

and brought five enforcement actions under COPPA since it was modernized.[9] While COPPA is only one example of the FTC's privacy guidance and enforcement work, the COPPA rule and its enforcement represent a strong illustration of how the FTC provides all consumers with protection from online intrusions and collection of personal information.

Student Privacy

If you are a student, your privacy is better protected because hundreds of companies have agreed to protect your data in consistent and understandable ways – or face legal action from the FTC. Students now have access to a vast new array of technologies, in part due to the work of the Administration's ConnectED program which is on track to connect 99 percent of America's students to high-speed broadband by 2018.[10] Educational apps, websites, digital textbooks, and other tools, made possible by access to the Internet, individualize the learning experience and provide new modes of instruction, but those same technologies have the capability to track, store, and share students' and educators' data. While this capability may seem worrisome for student privacy, it is also what enables the educational benefit – it is the "personalized" in personalized learning.

That is why, in order to reap the benefits of these technologies while protecting privacy, President Obama endorsed the Student Privacy Pledge, which has been signed by over 250 companies, including some of the Nation's largest, that have agreed to limit collection and sharing of student data.[11] That is also why the Department of Education and its Privacy Technical Assurance Center unveiled a standard for online educational tools' terms of service to guide educators in selecting education technologies for their classrooms that will protect students' privacy. These efforts set out guidance for companies and educators to meet students' expectations of privacy. Students should not have to face a tradeoff between their privacy and the opportunity to benefit from personalized learning; the Student Privacy Pledge ensures that they can have both privacy and better learning tools.

Privacy's Interaction with Public Life

Securing Online Information

Good cybersecurity is essential to privacy – and to the success of the digital economy. Americans must be able to trust that their data is secure and protected from data breaches and

---

[9] *See* FTC, *The Children's' Online Privacy Protection Act (COPPA): What Parents Should Know*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/kids-privacy-coppa (last visited Dec. 29, 2016).

[10] The White House, ConnectEd Initiative, https://www.whitehouse.gov/issues/education/k-12/connected (last visited Dec. 29, 2016).

[11] Future of Privacy Forum, Student Privacy Pledge, endorsed by President Obama Jan. 12, 2015, https://studentprivacypledge.org/ (last visited Dec. 29, 2016).

cyber theft, manipulation, or disruption. Companies and individuals also have their own role to play in protecting privacy. Companies can reduce the risk of data breaches by implementing proactive cybersecurity measures. By adopting good cybersecurity practices, consumers can protect not only themselves and their families, but also their entire networks of online contacts.

Business owners have a responsibility to keep their customers' and employees' information secure, and can better do so by following standards and best practices laid out by the National Institute of Science and Technology (NIST), FCC, and FTC. NIST has released an easy-to-use risk-assessment guide to help businesses evaluate the proactive security steps they should take so that organizations do not have to invent standards for strong cybersecurity practices from the ground up. A NIST partnership with the FTC has provided guidance specifically focused on small businesses, so that when business owners visit any of the Small Business Administration (SBA) regional offices in the United States, they can receive practical, real-time advice on steps to secure their business, employees, and customers. Likewise, the broadband privacy rules voted on by the FCC in October 2016, and modeled on the NIST guidance, require ISPs and other telecommunications companies to protect the security of their subscribers' personal information, including your web browsing and app usage history and your telephone call detail records. Similarly, the FTC has released a host of guidance materials for businesses, including a Start with Security guide, a guide for mobile app developers, and a guide for IoT companies.

NIST's Cybersecurity Framework functions as a voluntary how-to guide for organizations in the critical infrastructure community to enhance their cybersecurity. It provides standards, guidelines, and practices to promote the protection of critical infrastructure.[12]

The Administration has also partnered with industry, academia, civil society, and security professionals to tackle cybersecurity issues. Engagements through NTIA's multistakeholder process have produced initial findings, recommendations, and resources that will enhance cooperation on vulnerability disclosure, which will help organizations to better understand and fix flaws in their security and data protection systems.[13] Likewise, consistent with the Cybersecurity Information Sharing Act (CISA), the Department of Homeland Security (DHS)'s Automated Indicator Sharing (AIS) initiative enables the exchange of cyber threat indicators between the Federal Government and the private sector while offering new protections for personally identifiable information (PII) and other sensitive information not directly related to the cybersecurity threat.[14] Today, there are more tools available to help business owners –

[12] NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, v.1, Feb. 12, 2014, *available* at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[13] *See* Deputy Assistant Secretary of Communications and Information Angie Simpson, NTIA Blog, https://ntia.doc.gov/blog/2016/improving-cybersecurity-through-enhanced-vulnerability-disclosure (last visited Dec. 29, 2016).

