HUMAN RIGHTS WATCH

Internet at a Crossroads

How Government Surveillance Threatens How We Communicate

By Cynthia M. Wong

We have reached an inflection point for the future of the Internet. To preserve the Internet as an open, global platform for rights, development, and commerce, we need principled rules to govern digital surveillance and protect privacy that apply to every government. Until the summer of 2013, the global movement for Internet freedom had been gaining momentum. A diverse range of governments had formed the Freedom Online Coalition and publicly committed to promoting a free, open, and global Internet through coordinated diplomatic efforts, led by the United States, United Kingdom, and their allies. There was broad recognition at the United Nations Human Rights Council that the same rights we enjoy offline must also apply online.

However, global trust in US and UK leadership on Internet freedom has evaporated ever since former National Security Agency (NSA) contractor Edward Snowden began releasing evidence of mass surveillance by the NSA and its British counterpart, the Government Communications Headquarters (GCHQ). In a blistering critique at the UN in September 2013, Brazilian President Dilma Rousseff condemned these practices: “In the absence of the right to privacy, there can be no true freedom of expression and opinion, and therefore no effective democracy,” Rouseff declared. “The right to safety of citizens of one country can never be guaranteed by violating the rights of citizens of another country.”

Snowden’s revelations laid bare the rift between the stated values of the US and UK and their behavior. Even while championing an open and free Internet, these governments were collecting data on hundreds of million people worldwide every day, including, in the case of the US, Dilma Rousseff herself. To make it easier to spy on people online and identify security threats, they have also surreptitiously weakened Internet security, paradoxically making all Internet users less safe and more vulnerable to hackers and identity thieves.

While many governments expressed outrage over snooping by the NSA and GCHQ, many may have also responded privately with envy. Though few can match the resources of the NSA or GCHQ, governments everywhere are expanding their own mass surveillance capacity, and are likely emulating the US and UK.

Left unchecked, this dynamic could soon produce a world in which every online search, electronic contact, email, or transaction is stored away in one or more government databases. With no government able to ensure the privacy of its own citizens from foreign snooping and intelligence agencies teaming up to share data about the citizens of other countries, a truly Orwellian scenario could unfold. While the US asserts it will not use intelligence gathering to quash dissent or discriminate, governments have repeatedly used surveillance to these ends.

President Obama has welcomed a debate about modern surveillance, but talk of safeguards and reform in the US has led to little or no discernible change for global Internet users. The Obama administration has committed to additional protections for personal information it has collected but has done little to rein in the sheer scale of surveillance the NSA conducts, especially abroad. The UK, for its part, has refused to answer even the most basic questions about its intelligence gathering practices and, in an astounding act of hubris and blatant disregard for rights, rushed through a law in July 2014 that extends its surveillance powers. In defending its program, neither government has been fully willing to recognize the privacy interests of people outside its borders.

The picture is not entirely bleak, however. In 2014, several important actors stepped into the leadership void left by the US and UK. Major UN human rights institutions have begun to articulate what it means to protect privacy when technology makes surveillance potentially ubiquitous. And a new coalition of states, led by Germany and Brazil, has taken up the mantle of Internet freedom to press these efforts, while the Freedom Online Coalition strives to restore its credibility.

It is critical to continue pushing the US and UK for real reform, but the rest of the world should not wait for them to act. Fears of terrorism, and the comparative advantage that the US and UK have in surveillance are blinding them to the harms their practices pose, not only to their alliances but also to their own democratic institutions. Those harms include chilling basic freedoms of expression and association, weakening the press and freedom

of information, and degrading access to legal advice and defense. Indeed, these countries might not change course until their own citizens face comparable levels of surveillance by foreign powers.

In the meantime, other countries should keep surveillance and privacy on the human rights agenda at the UN and elsewhere. These issues should be consistently raised in bilateral meetings as well so the US and the UK are not let off the hook. Experience has shown that the US and UK, though often unwilling to be at the vanguard in developing international norms, eventually conform their practices to principled rules to which other countries agree to be bound.

"Collect it All"

We now live in an age of "big data," when our communications and activities routinely leave rich digital traces that can be collected, analyzed, and stored at low cost. In parallel, commercial imperatives drive a range of companies to amass vast stores of information about our social networks, health, finances, and shopping habits. The plummeting cost of storage and computing means that such data can be retained for longer and mined for future, unforeseen purposes.

These digital dossiers appeal to governments for a range of purposes, both legitimate and illegitimate. By accessing data held by the private sector, governments can easily uncover patterns of behavior and associations, both offline and online—whether to thwart security threats or to identify a particularly vocal online critic of government policy.

