HUMAN RIGHTS WATCH

350 Fifth Avenue, 34th Floor
New York, NY 10118-3299
Tel: 212-290-4700
Fax: 212-736-1300 ; 917-591-3452

HUMAN RIGHTS WATCH

HRW.org

January 16, 2014

President Barack Obama
The White House
1600 Pennsylvania Avenue NW
Washington, DC 20500

Re: Surveillance Reforms

Dear President Obama:

As you consider reforms to US electronic surveillance practices, you have an opportunity to demonstrate that safeguarding national security does not have to come through the sacrifice of American ideals or universal rights. This is a moment when your moral leadership is urgently needed to rein in a security apparatus that has clearly given inadequate weight to the public's privacy rights. We strongly urge you to adopt a number of essential reforms to the way the US conducts electronic surveillance both within and outside the country–many also endorsed in the recent report of your Review Group on US Intelligence and Communications Technologies.

In particular, we wish to draw your attention to the harm that National Security Agency (NSA) surveillance has inflicted not only on the rights of US persons, through bulk metadata collection, but also on the rights of millions of other people outside the US. Inside the US there has been limited debate about this issue. However, as an international organization we are keenly aware that broad, unfocused surveillance of non-US persons with few restraints has chilled the exercise of basic rights and undermined an important US foreign policy objective: promoting global Internet freedom. A potentially damaging backlash is gathering force against US leadership in this area, with important implications for a free and open Internet in the years ahead. We are already seeing countries moving to erect walls against NSA surveillance, proposing far-reaching restrictions on Internet data that, over time, could lead to a "Balkanized" Internet. If the US does not rein in mass surveillance programs, moreover, it gives a green light to other governments to emulate its approach, with grave consequences to privacy online.

The US government should make clear in words and in practice its commitment to respecting the privacy rights of all people, in the US and beyond. Congressional action is needed to fully address concerns over existing programs, but there are many important reforms that you could adopt directly. In particular, we urge you to implement the following four recommendations immediately:

End Bulk Metadata Collection

Under Section 215 of the USA PATRIOT Act, the NSA has been collecting the telephone metadata records of nearly every person in the US for years. It has been authorized to maintain this data for five years, in some cases longer. The program sweeps up vast amounts of information from people accused of no wrongdoing that can reveal the most intimate details of their lives. Concern over the collection and querying of this data also risks chilling speech and association—shaping how people in this country communicate by phone and email, and ultimately harming the quality of debate and democratic governance in this country.[1]

Although the stated purpose of this sweeping data collection is to protect the nation from terrorism, the program has not been shown necessary to preventing terrorist attacks.[2] As the review group found, after having reviewed all relevant classified materials, any contributions to terrorist investigations "could readily have been obtained in a timely manner using more conventional 215 orders."[3]
Your administration can use existing authority to simply stop collecting such information under this program. We urge you to do so as soon as possible and to lend your support to legislative efforts that would formally end the program.

The review group alternatively suggested that the data be "voluntarily" maintained by the telecommunications companies or a private third party for a period of no more than two years or that retention be mandated if a voluntary program proves infeasible. However, we do not believe that either approach addresses the indiscriminate nature of mass data collection or adequately regulates government access.

While intelligence and law enforcement agencies will always want to have more information at their disposal in the hope it may someday prove useful, forcing companies to retain data for longer than they otherwise would for ordinary business reasons renders the collected troves of highly revealing metadata vulnerable to breach, theft, or misuse for unclear gain. If the NSA's maintenance of metadata records for five years has not been particularly valuable in thwarting terrorist attacks, requiring companies to hold such data for two years will be no more productive.

Protect the Privacy Rights of Non-US Persons

In today's world, where 150 billion emails crisscross the globe daily, and commerce and the flow of information depend on a borderless Internet, affording persons outside the US lesser rights only erodes confidence in the US as a voice in Internet governance and a proponent of online

---

[1] Committee to Protect Journalists, "The Obama Administration and the Press," October 10, 2013 http://cpj.org/reports/2013/10/obama-and-the-press-us-leaks-surveillance-post-911.php (accessed January 14, 2014); PEN American Center, "Chilling Effects," November 11, 2013, http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf (accessed January 14, 2014).

[2] New America Foundation, "Do NSA's Bulk Surveillance Programs Stop Terrorism?" January 2014, http://newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1.pdf (accessed January 14, 2014); The President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World," December 12, 2013, http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (accessed January 14, 2014), p. 104.

[3] "Liberty and Security in a Changing World," p. 104.

freedom. The US dominates digital communications, with most of the world's Internet traffic moving through its territory or companies. With this extraordinary power comes heightened responsibility for upholding human rights. A new approach is probably also necessary if the United States does not want to see the significance of its Internet role diminished.

Section 702 of the Foreign Intelligence Surveillance Act (FISA) authorizes the warrantless surveillance of non-US persons reasonably believed to be outside the US. Executive Order 12333 also governs US surveillance practices abroad; more needs to be disclosed about its scope, interpretation, and application.