[14] *See* DHS, Automated Indicator Sharing (AIS), https://www.dhs.gov/ais (last visited Dec. 29, 2016).

whether they be individuals running small business or executives of multinational corporations – improve cybersecurity and handle your data securely.

Consumers themselves can also take steps to keep their data – and the data of everyone else in their networks – secure. Innovative tools that companies are offering as a part of the Administration's security campaign ensure that Americans are better informed about how to secure their digital information and protect themselves and others online. That is why the Administration, working with the National CyberSecurity Alliance, supported a public campaign, called "Lock Down Your Login," to educate consumers on simple steps they can take to strengthen the security of their online accounts through stronger authentication.[15] "Lock Down Your Login" is a follow-on campaign to the DHS's Stop.Think.Connect, a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online.

Moreover, the Department of State has worked to improve global cybersecurity, benefiting businesses and consumers at home and abroad, by promoting the widespread adoption of cybersecurity best practices around the world; assisting in cyber capacity building exercises with foreign partners; enhancing cooperative international partnerships to mitigate and deter cyber threats; and supporting a strategic framework of international cyber stability.

Citizens Accessing Government Services

More of your life takes place online than ever before, and that includes the way you access government services. With this in mind, the Administration has prioritized good cybersecurity practices and strong privacy protections for data held by the government. Despite ever emerging threats, the Federal Government is better prepared than ever before to protect the data of American citizens. If you are a citizen accessing government services – applying for a passport, applying for health insurance, or submitting your tax returns, for instance – your privacy is more strongly protected today because of improvements to the way the Federal Government manages personal data, including reducing – and in some cases eliminating – the use of social security numbers on Federal forms and new agency guidance on how to protect against and respond to data breaches.

Because effective protections for citizens' data requires coordination across Federal agencies, the Administration has set up bodies to facilitate cross-cutting agency engagement on privacy and security policies. The Federal Privacy Council, established by Executive Order, is a new government body charged with overseeing and improving government privacy practices across agencies.[16] Further, the President's Cybersecurity National Action Plan directs government

---

[15] National CyberSecurity Alliance, Public Service Campaign, https://www.lockdownyourlogin.com/ (last visited Dec. 29, 2016).

[16] President Barack Obama, Executive Order 13719, *Establishment of the Federal Privacy Council*, Feb. 9, 2016, *available* at https://www.whitehouse.gov/the-press-office/2016/02/09/executive-order-establishment-federal-privacy-council.

agencies to secure information technology systems and citizen accounts and to raise the level of cybersecurity across the country by investing in information technology modernization and upping the cybersecurity capabilities and level of talent in the Federal workforce.

In February 2016, the Administration established the first-ever Federal Privacy Council as the principal interagency forum to improve the Government privacy practices of agencies and entities acting on their behalf. The establishment of the Privacy Council helps Senior Agency Officials for Privacy better coordinate and collaborate, educate the Federal workforce, and exchange best practices. The Federal Privacy Council has also released a new website to encourage coordination across government programs as well as to increase public awareness of Federal privacy policies and steps agencies have taken to protect individuals' data.[17]

Equal Opportunity and Civil Rights

This Administration has taken steps to ensure that the right to privacy is available to every person no matter their ethnicity, race, gender, national origin, religion, sexual orientation, or gender identity. Furthermore, the Administration laid out principles for protecting against discriminatory uses of data and surveillance capabilities. In 2015, a Presidential Memorandum directing Federal agencies to establish policies for the use of UAS also required that any Federal agency wishing to use UAS technology must ensure that their "collection, use, retention, or dissemination of data" from UAS is not discriminatory on these bases.[18] Furthermore, in "Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights," the Administration laid out principles for "equal opportunity by design" in data systems, to ensure that they are built to protect against discrimination.[19]

In 2016, the Administration released "Big Data: A Report on Algorithmic Systems, Opportunity and Civil Rights" to comprehensively address how changes in business models brought on by the digital ecosystem impact and interact with consumer protections that were passed in the Civil Rights Era. The report charts pathways for fairness and opportunity but also cautions against re-encoding bias and discrimination into algorithmic systems.

