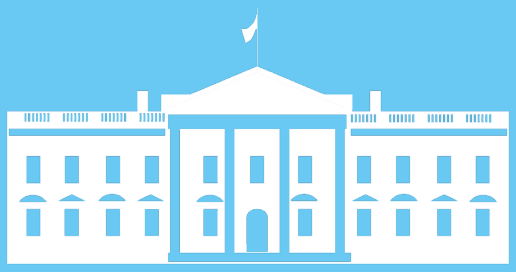
CENTER FOR DEMOCRACY & TECHNOLOGY

TECH POLICY PRIORITIES FOR THE



NEW ADMINISTRATION

NOVEMBER 2016

WHO WE ARE

A nonprofit advocacy organization, CDT works to promote democratic values by shaping technology policy and architecture, with a focus on the rights of the individual. CDT supports laws, corporate policies, and technological tools that protect privacy and security and enable free speech online. Based in Washington, D.C., and with a presence in Brussels, CDT works inclusively across sectors to find tangible solutions to today's most pressing technology policy challenges. Our team of experts includes lawyers, technologists, academics, and analysts, bringing diverse perspectives to all of our efforts.

To learn more about us, please visit our website at cdt.org/about.

CENTER FOR DEMOCRACY & TECHNOLOGY

Dear President-Elect Trump:

In your victory speech on election night, you said, “It is time for us to come together as one united people. It’s time.” At the Center for Democracy & Technology, we agree.

We believe that there are core beliefs that unite every American. The right to privacy, to be left alone in society without the government tracking your movements or communications. The right to free expression, to speak freely without fear of retribution in public or online. The right to be secure, to have the best protections against cyber criminals and hackers.

Attached are a series of policy recommendations for you as our nation’s 45th president. They are moderate, pragmatic proposals aimed at firmly establishing America’s role as the global leader in both innovation and internet freedom. As your Administration assumes leadership of the government, we encourage you to chart a forward-looking course that protects our individual rights, keeps the country secure, and enables further innovation in our hyper-connected reality.

Privacy and National Security. On the internet, cybersecurity has become a crucial component of national security. America’s global reputation continues to suffer harm from revelations of mass spying. You must recognize this reality. We urge you to take the following measures to protect privacy and national security:

1. State a strong commitment to advancing encryption as a linchpin to internet security and reject backdoors or other efforts to weaken encryption;
2. Create a climate where security research can flourish and vulnerabilities can be quickly identified and patched;
3. Reform NSA surveillance, including stopping warrantless spying on Americans; and
4. Safeguard the contents of domestic communications from federal and state law enforcement.

U.S. Global Leadership on Internet Freedoms. The U.S. is a leader in promoting internet rights around the world, and today free expression is under attack from a variety of proposals aimed at monitoring the web and enabling censorship. You can protect the global internet in the following ways:

1. Reject policies that force companies to unduly monitor their users and report on suspicions of terrorism;
2. Oppose de facto censorship where the government seeks to use the terms of service of intermediaries to stifle speech;
3. Assure that demands from governments for citizens’ communications meet strong human rights standards; and
4. Protect the open internet rules.

CENTER FOR DEMOCRACY & TECHNOLOGY

Responsible Use of New Technology. Connected devices and data analysis continue to become more prevalent and sophisticated. These advancements require policy solutions that address inequality and user trust. You can:

1. Combat the potential for technology to exacerbate inequality and lead to discrimination in automated systems;
2. Cultivate technological talent within the federal government; and
3. Improve data protection both by pushing for comprehensive privacy legislation and by supporting privacy initiatives in individual sectors.

We are committed to working with your Administration where possible. Even more so, we are committed to ensuring that technology advances the civil rights of everyone, and that it serves as an empowering and equalizing force. We are ardent defenders of civil liberties and will be vocal advocates against any attempt to leverage the internet or technology to infringe upon them. We hope we can join together to safeguard our shared values and protect the freedoms upon which not just the internet but our very nation was founded.