To protect the privacy rights of non-US persons, we urge you to:

* *Adopt the review group's recommendation to limit the scope of collection under 702 and any other authority that authorizes surveillance abroad* to what is "directed exclusively at the national security of the United States or [its] allies" and ensure that surveillance is not used for illegitimate ends such as commercial gain.[4] Under Section 702, the US can collect "foreign intelligence information." But this term is defined extremely broadly to include things that need only "relate to" terrorism, intelligence activities of another government, the national defense, or the foreign affairs of the United States. The content of communications can be obtained, not just metadata, as can communications "about" the targets. Indeed, according to media reports based on documents leaked by former NSA contractor Edward Snowden, the NSA taps into main communication links of data centers around the world and collects millions of records every day, including metadata text, audio, and video.[5] This type of over-collection cannot possibly be proportionate or necessary to US national security goals.

* *Conform standards regulating what data may be collected to international legal requirements.* The review group acknowledged the need to bolster the protection of rights of non-US persons under 702 but suggested adding only a lower "reasonable suspicion" requirement for surveillance of the content of the communications of non-US persons, maintaining a more robust "probable cause" requirement for US persons.[6] While this would be better than the current practice of permitting such surveillance on the basis of virtually no factual showing at all, it still falls short of compliance with international human rights law. The US should ensure that surveillance of the content of any person's communications, wherever located, only takes place when genuinely necessary for a legitimate purpose, such as national security, and that data collection and retention be strictly proportionate to that end. A "probable cause" standard is necessary to accomplish this goal and would help to put the US in compliance with its international obligations (though full compliance also will require substantially narrowing the substantive purpose of collection, as noted above).

---

[4] "Liberty and Security in a Changing World," p. 151.

[5] Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," Washington Post, October 30, 2013, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (accessed January 16, 2014).

[6] "Liberty and Security in a Changing World," p. 156, 157

* *Forbid the use of evidence collected under 702 in criminal investigations.* Because the standards for acquiring information under Section 702 are much lower than what would be required in a criminal case, we also agree with the review group that evidence collected under 702 should not be used in certain criminal investigations. Such use would circumvent US protections against unreasonable searches and seizures under the Fourth Amendment to the US Constitution. And it would also run afoul of due process and fair trial rights protected under human rights law (and to which non-US persons are also entitled). Allowing law enforcement to use evidence from section 702 for criminal investigations would open the door to the evisceration of fundamental principles that the US has traditionally embraced. Though the review group would bar Section 702 evidence only in criminal cases against US persons, we would extend this to non-US persons as well.

Some policymakers have implied that the 702 program has been more useful than the Section 215 program in preventing terrorist attacks. But as noted by the review group, "the question is not whether granting the government authority makes us incrementally safer, but whether the additional safety is worth the sacrifice in terms of individual privacy, personal liberty and public trust."[7] Given the massive invasion of privacy involved and the at-best modest security gains, the answer to that question is clearly no.

Further, there is no convincing evidence so far that a more targeted approach requiring a warrant and probable cause would not have produced the same sort of intelligence. According to media reports, the key information acquired in the main case officials repeatedly cite in support of Section 702 – that of Najibullah Zazi – could have been obtained through a warrant and probable cause.[8] Zazi was convicted in 2010 on charges related to plans to attack the New York City subway system.

Protect Encryption and Online Security

The US has spent millions of dollars to improve digital security for human rights defenders. US technology companies also enjoy dominant market share in many places around the world. Yet recent media reports suggest that the NSA has deliberately weakened encryption standards and may be asking companies to disclose encryption keys or otherwise undermine the security of their products. Trust that online communications are secure is essential to the functioning of many businesses and institutions, including those in the financial and heath sectors, as well as to those in the creative and artistic fields. Actively weakening encryption standards would undermine this trust and damage the reputation of US technology companies. Such actions also badly damage the reputation of the United States as a supporter of Internet freedom, as well as its economic interests. We agree with the review group that the US should not undermine security standards or weaken the security of generally available software and online services. If the US hopes to restore trust, it must signal its commitment to preserving strongly protected online encryption mechanisms as soon as possible. We urge you to end programs aimed at reducing security of commercial hardware and software and actively oppose any future legislative efforts to mandate back doors into US technology.

---

[7] Ibid., p. 114

[8] Matt Apuzzo and Adam Goldman, "NYC Bomb Plot Details Settle Little in NSA Debate," Associated Press, June 11, 2013, http://bigstory.ap.org/article/nyc-bomb-plot-details-settle-little-nsa-debate (accessed January 14, 2014).

Increase the Transparency of Surveillance Programs

Vast changes to US law on surveillance have happened in secret without adequate oversight. The lack of public information has prevented debate about issues of great importance to the democratic process and individual rights. In addition, the companies and organizations that have participated in US surveillance programs have been prevented from disclosing basic data about the information that the government has been demanding of them.