[17] Visit the Federal Privacy Council's website at https://www.fpc.gov/.

[18] *Supra*, note 7.

[19] The White House, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, May 2016, *available* at https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf.

III.
Protecting Privacy in the Global Digital Economy

Global economic growth requires consumer confidence, and consumer confidence requires clear, appropriate privacy protections. Thus, as the global economy goes digital and cross-border data flows have grown exponentially, this Administration has worked to ensure that data can be transferred internationally with stronger privacy protections for people around the world.

International Commercial Privacy

Transatlantic Commercial Privacy

The Administration's work to put in place the EU-U.S. Privacy Shield Framework represents a significant achievement for data protection for individuals and for U.S. and European Union (EU) businesses.[20] Today, if you are an EU citizen buying American goods online or using a U.S. website, your privacy is more protected because thousands of companies, including many of the Nation's largest firms, are participating in the EU-U.S. Privacy Shield, providing you with comprehensive privacy protections backed up by strong FTC enforcement and multiple options for redress. Likewise, if you are an EU citizen concerned that U.S. signals intelligence activity may have resulted in the mishandling or misuse of your data transferred to a company in the United States under Privacy Shield, you can now seek redress from the Privacy Shield Ombudsperson at the U.S. Department of State.

The EU-U.S. Privacy Shield Framework is a framework designed by the Obama Administration and European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce.

The Privacy Shield framework is a key part of the Administration's efforts to ensure that cross-border commercial data transfers are conducted in accordance with the highest standards of personal data protection. Privacy Shield supports data flows that underpin the United States' largest trade and investment relationship, supporting $290 billion in digital services traded annually between the United States and Europe and paving the way for future growth in the

[20] For more information visit the EU-U.S. Privacy Shield website at https://www.privacyshield.gov/welcome; Privacy Shield Framework, EU-U.S., 2016, *available* at https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg.

digital arena and more broadly.[21] The ability to share data, products, services, and other information across borders is essential for individuals and companies across all sectors in the 21st century. Data flows support supply chain connectivity; enable global business operations; and allow companies of all types and sizes to train, promote, and pay employees around the world.

The United States and the EU both have strong privacy protections, but they are rooted in distinctly different legal frameworks for privacy. To bridge this gap, in July 2016, after more than two years of negotiations, the United States and the EU finalized Privacy Shield, creating certainty for companies, and protecting privacy for consumers on both sides of the Atlantic. Privacy Shield provides a legal mechanism for transatlantic data transfers consistent with EU data privacy law, benefiting both consumers and business in the global economy.[22] Companies participating in Privacy Shield commit to applying robust and enforceable protections for personal data under the program, with those commitments being enforceable under U.S. law. Privacy Shield ensures transparency regarding how participating companies use personal data, provides for strong U.S. Government oversight, and increases cooperation between U.S. authorities and EU data protection authorities. Privacy Shield offers EU individuals access to multiple avenues to address concerns regarding participants' compliance with the Framework, including free dispute resolution. Privacy Shield also ensures the same level of protection when personal data is transferred to third parties.

Privacy Shield is underpinned by the United States' strong limitations and safeguards on national security and law enforcement access to data. In connection with the finalization of Privacy Shield, the United States has laid out in writing the robust protections and safeguards established by Presidential Policy Directive 28 on Signals Intelligence; the multiple layers of constitutional, statutory, and policy safeguards that apply to U.S. signals intelligence activities; and descriptions of the oversight all three branches of the United States Government provide. Likewise, the Department of Justice provided an overview regarding limits on United States Government's access to commercial data and other record information held by corporations in the United States for law enforcement and public interest purposes. Finally, Privacy Shield includes a specific channel for EU individuals to raise questions regarding access to their data through signals intelligence activities. This Administration has established a new Ombudsperson at the State Department through whom EU individuals will be able to submit inquiries regarding United States access to their data through signals intelligence, and has committed to respond to appropriate requests consistent with our national security obligations.