Sincerely,

Nuala O'Connor
President and CEO
Center for Democracy & Technology

CENTER FOR DEMOCRACY & TECHNOLOGY

Privacy and National Security

In today's hyper-connected world, security on the internet is rapidly evolving. National security will always be a key priority, and it cannot be considered as something separate from advancing strong privacy and cybersecurity. The unending torrent of data breaches combined with the interconnected nature of critical systems represents an ongoing vulnerability of both the American economy and the privacy and security of individual Americans.

We must also recognize that America's global interests are not well-served by mass, untargeted government surveillance. While the 114th Congress enacted the first legislation to roll back a government surveillance program in a generation, there is still more work to be done. With the country continuing to grapple with and address the serious civil liberties implications of mass surveillance, the next Administration must remain focused on national security efforts that keep the country safe and protect our fundamental freedoms.

The government can keep people safe while engaging in targeted surveillance that does not undermine communications security. It can also protect researchers whose work promotes that security. Detailed below are the core issues we encourage the incoming Administration to act on when addressing the issue of privacy and security in the digital age.

1. Protect Strong Encryption

Encryption policy has been at the core of technology and national security for decades. It is essential to protecting sensitive information and the rights of citizens living under authoritarian regimes. At the same time, some law enforcement officials - led by FBI Director James Comey - have argued that encryption hinders law enforcement and makes it harder to access information as part of criminal investigations. This resurgence of the "Crypto Wars" of the 1990s has sparked renewed debate about encryption. Industry and civil society have been unwavering in their support for strong encryption because it forms the basis for all internet communication, commerce, and security. It will be crucial to our nation's security and economic success for the President to articulate a policy stance that works to protect strong encryption.

Action: In the first 100 days the President should pledge that: 1) there will be no explicit or implicit mandates for backdoors or key recovery systems; and, 2) the United States will discourage through diplomatic means extraterritorial requests from other governments that require services to build backdoors or key recovery systems.

Action: In the first 100 days the President should form an interagency commission to determine alternatives to subverting strong encryption standards that will assist law enforcement, including additional funding for technical support at the federal, state, and local levels.

CENTER FOR DEMOCRACY & TECHNOLOGY

Further Background:

- Center for Democracy & Technology, "Issue Brief: A 'Backdoor' to Encryption for Government Surveillance" (March 2016)
- Center for Democracy & Technology, "CALEA II: Risks of Wiretap Modifications to Endpoints" (May 2013)

2. Improve the Process for Discovering Security Vulnerabilities

Strong cybersecurity depends on extensive, ongoing research and the ability to share information about potential vulnerabilities and effective mitigations. Software producers and cybersecurity researchers must work together to discover and mitigate vulnerabilities. Unfortunately, such collaborative partnerships rarely exist. Moreover, laws such as the Computer Fraud and Abuse Act (CFAA), Section 1201 of the Digital Millennium Copyright Act (DMCA), the Electronic Communications Privacy Act (ECPA), and their state counterparts can subject cybersecurity researchers to criminal and civil liability for using technology in an "unauthorized" manner. This can chill good-faith security research and expose researchers to disproportionate, uncertain, or unjust penalties. The result is continuing vulnerability and researchers who are reluctant to explore or disclose their findings.

It will be important for the new Administration to clearly signal that security research and vulnerability mitigation are important features in shoring up global cybersecurity. The new Administration should state that security research is valuable to national security and the economy, as fewer vulnerable products mean less waste, less fraud and malicious activity, and fewer errors that could have catastrophic results.

Action: In the first 100 days, the President should direct the Department of Justice to issue guidelines for prosecutors that clearly identify those narrow cases of illegal hacking that are properly subject to the CFAA. This would give "tinkerers" and good-faith researchers more certainty as to the scope of the law. A presidential task force should be formed to study the kinds of activities and sources of statutory power that lead to chilling effects, and consider penalties for misuse of civil statutes to threaten researchers.

Action: The President should work with Congress to amend statutes like the CFAA to offer a clear safe harbor for good-faith forms of security research. The new Administration should promise to veto any bill that would potentially increase chilling effects on security researchers.

