ACLU
AMERICAN CIVIL LIBERTIES UNION

The Path to Privacy Reform:
After One Year of Snowden Revelations, What Comes Next?

One year ago, the world had never heard of Edward Snowden. Not coincidentally, one year ago the world knew very little about the breathtaking scope of U.S. government surveillance. One year later, we are in a very different place. Since Snowden acted, we have learned that the National Security Agency is tracking Americans' domestic phone calls, scanning the contents of our international communications as they cross the border, collecting worldwide location data on an enormous scale, and deliberately weakening the security of the Internet. We've also learned the NSA's unofficial, Orwellian motto: "Collect it All; Process it All; Exploit it All; Partner it All; Sniff it All; Know it All."

Without popular consent or even democratic debate, the NSA has fundamentally altered the relationship between the government and its citizens. It has also trampled on the privacy rights of hundreds of millions around the world. Our country's own not-so-distant history demonstrates that when the government assumes for itself extraordinary surveillance powers, those powers will inevitably be abused. It also shows that unchecked surveillance can have devastating chilling effects on the exercise of our constitutional and human rights and on our freedom to think, debate, and create.

What we didn't know at this time last year is now at the heart of an unprecedented global debate — a debate joined in full force by the American people, all three branches of the U.S. government, the technology industry, and the international community. However, concrete action is needed to translate momentum for reform into meaningful change. Below, we outline steps that the president, Congress, the courts, and technology companies should take in order to do their part in ending the indiscriminate collection of our personal information, to return democratic accountability to our nation's surveillance policies, and to ensure that Edward Snowden's act of courage — now one year old — bears the fruit of real and lasting reform.

Congress

It is clearer than ever that Congress has failed to effectively check the NSA's surveillance activities, and that it has allowed advances in technology to outpace legal restraints on government spying. The time for reform in these areas is now.

- **End dragnet surveillance under the USA Patriot Act:** Congress is on the brink of passing the USA Freedom Act, potentially the most significant surveillance reform in four decades. There is still much to be done — for starters, the Senate should strengthen the much-weakened bill passed by the House of Representatives by more clearly prohibiting large-scale collection. Any new law must ensure that bulk collection becomes a thing of the past.
- **End dragnet surveillance under the FISA Amendments Act:** Much of the government's global communications dragnet operates under the FAA, passed by Congress in 2008. While this law was sold to Americans as one focused on foreign terrorists, it actually permits the collection, scanning, retention, and dissemination of millions of Americans' communications under programs like PRISM and UPSTREAM. In defending these programs, the government has taken the position that Americans have virtually no privacy interest in their international communications, so it may sift through them en masse. Whether through the Senate's version of the USA Freedom Act or something else, Congress must require the government to obtain warrants based on individualized suspicion before accessing Americans' communications.
- **Update our communications laws for the digital age:** Since Congress passed the Electronic Communications Reform Act in 1986, both technology and the ways we use it in our everyday lives have changed dramatically. Congress must address these changes by making clear that our electronic communications are just as sensitive, private, and deserving of protection as our physical ones. It should also pass the GPS Act, legislation that would require the government to obtain warrants before demanding location information from telecommunications companies.

President Obama

While President Obama has indicated that he supports efforts to rein in many of the surveillance activities uncovered by Edward Snowden, the executive branch must do much more to increase privacy protections for both Americans at home and foreigners abroad, to ensure public accountability of surveillance programs, and to improve Internet security instead of harming it.

- **Secure, don't break, the Internet:** The recent disclosure of the Heartbleed bug reminded Americans just how important online security is to our everyday lives. The encryption technology that protects our private emails, financial information, and reading habits — as well as our passwords to all kinds of sites — should be truly secure. But the Snowden disclosures make clear that the NSA is deliberately undermining Internet security through widespread hacking, sabotage of global encryption standards, and hoarding and exploitation of so-called "zero day" vulnerabilities. When the government undermines Internet security, it makes everyone less safe.
- **Release documents showing how the government interprets surveillance laws:** In the past year, we have learned that the Department of Justice and the NSA have interpreted surveillance laws in surprising ways, using secrecy as an opportunity to give conventional words unconventional meanings. The government should release significant agency interpretations of these laws to the public so that we all understand what the government thinks they mean.