Security agencies in the US and UK have responded by building enormous storage facilities and voraciously collecting as much data as they can. In a 2008 visit to the United Kingdom, US General Keith Alexander, then-director of the NSA, asked, "Why can't we collect all the signals, all the time?" The UK set out to meet that challenge with its Tempora program, which involves mass interception of data flowing over 200 undersea cables connecting Europe to the Americas, Africa, and beyond. Media reports from the past year also indicate that the GCHQ may be secretly capturing and storing webcam images of millions of Internet users.

In the US, the NSA has wholeheartedly embraced bulk collection of metadata from private telecom operators (and perhaps other unknown entities), as well as mass fiber optic cable tapping. In 2014, reports based on the Snowden documents showed that the US may be collecting millions of text messages worldwide each day, gathering all mobile phone metadata in five countries, and intercepting all phone calls in two of these countries.
In the name of security, the US and UK have thrown away any notion of proportionality, where surveillance is targeted only at individuals they have reason to believe present a genuine threat. Only a tiny fraction of Internet or mobile phone users being surveilled today will ever be suspected of wrongdoing, let alone ties to terrorist activity.
Most of this has happened largely in secret, punctuated with brief windows of insight provided by national security whistleblowers over the years and the much larger window opened by Snowden's disclosures.

Failure of Leadership

What have the US and UK done to rein in mass surveillance in response to public outrage? For the billions of global Internet users outside these countries, the answer is: almost nothing.

On January 17, 2014, President Obama announced measures to restrict the use, retention, and dissemination of personal data gathered by intelligence agencies in Presidential Policy Directive 28. These new measures purport to bring rules for data collected on non-US persons (foreigners abroad) closer to those governing data collected on US persons. While the directive represents a greater level of disclosure (especially compared to most governments), the rules themselves are vague, do not go far enough to prevent abuse, and do not create rights that non-US persons can assert in court. They are also not entrenched, given that they are not embodied in legislation and can therefore be changed by any subsequent US administration. Most critically, the new measures do not prevent large-scale gathering of data and communications of individuals not linked to any wrongdoing, leaving the vast databanks of intercepted information growing larger for future administrations to exploit.

The USA Freedom Act, the main legislative vehicle for reform in the US, intended to end bulk collection of metadata and other records in the US. The bill failed to move forward in Congress in November 2014. However, even if the USA Freedom Act had passed, important

as its passage would have been, it would have addressed only one of the programs revealed by the Snowden documents and would have done almost nothing to address the privacy concerns of billions of global Internet users outside the US whose personal information may be sitting in NSA databases. At time of writing, it appears that a Republican-led Congress may be even less receptive to efforts to rein in bulk collection.

In the UK, authorities continue to "neither confirm nor deny" that GCHQ intercepts the communications of millions of individuals. The government has refused to answer the most basic questions about its practices, so it is exceedingly difficult to assess its claims that these programs are lawful and necessary for protecting security. However, in a response to a court challenge, the UK government acknowledged that it interprets the law to allow agencies to gather potentially millions of communications via popular services like Twitter, Gmail, and Facebook without a warrant, merely because the servers of these companies are often located abroad. This disclosure raises serious questions about the GCHQ's claims that these powers are necessary to protect public safety.

Most troubling, the US and UK continue to argue that they have no legal obligation to safeguard the privacy of anyone outside their respective territories. In other areas of human rights law, the US has argued that it has no obligations to individuals outside its territory and has only admitted this year that it may have some duties under the Convention against Torture towards foreigners it physically captures, but only in territories where it exercises "governmental authority." In contrast to its resistance to assuming extraterritorial obligations with respect to surveillance, the US asserts authority to compel US-based companies to hand over information about any user around the world, regardless of where that data is stored, with almost no protections for the privacy of non-Americans abroad. The UK has also conceded extraterritorial human rights obligations in circumstances such as detention of foreigners abroad. But in the area of privacy and surveillance, the UK labels communications that travel outside the British Isles as "external," and UK law provides scant safeguards for the privacy of "external" communications.

The shortsighted approaches of the US and UK will almost certainly come back to harm their own citizens as other governments follow their lead. As Internet networks continue to globalize, an increasing amount of data about American and British residents will travel outside US and UK territory, and other countries will feel free to gather and store that data without limit.

The US and UK have provided a roadmap for governments of all political persuasions to build their own systems of mass surveillance. Though few can match the NSA's and GCHQ's resources or capabilities today, many other governments take an equally opaque and rapacious approach to digital data gathering.

Vilifying Encryption

The Snowden documents reveal that the NSA has also weakened encryption standards and withheld information about security holes in commercial products so that it can exploit them before companies can fix them. In addition, media reports suggest the GCHQ is developing ways to defeat encryption, especially for Internet traffic that it intercepts. These tactics can facilitate surreptitious monitoring and data collection from devices and networks, not just by the US and UK but potentially by other actors as well. While code breaking has always been at the heart of the NSA's mission, any techniques that undermine the broader security of Internet applications and networks put all Internet users at risk.