You have in the past stated that you welcome a debate about these matters, and your decision to establish the review group to recommend possible reforms implicitly recognizes the importance of this discussion. Yet it is impossible to have a healthy and open democratic debate about these matters when the public – and most of the US Congress – is kept in the dark about the scope of the programs and their implementation. There are legitimate reasons to classify certain types of information – for example, to protect the identities of vulnerable individuals or to protect the public from harm. But classification can too easily become a tool to prevent embarrassment or exposure of wrongdoing, or to conceal information about the functioning of public institutions. Protecting national security does not have to come at the expense of public accountability. For example, there was no legitimate reason why the extent of the government collection of metadata should have been kept from the general public.

We urge you to disclose much more about the scope of terms of surveillance occurring under Section 702 and Executive Order 12333, which could have enormous implications for the rights of foreigners abroad. US persons have the same interest as those abroad in knowing when their privacy rights are protected, and that can be revealed without disclosing information that would threaten national security. We also encourage you to support legislative reforms suggested by the review group, including transparency measures to require greater reporting to Congress and the public about use of intelligence gathering powers, and to permit technology companies to report on the number of orders they receive for user data. They also recommended a strong presumption of transparency in decisions about whether to keep programs of the magnitude of the 215 bulk telephony metadata program secret. These measures will not only assist democratic debate today, but guard against abuse of power in the future.

The review group also made a number of other specific recommendations with which we agree, and which we hope you adopt and encourage Congress to act on. These include:

* *Ending the widespread use of National Security Letters (NSLs) without judicial review*: National security letters are a form of administrative subpoena that give the FBI and other government agencies expanded power to compel the production of records. Under the PATRIOT Act of 2001, authorization for their use was greatly expanded; the need for individualized suspicion was reduced and a broader array of officials became authorized to issue them. As a result, the use of NSL's dramatically increased to the point where the FBI currently issues nearly 60 NSLs per day without judicial approval and accompanied by strict gag orders on the recipients. According to a report by the Office of the Inspector General in the Department of Justice, the lack of oversight has

resulted in serious compliance issues and extensive misuse of NSL authority.[9] The review group effectively called for an end to this practice, saying that NSLs should be subject to judicial authorization, like 215 orders. We agree with these recommendations, and though they require Congressional action we strongly urge you to support them.

* *Creating an Institutional Advocate at the Foreign Intelligence Surveillance Court (FISC)*: For years, the FISC has been authorizing dramatic changes to US law in secret without any adversary's view being part of the process. That is a recipe for decisions that set the wrong balance between security and rights, because any judge is more likely to be persuaded by the side whose views he or she hears. The panel supported creating an institutional advocate with appropriate security clearances at the FISC to represent the public's privacy interests. We strongly urge you to support legislative action on this matter.

* *Strengthening the Privacy and Civil Liberties Oversight Board (PCLOB) and Investing It with Whistleblower Reporting Authority*: The PCLOB was established by Congress after September 11, 2001, to conduct oversight of the intelligence community and make recommendations about how to improve privacy and civil liberties protections. But for years, the board remained dormant, without a chairman or staff. It now has a chairman and staff but limited resources. If strengthened further and provided with adequate resources, it can help to check the powers of an intelligence community that gravitates toward over-classification and secrecy.

  Additionally, we agree with the review group that the PCLOB should be empowered to receive whistleblower complaints. Would-be whistleblowers need an independent and effective body to which they can report abuses or wrongdoing without having to report them internally first. A presidential policy directive issued in 2012, intended to improve whistleblower protections for federal employees, does not cover contractors and requires whistleblowers to report to a person in their direct chain of command instead of a more independent body.[10] While this would not adequately address the need for whistleblower reform that Human Rights Watch has previously identified, it would be a starting point.
  More complete whistleblower reform would require more than just creating an independent body to report wrongdoing. It would also require providing whistleblowers with legal protection against retaliation and legal defenses to prosecution. We urge you to propose to Congress a law that will grant such protections to federal employees and consultants in this sector.

The rules that the United States establishes today on these matters will likely govern surveillance long after your administration has completed its term. They will also set a key precedent to which other countries will look to as they debate crucial questions about privacy and Internet freedom across the world. We strongly urge you, even as US surveillance capabilities continue to increase, to ensure that those capabilities are effectively regulated,

---

[9] "Liberty and Security in a Changing World," p. 92, n. 78 citing Department of Justice, Office of the Inspector General, A Review of the Federal Bureau of Investigation's Use of National Security Letters (Unclassified) (March 2007) and noting that subsequent reports from the IG have noted the FBI and the DOJ have resolved many of the compliance incidents.
[10] "Liberty and Security in a Changing World," p. 127, n. 124.

within a framework of the rule of law, maximum transparency, and respect for democracy and human rights. Adopting the recommendations outlined above will be a first step in that direction.

Sincerely,

Kenneth Roth
Executive Director