ACLU

- **Respect the privacy rights of citizens of other countries:** In January 2014, President Obama delivered a national address and issued a presidential directive that acknowledged that all people, not just Americans, have a right of privacy, and that all people, not just Americans, are entitled to "dignity and respect." The president also highlighted the close relationship between privacy and other human rights, including the freedom of expression. But while the presidential directive would impose some restrictions on the retention and dissemination of non-citizens' communications, it would not limit the collection of these communications in the first place. The president should adopt stronger, binding protections for the data of innocent foreign citizens caught up in the government's communications dragnets.

The Courts

The courts have a crucial role to play in ensuring that the government's surveillance efforts are consistent with domestic and international law.

- **Unseal judicial opinions authorizing dragnet surveillance:** Throughout our history, the public has enjoyed a First Amendment right of access to judicial opinions, particularly to opinions that contain significant interpretations of laws that affect constitutional rights. That right extends to opinions of the Foreign Intelligence Surveillance Court. The FISC should publish all opinions that interpret the meaning, scope, and constitutionality of our surveillance laws — in particular, any opinions that authorize forms of dragnet surveillance — with only minimal redactions to protect actual sources and methods.
- **Subject the government's secrecy claims to more careful review:** The last year has brought a wave of revelations about the ways in which the government misrepresented its surveillance activities and practices to courts, including the Supreme Court and the FISC. Now, more than ever, the courts must recognize their constitutional duty to act as a meaningful check on the executive branch — especially in matters related to national security.
- **Reject improper government efforts to insulate surveillance laws from legal challenges:** For decades, the government has asserted doctrines like "standing" and "state secrets" to improperly block litigation in national security cases. Courts have increasingly interpreted these doctrines broadly. But these procedural defenses were never meant to be wholesale shields preventing the judicial review of government conduct. Courts should return these doctrines to their narrow origins and ensure that plaintiffs who can demonstrate a reasonable likelihood that they have a valid claim have recourse to our courts.
- **Ensure surveillance laws are tested in open court, not behind closed doors:** Both the regular federal courts and the FISC have the authority to invite the participation of the public when they are faced with serious legal issues that will affect Americans' right to privacy. The courts should invite experienced public interest groups to weigh in on important constitutional and statutory issues. Americans' constitutional rights should never be argued and interpreted away behind closed doors, and the federal courts are well equipped to safeguard sensitive information while ensuring a robust and adversarial legal debate.

Technology Companies

Because technology companies are the custodians of our sensitive information and also the recipients of government demands for that information, they have a pivotal role to play in protecting users' privacy.

- **Insist on warrants:** Companies must understand that as stewards of their users'

private information, they have an obligation to push back against intrusive and novel government requests for users' data. The fact that the government often withdraws requests when companies push back demonstrates just how out of control the government's informal information-gathering has become. Especially when faced with requests for extraordinarily sensitive information (like location information), technology companies should refuse to comply unless presented with a warrant based upon probable cause.

- **Notify users of surveillance requests:** Even though most government demands for customer information do not prevent technology companies from notifying the affected users, many companies choose to remain silent when served with such requests. But technology companies should be champions, not adversaries, of their users' privacy, and they should always provide notice when user information has been requested. More companies should follow the lead of firms like Apple, Google, and Microsoft in adopting public policies about notice, which guarantee users they have their customers' backs when it comes to privacy.

- **Minimize data collection and retention:** The best way to keep the government from obtaining our private information from Internet and telecommunications companies is to ensure that the companies don't hold it for any longer than they need it. Companies should limit the amount of information that they retain, and how long they retain it, to what is needed for genuine business purposes. Companies shouldn't be holding onto our information without a truly valid business reason to do so.

- **Encrypt and protect our communications:** When email travels between services, it is at risk of interception by the government or others. Email services should use STARTTLS to protect email sent from one service (like Gmail) to another (like Hotmail). For even stronger protection, email services should publish DANE records for their SMTP hosts and verify them during transfer. And with respect to video, voice, and instant-messaging services, technology companies should follow the lead of companies like Apple, which protect internal messaging services with end-to-end encryption. What we say privately deserves protection no matter whom we're saying it to.

- **Publish meaningful statistics about government surveillance requests:** Technology companies are the only ones who can give the public a full understanding of the way in which the government is using its various law-enforcement authorities to collect user data. Insisting on the publication of data about surveillance requests, which are both comprehensive and useful to the public, is crucial to filling the information void created by excessive government secrecy over surveillance, and to the ongoing public debate about reform.