Further Background:

- "Cybersecurity Research: Addressing the Legal Barriers and Disincentives," Report of a Workshop convened by the Berkeley Center for Law & Technology, the UC Berkeley School of Information and the International Computer Science Institute (September 2015)
- Center for Democracy & Technology, "A Deep Dive on the Final CISA Guidelines" (June 2016)
- Center for Democracy & Technology, "All Bots Must Die: How a New Senate Bill to Combat Botnets Could Put Privacy at Risk" (August 2016)

CENTER FOR DEMOCRACY & TECHNOLOGY

3. Reform Surveillance Directed Abroad

Section 702 of the Foreign Intelligence Surveillance Act (FISA), which governs surveillance conducted in the U.S. that targets non-Americans reasonably believed to abroad, expires on December 31, 2017. The breadth of this surveillance and the lack of judicial control over it are striking. The government need only satisfy itself that a person is sending or receiving communications that are "relevant" to U.S. foreign policy or national security, is abroad, and is not an American. That person can be wiretapped and have his stored email disclosed to the government – including all of his communications with Americans – without a warrant. Communications that are "about" a target and that mention a target's identifier (such as a phone number or email address) can be collected under this statute. And, even though surveillance conducted under Section 702 is promoted as surveillance of foreigners abroad, it is often used intentionally to collect the communications of Americans without a warrant.

Ultimately this privacy invasion harms America's standing abroad, creates suspicion toward U.S. providers, and invades the privacy of Americans. The President should work with Congress to reform Section 702 prior to its expiration date. He should limit the purposes for which this surveillance can be conducted by ensuring it is used only for specified national security purposes, such as the prevention of terrorism, espionage, and proliferation of weapons of mass destruction. Second, the President and Congress should permit collection only of communications to or from legitimate targets. Third, the President and Congress should close the "backdoor search" loophole by ensuring that the product of this surveillance – which is supposed to target non-Americans outside the U.S. – cannot be searched for the communications of Americans without a warrant.

Action: In the first 100 days, the President should issue a Directive to the Intelligence Community requiring that Section 702 surveillance be conducted only for specified national security purposes. President Obama issued a similar directive – PPD-28 – that specified that information collected through bulk surveillance would be *used* only for six specific national security purposes.

Action: As well as other significant changes to Section 702, the President should work with Congress to enshrine into law limitations to Section 702 like those described above:

- It can only be used for fighting terrorism, preventing attacks and WMD proliferation, and protecting against secret intelligence activities;
- Collection should only come from legitimate targets; and
- The backdoor search loophole be closed.

Further Background:

- Center for Democracy & Technology, Statement for the Record on Section 702 and the EU-US Safe Harbor (November 2015)
- Center for Democracy & Technology, "Tech Talk" on reform of Section 702 (June 2016)

CENTER FOR DEMOCRACY & TECHNOLOGY

- Center for Democracy & Technology, Myths and Facts about Section 702 reform (October 2015)

4. Require a Warrant to Access Content Stored in the Cloud

The Electronic Communications Privacy Act (ECPA) became law thirty years ago and has not had a substantial update to account for new communications technologies. ECPA should be amended to require law enforcement to obtain a warrant for stored communications content to put email stored in the cloud on a level playing field with a letter in a desk at home.

ECPA reform has wide support in the privacy and tech communities, and in Congress. The Digital Due Process coalition consists of over 100 companies, trade associations, and civil society groups from across the political spectrum, all dedicated to reforming ECPA. In April 2016, on a vote of 416-0, the House of Representatives passed the Email Privacy Act, an ECPA reform bill that would require the government to obtain a warrant for stored electronic communications.

Action: In the first 100 days, the President should order the Attorney General to direct federal prosecutors to obtain a warrant in order to gain access stored communications content in criminal cases, absent an emergency. This is consistent with the current practice of the Justice Department, but it has not yet been "codified" in a binding directive.

Action: The President should endorse and promote the Email Privacy Act when it is introduced in the next Congress.