---

[21] U.S. Dept. of Commerce Sec. Penny Pritzker, Keynote Address, *Digital Privacy and Security at Council of Foreign Relations*, Nov. 16, 2016, transcript at https://www.commerce.gov/news/press-releases/2016/11/us-secretary-commerce-penny-pritzker-delivers-keynote-address-digital (last visited Jan. 4, 2017).

[22] *Supra*, note 21.

Commercial Privacy in Asia

The Administration's commitment to protecting privacy also extends to the Asia-Pacific region. If you are a citizen of one of the Asia Pacific Economic Cooperation (APEC) economies that is a participant in the APEC Cross-Border Privacy Rules (CBPR) System, a multilateral framework for privacy protection, your privacy is more strongly protected today. On November 20 in Lima, Peru, APEC leaders recognized the importance of implementing the CBPR system, helping facilitate trade and economic growth through enhancing digital trade and strengthening consumer privacy protections across the Asia Pacific region.[23] The CBPR system was developed by participating APEC economies after seeking the views of industry and civil society, to build consumer, business and regulator trust in cross border flows of personal information.[24] The CBPR system requires participating businesses to develop and implement data privacy policies consistent with the APEC Privacy Framework, with requirements generally similar to those under Privacy Shield, and enforced by the FTC. The United States has also sought multilateral endorsement of strong protections for personal data in other fora in order to promote digital trade. On September 5 in Hangzhou, China, the G-20 Leaders endorsed applicable frameworks for privacy and personal data protection to strengthen confidence and trust in the digital economy and to enable the free flow of data.

Privacy, National Security, and Law Enforcement

The Administration's efforts to promote the privacy of persons around the world in the commercial sphere is reinforced by the unprecedented steps the President has taken to ensure that privacy is respected regardless of nationality, while ensuring the safety and security of all Americans. These efforts are rooted in the Administration's belief that all persons should be treated with dignity and respect, regardless of their nationality or place of residence, and that all persons have a fundamental interest in privacy.

Legislative Reforms

If you are an American citizen, you have stronger privacy protections today because of steps this Administration has taken to reform the government's surveillance policies. In 2015, President Obama signed into law the USA FREEDOM Act.[25] Among other things, this ended the U.S. Intelligence Community's collection of bulk telephony metadata under Section 215 of the USA PATRIOT Act. In its place, the USA FREEDOM Act created a more targeted approach whereby the United States Government no longer acquires data under this statute in bulk, but instead accesses call records held by telecommunications providers, generally after receiving judicial permission to do so. The USA FREEDOM Act also created a panel of court-appointed lawyers

[23] APEC, *2016 Leaders' Declaration*, Nov. 20, 2016, Lima, Peru, http://www.apec.org/Meeting-Papers/Leaders-Declarations/2016/2016_aelm.aspx (last visited Jan. 4, 2017).

[24] APEC, *Cross Border Privacy Rules System*, http://www.cbprs.org/ (last visited Jan. 4, 2017).

[25] USA Freedom Act of 2015, Pub. L. 114-23 (codified at 50 U.S.C. § 1861).

who can advocate for greater privacy protections in significant or novel Foreign Intelligence Surveillance Court (FISC) proceedings and mandated additional transparency by requiring the government to publicly disclose significant FISC decisions related to surveillance capabilities authorized under the Foreign Intelligence Surveillance Act (FISA).

> *The USA FREEDOM Act strengthens civil liberty safeguards and provides greater public confidence in U.S. surveillance programs, including by prohibiting bulk collection through the use of Section 215, FISA pen registers, and National Security Letters and by providing the American people with additional transparency measures.*[26]