Further Background:

- Center for Democracy & Technology, Primer on ECPA (May 2015)
- Coalition letter on Email Privacy Act (April 2016)
- Center for Democracy & Technology, Testimony on ECPA Reform (November 2015)

CENTER FOR DEMOCRACY & TECHNOLOGY

U.S. Global Leadership on Internet Freedom

The United States has long been a leading nation in promoting human rights globally. We extol the virtues of free expression, privacy, and individual freedom. All of these have the potential to be advanced by the internet, and the next Administration should continue to put forth policies that promote and protect these fundamental rights.

In 2012 the U.S. government joined a chorus of voices at the UN Human Rights Council saying "the same rights that people have offline must also be protected online." As the separation between the online and offline world further dissipates, protecting these rights in the digital realm only grows in importance.

Detailed below are the key issues the incoming Administration should focus on in order to continue to advance internet freedoms.

1. Protect Online Intermediaries

The global internet has become an indispensable medium for the freedom of expression. Billions of people around the world use the internet to exchange ideas and information; gather and disseminate news and research; discuss and debate social and economic policy; create, share, and preserve art and literature; and more. Out of technical necessity, all of this online expression relies on the use of the equipment and services of a series of third-party intermediaries who can, absent legal protections, be vulnerable to pressure from governments and private parties to censor and block access to information.

There is international recognition of the importance of legal protections for intermediaries, to shield them from liability for third parties' speech. These protections face constant encroachments in the U.S., however, and some of the U.S.'s closest allies in Europe are proposing changes to EU law that would create new obligations for intermediaries to monitor and filter all traffic on their systems. While this obligation is sometimes framed as a safeguard for intellectual property or protection against terrorism, embrace of this sort of mandatory monitoring by democratic nations would send the wrong signals to authoritarian regimes around the world. It would also create potentially insurmountable regulatory hurdles for smaller innovators at home and abroad.

An extreme form of attack on intermediaries occurs when governments shut down or otherwise disrupt access to the internet or specific internet-based apps and services. This is often in response to political sensitivities or localized unrest. These disruptions have important negative implications—for citizens' human rights, countries' economic activity and development, and U.S. businesses' success. They are almost never appropriate or necessary.

CENTER FOR DEMOCRACY & TECHNOLOGY

Action: The next President should reject any policies that require internet intermediaries to proactively monitor or otherwise police the content they host.

Action: The next President should support policies that maintain a high level of protection for intermediaries – and thus for freedom of speech online – including intervening in court cases where there is an effort to hold intermediaries liable for their users' speech. In all foreign policy efforts relating to the internet, the President should promote intermediary liability protections and disfavor shutdowns of networks and services.

Further Background:

- Center for Democracy & Technology, "Shielding the Messengers: Protecting Platforms for Expression and Innovation" (December 2012)
- Center for Democracy & Technology, "Comments to the United Nations Special Rapporteur on Freedom of Expression on the Use of Encryption and Anonymity in Digital Communications" (February 2015)
- Coalition Statement in Opposition to Federal Criminal Publisher Liability (January 2015)
- Center for Democracy & Technology, "Content 'responsibility:' The looming cloud of uncertainty for internet intermediaries" (September 2016)
- Center for Technological Innovation at Brookings, "Internet shutdowns cost countries $2.4 billion last year" (October 2016)

2. Resist Attempts to Censor

The U.S. government and others around the world are understandably concerned about the availability of terrorist propaganda — so-called "extremist content" — online. But we must ensure that the fight against terrorist organizations such as ISIL does not undermine our democratic principles. Some of the U.S.'s closest allies have developed deeply concerning programs, such as the United Kingdom's Internet Referral Unit and the European Commission's Code of Conduct for Illegal Hate Speech, both of which are designed to circumvent the role of courts in determining what online speech violates the law.

These programs create a fast track for censorship without any safeguards for freedom of speech — and can be used by governments to target speech that may not even violate the law (and only violate an internet company's privately developed Terms of Service). Such programs will not be effective at stamping out terrorists' messages online and serve to legitimize extralegal government censorship in other countries. We urge the next Administration to recognize that the best counter to hateful ideology is the preservation of a free and open society.