Intelligence Community Transparency

Today, whether you are a U.S. citizen or a non-U.S. citizen abroad, you now have more confidence about what the United States does and does not do with regard to signals intelligence collection because of steps this Administration has taken to provide an unprecedented level of transparency regarding these activities. The Office of the Director of National Intelligence (ODNI) now maintains a public website (through its transparency and public outreach initiative tumblr site "*IC on the Record*") that provides the public direct access to information related to foreign intelligence surveillance activities of the United States.[27] Over the past three years, the ODNI has released through *IC on the Record* thousands of pages of previously classified documents related to the government's surveillance capabilities and activities. For example, the ODNI has publicly released the minimization procedures used by the U.S. Intelligence Community (IC) for collection under Section 702 of the Foreign Intelligence Surveillance Act. In addition, the ODNI has published the *Principles of Intelligence Transparency for the Intelligence Community*, which the IC is now implementing through a range of initiatives designed to enhance public understanding of the IC – particularly its rules and oversight framework – while continuing to protect national security information.[28]

Signals Intelligence Reform

The President's commitment to strengthening privacy protections for all citizens while preserving important tools that keep citizens safe is enshrined in Presidential Policy Directive 28

---

[26] President Barack Obama, Press Release, *Statement by the President on the USA FREEDOM Act*, June 2, 2015, *available* at https://www.whitehouse.gov/the-press-office/2015/06/02/statement-president-usa-freedom-act.

[27] Office of the Director of National Intelligence's transparency website is available at https://icontherecord.tumblr.com/.

[28] ODNI, *Principles of Intelligence Transparency for the Intelligence Community*, Oct. 27, 2015, *available* at https://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles/80-dni/dni-ic/1169-intelligence-transparency?tmpl=component&format=pdf.

(PPD-28), which was issued in January 2014.[29] Among other things, the directive set forth the principles that govern how the United States conducts signals intelligence collection, limited the use of signals intelligence collected in bulk to six specific enumerated purposes; and required an annual senior-level review of signals intelligence priorities and requirements, taking into account national security interests, privacy concerns, and our partnerships abroad.

While the United States has unique capabilities with regard to signals intelligence collection that protect not only the United States, but our friends and allies as well, U.S. global leadership demands that we meet our security requirements while also maintaining trust and cooperation among people and governments around the world. Furthermore, PPD-28 and the protections it includes serve as an essential foundation for Privacy Shield, directly supporting jobs and economic growth in the United States. To these ends, the President took the unprecedented step of extending certain privacy protections afforded to Americans to people around the world. In particular, PPD-28 requires that U.S. signals intelligence activities include safeguards for the personal information of all individuals, regardless of nationality. These safeguards include limits on the duration we can hold personal information, while also restricting the use of this information. No other country has provided such assurances, extended such protections to citizens of other nations, or demonstrated such unprecedented transparency regarding its intelligence activities.

PPD-28 lays out the principles that govern how the United States conducts signals intelligence collection, and strengthened executive branch oversight of U.S. signals intelligence activities. PPD-28 ensures that the United States takes into account our security requirements, but also our alliances; our trade and investment relationships, including the concerns of our companies; and our commitment to privacy and basic liberties.

Law Enforcement Cooperation

Unprecedented steps have been taken on both sides of the Atlantic to enhance the ability of law enforcement agencies in the United States and Europe to cooperate with each other to combat crime and terrorism, while upholding the highest standards of privacy protection. To this end, this Administration has also taken important steps to ensure that personal data transferred to the United States in the context of law enforcement cooperation will be appropriately protected.

In a landmark step for transatlantic law enforcement cooperation, in June 2016 the United States and EU signed the Data Protection and Privacy Agreement (DPPA). The DPPA will protect the security and the privacy of citizens on both sides of the Atlantic by setting out protections for personal information that is passed between the United States and European Union Member States for the purpose of preventing, investigating, or prosecuting crimes, including terrorism. The DPPA provides for mutual respect between EU and U.S. law enforcement data privacy

[29] President Barack Obama, Presidential Policy Directive 28, *Signals Intelligence Reform*, Jan. 17, 2014, *available* at https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

frameworks, and clarifies the application of U.S. and EU data protection measures to existing law enforcement cooperation agreements. Before finalizing the Agreement, the EU requested that EU citizens be allowed to seek redress in U.S. courts for major privacy violations related to personal information covered by the DPPA. In order to provide this protection to our EU partners and ensure strong transatlantic law enforcement cooperation, this Administration worked with Congress on the Judicial Redress Act of 2015, which the President signed into law in February 2016, highlighting the United States' commitment to ensure that personal "data is protected in the strongest possible way with our privacy laws -- not only American citizens, but also foreign citizens."[30] This means that if you are an EU or U.S. citizen involved in a law enforcement investigation involving cooperation between the United States and an EU Member State, your privacy will be protected by the U.S.-EU Data Privacy Protection Agreement (DPPA), once it enters into force. Likewise, once the necessary designations have been completed, if you are an EU citizen, you will be able to seek redress in U.S. courts for certain violations of the Privacy Act in the same manner as U.S. citizens.