Action: The next President should reject extralegal government censorship and should encourage our allies in Europe to do the same. Any policy aimed at stopping the commission of terrorist acts must be rooted in

CENTER FOR DEMOCRACY & TECHNOLOGY

evidence that it will be effective and must respect the Constitution and the rule of law. Removal of online content by government must only be through judicial proceedings with adequate due process protections.

Further Background:

- Center for Democracy & Technology, Statement to United Nations Counter-Terrorism Executive Directorate on Human Rights and Extremist Content (December 2015)
- Center for Democracy & Technology, Comments to the UN Special Rapporteur on Freedom of Expression on the Role of the Private Sector in Freedom of Expression Online (December 2016)
- Center for Democracy & Technology, "Letter to European Commission on Code of Conduct for 'Illegal' Hate Speech Online" (June 2016)

3. Assure Transnational Government Demands for Data Meets Human Rights Standards

Because the U.S. is home to major cloud service providers, digital information relevant to criminal investigations is often stored here. This means that when foreign governments need this information they are bound by U.S. procedural rules and must operate through bilateral Mutual Legal Assistance Treaties (MLATs). This creates a high degree of protection for some information (such as the content of communication), but not other information (such as metadata), and also results in long delays in processing. This system faces serious challenges as foreign governments demand speedier access and human rights advocates strive to maintain and improve privacy protections.

Governments that can't gain access to the data they need for legitimate law enforcement investigations may force technology companies to localize their data so the foreign government has jurisdiction over it. This practice directly undermines the free and open structure of the internet. Instead of traveling by the most technically viable routes, data flows are constrained by geopolitical considerations and regulations. Such requirements balkanize the internet, reduce individuals' access to valuable information and communication tools, and discourage global innovation.

The U.S. Department of Justice (DOJ) proposed legislation in July of 2016 that would authorize the Department to enter into agreements with foreign governments that permit them to make direct surveillance demands on U.S. providers. The proposed legislation fails to meet human rights standards, would diminish privacy worldwide, and does nothing to close the metadata loophole in current law. It would also authorize foreign governments to engage in wiretapping in the U.S. for the first time.

Action: In the first 100 days the President should reconvene the interagency working group that crafted the DOJ proposal and make revisions. The revised proposal should permit foreign governments to make direct surveillance demands to U.S. providers only if those demands, and the foreign government's laws and practices,

meet specific and strict human rights requirements to ensure that users' human rights protections are at least as strong under the revised procedures as they are today.

Action: The President should work with Congress to improve the MLAT system and to promote cross-border law enforcement agreements and legislation, as well as other solutions, that meet strong high human rights standards.

Further Background:

- Center for Democracy & Technology, "MLAT Reform: A Straw Man Proposal" (September 2015)
- Center for Democracy & Technology, "Cross-Border Law Enforcement Demands: Analysis of the
- Department of Justice's Proposed Bill" (August 2016)

4. Protect the Open Internet

In 2014 and 2015 internet users rose up in support of open internet (net neutrality) rules. The submission of nearly four million comments was a development that the FCC could not ignore. It resulted in a clear rule against blocking, throttling, and paid prioritization, not just a promise that such practices would be "commercially reasonable," as the FCC originally proposed. The rule preserved and advanced the basic end-to-end nondiscrimination principle that has been essential to the internet's evolution, as well as its power as an engine of economic growth and democratic discourse. It also enshrines the idea of permissionless innovation where new internet services and new speakers can grow unimpeded by potential gatekeepers.

Action: The President should preserve the 2015 open internet rule and protect it against legal challenge.

Further Background:

- *United States Telecom Association v. Federal Communications Commission*, Joint Brief for Intervenors, Dec. 4, 2015.