The DPPA sets high standards for the protection of personal data transferred by law-enforcement authorities between the United States and the EU. It also strengthens legal certainty and enhances the rights of citizens which in turn will facilitate EU-U.S. cooperation to combat crime, including terrorism. The EU and the United States have committed to work together in the implementation of this agreement to ensure that it benefits both citizens and law enforcement cooperation.

Similarly, the United States and the EU are working together to protect personal data in other law enforcement contexts. In December 2011, the United States and the European Union signed an agreement on the use and transfer of airline Passenger Name Records (PNR) to DHS.[31] After ratification by the European Parliament, the agreement entered into force on July 1, 2012. Conclusion of the PNR agreement, governing the use of air passenger data for the prevention, detection, investigation, and prosecution of terrorism and other serious, transnational crimes was a significant step forward in strengthening transatlantic cooperation to protect international travelers while respecting our commitment to privacy and data protection. Specifically, the PNR agreement provides strong assurances as to how EU citizen data transferred to the United States under the agreement will be protected, with restrictions on what PNR data can be used, how long it is retained, and how it can be transferred to other agencies.

[30] President Barack Obama, Press Release, *Remarks by the President at the Signing of the Judicial Redress Act Bill*, Feb. 24, 2016, *available* at https://www.whitehouse.gov/the-press-office/2016/02/24/remarks-president-signing-judicial-redress-act-bill; *See also*, Judicial Redress Act of 2015, Pub. L. 114-126.

[31] Passenger Name Records Agreement, U.S.-European Union, Dec. 14, 2011, *available* at https://www.dhs.gov/sites/default/files/publications/privacy/Reports/dhsprivacy_PNR%20Agreement_12_14_2011.pdf.

In July 2016, the Administration also submitted a legislative package to Congress that would enable bilateral treaties with countries with similarly strong protections for privacy and due process in order to better facilitate those countries' legitimate requests for data stored in the United States and vice versa. Currently, if foreign countries require for law-enforcement purposes data from U.S. companies, they must request it via the time-consuming Mutual Legal Assistance (MLA) process. U.S. companies also may face conflicting legal obligations when foreign governments require them to disclose information that U.S. law prohibits them from disclosing. The proposed legislation would create a more streamlined process that would permit our foreign partners to have timely access to the information of non-U.S. persons located outside of the United States relating to serious crimes, such as terrorism, that is stored on infrastructure located in the United States, provided they are able to demonstrate that they have met specific thresholds to ensure they provide robust protections for privacy and civil liberties. The United States has some of the strongest privacy protections around the world, and this effort would enhance public safety while encouraging improvement of global privacy protections.

IV.
Areas for Further Attention

The progress that this Administration has made over the past eight years, coupled with the challenges that we have faced, illustrates how the privacy of both Americans' and non-Americans' information will continue to be a paramount consideration for policymakers. As President Obama has said,

> One thing should be clear, even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever.

Americans' relationship with technology will continue to change, but what has remained unwavering is the United States' commitment to protecting privacy. It is fundamental to individual dignity and participation in a democratic society. Further, privacy protections strengthen the digital economy by building trust in the Internet and other networked technologies. While we do not have the ability to predict every impact that technology will have on the daily lives of people around the world, there are overarching trends that we have witnessed over the last eight years and that we expect will continue in the future.

1) Technology will pose new consumer privacy and security challenges.

It is inevitable that technology will continue to drive innovation and economic growth. We expect tools for consumer privacy and security to follow a similar path. Consumers are changing their expectations for how their data is collected and used. Some companies are beginning to "bake in" privacy to their products, but a fundamental concern for policymakers should remain whether there is sufficient transparency and education to enable consumers to make informed choices.

Because companies from more traditional economic sectors are increasingly offering networked products, there may be increased need for a baseline set of principles that govern consumer privacy expectations and protections. Baseline principles not only set a foundation for consumers to understand and exercise their rights, but also create a level playing field for all companies. Frameworks like the Consumer Privacy Bill of Rights offer strong protections for consumers, based on the notion that consumers have rights over data about them and that they themselves produce, but also reflect the fact that in many contexts consumers are willing to allow collection and use of their information in order to benefit from innovative and tailored products.

2) Emerging technology may simultaneously create new challenges and opportunities for law enforcement and national security.

In the last two years alone, people have created over 90% of the data that exists in the world. The influx of new applications that allow people to create and communicate helps them keep a record of their lives where in the past they may have forgotten a conversation or an uncaptured moment. These records, properly obtained through court orders, can offer law enforcement insight not previously possible. For instance, photographs of hotel rooms are helping the FBI identify sex trafficking routes, and a cellphone's recorded GPS location can offer proof of an accused's innocence. Technology has the ability not only to solve previously unsolvable crimes, but also to offer recorded evidence in the judicial process.

As technology offers law enforcement greater ability to investigate crime, this Administration has consistently committed to ensuring that Americans' privacy protections are upheld regardless of the method used by police to conduct investigations. To this end, the Administration has long been a champion of modernizing the Electronic Communications Privacy Act to ensure that the standard of protection for online, digital content is consistent with that afforded in the physical world – including by removing archaic distinctions between email left unread or over a certain age. The Administration has been encouraged by the reform efforts led by bipartisan support in Congress, and hopes that legislators will continue to work towards a modernization proposal.

Even though law enforcement has access to new methods of data collection, technology may also sometimes limit law enforcement's ability to access data for which it has valid legal authority. Successful navigation of the opportunities provided by technologies that enhance privacy and security, and the challenges surrounding law enforcement access to data requires consideration of all of the equities, including public safety, cybersecurity, economic competitiveness, free speech and human rights, and the personal privacy of Americans.

3) The digital economy is making privacy a global value.

For decades the United States has supported a liberal international system of governance premised on the free flow of information and policies that would enable technologies to grow and flourish globally. In our record of supporting innovation, we have found that building consumer trust and protecting individuals' personal information encourages consumers to utilize new technologies and reap the benefits of participating online. The United States has one of the strongest records of commercial privacy enforcement through the work done by the Federal Trade Commission. The United States also has robust due process protections around the world by requiring law enforcement officers to have probable cause, signed off by an impartial judge, to obtain a warrant for the contents of communications and certain online activities. These protections are fundamental to our democracy. As the President has said,

> We pioneered the Internet, but we also pioneered the Bill of Rights, and a sense that each of us as individuals have a sphere of privacy around us that should not be breached, whether by our government, but also by commercial interests. And since we're pioneers in both these areas, I'm confident that we can be pioneers in crafting the

kind of architecture that will allow us to both grow, innovate, and preserve those values that are so precious to us as Americans.

This architecture of innovation and privacy protection is fundamental to a free and open global Internet and the ability of the digital economy to connect us across borders. Strong privacy protections and minimal barriers to the flow of information and services across borders is the lynchpin of the digital economy. With governments that similarly support the protection of their citizens' privacy rights, we have shown our continued respect for each other's citizens in our different legal systems through frameworks like Privacy Shield. Recently, some governments around the world have mandated proscriptive regulations that impede the free flow of data and deny their citizens privacy and free expression online. These measures include limiting Internet routing and data storage to particular jurisdictions and limiting the kinds of content and data types that are permitted online. As a result, companies operating, or attempting to operate, in those jurisdictions face a host of barriers to information flows in the international marketplace. Examples of such barriers include forced localization requirements, market access limitations, and censorship. For such countries, the United States continues to raise the bar and push for endorsement of privacy and data protection principles; freedom of expression; and the free flow of information, ideas, and knowledge through the G20, G7, and other multilateral processes. Protecting privacy and promoting the global exchange of information will ensure the digital economy continues to drive innovation, economic growth, and social prosperity.