CENTER FOR DEMOCRACY & TECHNOLOGY

Responsible Use of New Technology

Increased internet connectivity is rapidly changing society. “Data-driven innovation” and the “internet of things” are terms that have been bandied about in so many ways that it can be difficult to shape focused policies around them. In spite of that, they represent a crucial center of American innovation while also raising issues of privacy, security, and equality. This reality creates a bevy of challenges for the next Administration, both in terms of policy and in terms of expertise.

On the policy front, the Administration must consider issues of fairness, discrimination, and inequality through the lens of a data scientist. How are digital decisions made about consumers and citizens? What is the impact of interconnected devices with the potential for even greater data collection? Over the coming years the controls on data collection and use will be set by policy and law, not technological limitations. How can the U.S. create an environment where privacy, security, and innovation can thrive?

To answer these questions, the Administration will need to build on the progress of President Obama by bringing in even more technical expertise at all levels of the federal government.

1. Focus on How Technology Can Exacerbate Inequality and Enable Discrimination

Technology can be a great enabler of democracy and equality. However, as technological resources and achievements continue to grow, so does the gap between those who have access to emerging technology benefits and those who do not. Similarly, while new technologies and the societal shifts they enable can serve as drivers of economic growth and increased opportunity, they can also obviate certain jobs and function as a gatekeeping mechanism - whether intentionally or through assumptions introduced into the development process - that privileges certain groups over others. The President must confront the critical issue: How do we best ensure technological advances are used to reduce inequality and promote progress for all segments of society?

One specific technology, algorithmic decision-making, plays a central role in modern life, determining everything from search engine results and social media content to job and insurance eligibility. Hidden bias can be embedded into these algorithms, often inadvertently reflecting biases that their human creators are unaware of. To address these issues, the Obama Administration advocated for increased accountability fairness and transparency in algorithms in its 2014 report *Big Data: Seizing Opportunities, Preserving Values*. In order to address these issues, it’s critical to embed civil rights values into the process of innovating and building technology. It helps engineers, product managers, and data scientists mitigate bias throughout the process of developing an algorithm.

CENTER FOR DEMOCRACY & TECHNOLOGY

Action: In the first 100 days, the President should ask the Office of Science and Technology Policy (OSTP) to convene stakeholders to review potential bias and discrimination in the federal government's use of algorithms in automated decision-making, including how federal grant-making might be supporting the use of algorithms at the state and local level. OSTP should also begin a Request for Information to investigate whether there are voluntary best practices that businesses can develop to limit any inherent bias in algorithmic tools.

Action: The President must work with Congress to promote both access to the internet and development of the skills needed to compete for 21st-century jobs. Areas urgently in need of attention include subsidizing broadband access, ensuring that students acquire a solid foundation of basic literacy, numeracy, and civil skills, and creating public-private job training partnerships to respond quickly to workplace disruption driven by the expansion of artificial intelligence.

Further Background:

- One-page description of CDT's Digital Decisions Project
- Center for Democracy & Technology: "Policy tools in automated decision-making" (January 2016)
- Center for Democracy & Technology: Preparing for the Future of Artificial Intelligence: In Response to White House OSTP RFI (July 2016)

2. Cultivate Technical Talent in Government

The pace of technological development is staggering. It can be difficult for the government to keep up with this rate of change and integrate technical developments into government operations, policy, and law. Technologists command high salaries at modern tech companies and may find the restrictions of a government stifling. A study commissioned by the Ford and MacArthur Foundations found that deep questions remain about government's ability to "identify, cultivate, and retain individuals with the necessary skills for success in a world increasingly driven by information technology." The current administration has tackled this "technical pipeline" problem head-on through programs like the Presidential Innovation Fellows (PIF), the United States Digital Service (USDS), and 18F.

Action: In the first 100 days the President should initiate a study to examine how government can best incorporate technical insight and respond to technical change in a manner that lasts for much longer than a single presidential term of office. This investigation should be led by the Office of Management and Budget and focus on both operational/logistical needs of government as well as examine how the substantive work of government – be it policy, regulation, or jurisprudence – will be affected by rapid technological change. Programs that are working well now – such as PIF, USDS, and 18F – should be retained and considered for expansion.

CENTER FOR DEMOCRACY & TECHNOLOGY

Further Background:

- "A Future of Failure? The Flow of Technology into Government and Civil Society," a report by Freedman Consulting, LLC prepared for the Ford Foundation and the MacArthur Foundation (2014)

3. Develop a Strong Legal Framework that Protects Privacy

The United States is a global leader in technology innovation but not in data protection. The U.S. is one of only two democratic countries without a baseline privacy law. The U.S.'s inconsistent sectoral approach to privacy creates significant gaps in protection. All of this harms consumer trust in new technologies, makes it difficult to harmonize data use globally, and hinders economic growth. The Obama Administration suggested steps to fix these problems in its 2012 report *Consumer Data Privacy in a Networked World* and through draft legislative language released in March 2015.

While the ultimate step for privacy protection remains enacting baseline privacy legislation, two interim measures could provide immediate benefits for consumers. The first is the recently passed Federal Communications Commission (FCC) privacy protections for broadband internet access. Broadband providers have access to massive amounts of data about internet users' browsing activities, communications, and preferences. Connecting to the internet requires entrusting internet service providers with sensitive personal data, and consumers must be able to trust in the security and privacy of that information. The FCC rules give consumers meaningful control over the ways in which their data can be used and disclosed by broadband internet service providers, and require customers to opt in to most uses of their data that are not directly related to the services to which they have subscribed.

The second is the development of a policy framework for the internet of things (IoT) that respects the privacy of personal data. Interconnected devices are becoming an integral part of American life. It's critical to balance the benefits they bring for consumers with the new privacy and security challenges they also present. The advantages of a car that uses computing to avoid collisions are obvious. Equally obvious is the danger posed if that car is hacked. In addition, IoT devices have recently been employed as tools for cyberattacks. While the ultimate solution for privacy issues may lie with baseline privacy rules, there are important initial steps that the President can take in IoT. This includes required encryption for user sessions and for identifiable data in transit and storage; mandates for security upgrades and patching of security vulnerabilities; requirements for notification when personal data is breached or improperly accessed; clear disclosures on data retention and sharing practices; and safeguards for consumers when devices change ownership or software goes out of service.

Action: In the first 100 days, the President should signal support for comprehensive privacy legislation by introducing a revised Consumer Privacy Bill of Rights Act. The new version of the bill should focus on individual control, access, and correction; remove broad exemption for "customary business records"; tighten definitions

CENTER FOR DEMOCRACY & TECHNOLOGY

of personal information; disfavor retroactive changes to privacy policies; improve enforcement, including a private right of action; and add a mandatory breach notification provision.

Action: In the first 100 days, the President should signal support for the FCC's broadband privacy rules, which maintain broad definitions of what information is covered - and robust, opt-in rules for use of that data - and work to harmonize those rules with the rest of the internet ecosystem.

Action: The National Telecommunications and Information Administration (NTIA) has already convened a multistakeholder process on upgradability and patching for devices in the internet of things. In the first 100 days, the President should expand that effort to include privacy issues unique to the IoT. The Administration should also support the research and guidance currently underway at the National Institute for Standards and Technology (NIST), and direct NIST to apply its innovative work on privacy engineering to IoT.

Further Background:

- Center for Democracy & Technology: "Broadband Privacy Comments in Response to the FCC's NPRM" (May 2016)
- Center for Democracy & Technology: "Analysis of the Consumer Privacy Bill of Rights Act" (March 2015)
- Center for Democracy & Technology: "#IOTFail" (October 2016)
- Center for Democracy & Technology: "A Need for Strong Privacy and Security Standards in the Internet of Things" (January 2014)
- Privacy Engineering at NIST
- Feldman, Larry; Voas, Jeffrey M.; Witte, Gregory A. "Demystifying the Internet of Things" (Sept. 2016), National Institute of Standards and Technology

CONTACT US

CENTER FOR DEMOCRACY & TECHNOLOGY

1401 K STREET NW, SUITE 200
WASHINGTON, DC 20005

CDT.ORG | @CENDEMTECH

(202) 637-9800