4) Consumers' voices are being heard –and must continue to be heard – in the regulatory process.

Privacy is becoming an increasing concern for law and policymakers and there are opportunities for consumers to interact with the policy process to make their views on privacy, security, and consumer control known. Millions of Americans submitted comments to the FCC to voice their support for a free and open Internet. Then in subsequent rulemaking for broadband privacy, over 275,000 consumers and companies filed comments to voice their opinions. This ability is not limited to the FCC rulemaking process and citizens are able to file comments for any regulation proposed by the Federal Government that might have privacy implications. In fact, this Administration has taken steps to encourage civic participation in the government process by starting the We The People petition portal.[32] In 2014, over 100,000 consumers petitioned the government to protect consumer choice and make cell phone unlocking legal, leading to the first ever legislative fix created by this civic engagement tool. The ability for the public to participate directly with the government leads to stronger policies to protect innovation and individuals' rights. Additionally, if a consumer feels that a company is engaging in unfair or deceptive actions online, they can submit a complaint to the Federal Trade Commission to encourage the FTC to investigate the matter.

[32] Create, sign, and read responses to public petitions at https://petitions.whitehouse.gov/.

5) The Federal Government benefits from hiring more privacy professionals.

As innovation and technology impact all sectors of our economy, it becomes increasingly necessary for Federal agencies to hire staff familiar with privacy issues in order to create a robust policy process that can balance competing economic values. Agencies have long had professionals with experience in privacy, but the changes we face require full-time professionals to tackle multidisciplinary challenges that cut across law, technology, and policy. The new Federal Privacy Council, which was established by presidential Executive Order on February 9, 2016, has focused significant energy on developing the future workforce, both by creating and developing educational programs for the staff already tackling these issues and by developing model position descriptions, a new privacy position toolkit, and competency models for the development and hiring of future Federal privacy professionals. These professionals enable the government to properly deploy the full benefits of technological innovation while ensuring that the government continues to respect the privacy rights of those it serves.

6) Transparency is vital for earning and retaining public trust.

The public expects more transparency than ever before to understand how personal information is collected and used, by both companies and the government. In order for our economy to continue to grow and succeed, the public must trust that personal information is being used appropriately and responsibly. Likewise, the public expects that the successful monitoring of national security threats to protect the public must include respect for privacy. The right to privacy is closely linked with free speech; and because democracy depends on robust political participation, the checks and balances on our surveillance capabilities must ensure that freedom of expression and freedom of association are protected while ensuring that our law enforcement and national security professionals have the tools they need to counter threats to our national security. This Administration has taken significant steps to increase transparency in government – from the Presidents' first memorandum to agencies to encourage open government principles to ODNI's transparency reports on U.S. surveillance activities on *IC on the Record*.

7) Privacy is a bipartisan issue.

Consumer advocates for commercial and governmental privacy education and protections range across the political spectrum. Privacy is not exclusively a Democratic or Republican value. It has served as a rallying point for Members of Congress to "cross the aisle" and create strong policies that protect their constituents. It is a fundamentally American freedom to be secure in your person and property whether it be in your home, your community, or with friends and family abroad. As President Obama has remarked on the state of consumer security,

> This is not a Democratic issue, or a Republican issue. This is not a liberal or conservative issue. Everybody is online, and everybody is vulnerable. The business leaders here want their privacy and their children protected, just like the consumer and privacy advocates here want America to keep leading the world in technology and be safe from attacks.

V.
CONCLUSION

For the past 240 years, the core of our democracy – the values that have helped propel the United States of America – have remained largely the same. We are still a people founded on the beliefs of equality and economic prosperity for all. The fierce independence that encouraged us to break from an oppressive king is the same independence found in young women and men across the country who strive to make their own path in this world and create a life unique unto to themselves. So long as that independence is encouraged, so long as it is fostered by the ability to transcend past data points and by the ability to speak and create free from intrusion, the United States will continue to lead the world. Privacy is necessary to our economy, free expression, and the digital free flow of data because it is fundamental to ourselves.

Privacy, as a right that has been enjoyed by past generations, must be protected in our digital ecosystem so that future generations are given the same freedoms to engage, explore, and create the future we all seek.