In 2014, major US technology companies redoubled efforts to harden the security of their devices and services against spying. These measures have become a commercial imperative as loss of trust drives users to non-American companies. In September 2014, Google and Apple announced that data stored on their mobile devices would be encrypted by default, and neither company would be able to decrypt stored data in response to government requests. Google, Microsoft, Yahoo, Facebook, and other services have taken additional steps to secure emails and messages as they transit the Internet changes that security experts and rights activists have pushed for years. As journalists and rights groups increasingly rely on global online tools for their work, many view these security improvements as a crucial post-Snowden outcome. For vulnerable groups or those living under authoritarian regimes, shielding communications and associations from abusive spying can be a matter of life and death.

Yet government officials in the US and UK have responded to these new security measures by accusing technology firms of facilitating murder, terrorism, and child abuse. In his first week in office in November 2014, Robert Hannigan, head of GCHQ, penned an op-ed calling US technology companies the "command-and-control network of choice for terrorists and criminals," citing increased encryption as especially useful for the extremist group Islamic State, also known as ISIS, and other terrorist organizations. Similarly, in a

September 2014 speech, James Comey, head of the FBI, argued that "encryption threatens to lead all of us to a very dark place" and puts criminals beyond the law. Officials seek even greater cooperation from major technology firms, including through "back doors" built into devices and services that will allow them greater access to user communication.

Law enforcement and security officials argue that encryption back doors are necessary to protect public security. Yet these actions ironically leave Internet and mobile phone users—all of us—less secure. Security experts affirm that such back doors, once in place, create new vulnerabilities since they can be misused by hackers, identity thieves, and other malicious actors. From a technical standpoint, it is almost impossible to create a back door that can only be exploited by designated "good" actors.

Opponents of encryption in the US and UK governments also forget that they are not the only ones who will demand access to back doors. If Google, Apple, and other firms capitulate to their demands, it will be difficult to refuse the same access by other governments. Baking privacy and security into technology by design is the most effective way to protect the security of users from a range of bad actors. If GCHQ cannot force Apple to unlock an iPhone because Apple does not hold the key, then neither can intelligence agencies in China or Russia.

True Costs of Surveillance

As a global community, we have not even begun to grapple with the true costs of surveillance, not only to privacy but also to other rights and closely held values.
A joint report published by Human Rights Watch and the American Civil Liberties Union in July 2014 documented the insidious effects of large-scale surveillance on the practice of journalism and law in the US. Interviews with dozens of journalists showed that increased surveillance, combined with tightened measures to prevent leaks and government contact with media, are intimidating sources, keeping them from talking to journalists (even about unclassified topics of public concern) out of fear that they could face retaliation, lose their security clearances or jobs, or even face prosecution. Ultimately, this is having a detrimental impact on the amount and quality of news coverage, particularly on matters related to national security, intelligence, and law enforcement. This effect undermines the role of the fourth estate in holding government to account.

Steve Coll, staff writer for the *New Yorker* and dean of the Graduate School of Journalism at Columbia University, explained: "Every national security reporter I know would say that the atmosphere in which professional reporters seek insight into policy failures [and] bad military decisions is just much tougher and much chillier." Public understanding of national security policies that are carried out in our name is essential to the functioning of healthy democracies and open societies.

Another national security reporter described the impact of the Snowden revelations on the ability of journalists to protect their sources: "I used to think that the most careful people were not at risk, [that they] could protect sources and kept them from being known. Now we know that isn't the case. That's what Snowden meant for me. There's a record of everywhere I've walked, everywhere I've been."

Many journalists are taking extraordinary measures to protect their sources and shield them from retribution, including by using disposable burner phones or strong encryption, or avoiding phones and the Internet altogether. As one journalist put it, they are being forced to adopt the tactics of drug dealers and criminals just to do their job. Lawyers—and particularly defense attorneys—who spoke to Human Rights Watch described adopting similar tactics to protect the confidentiality of their communications with clients, which is essential to the right to counsel.

In the UK, documents released in November 2014 as a result of a legal challenge show that UK security and intelligence services have policies permitting the interception of privileged lawyer-client communications on national security grounds, including potentially in cases in which the agencies were defendants. The human rights group Reprieve brought the case on behalf of Libyan families who allege that they were subjected to extraordinary rendition and torture. Reprieve's legal director, Cori Crider, stated that these policies raise "troubling implications for the whole British justice system" and questioned how often the government has "rigged the game in their favor in the ongoing court case over torture." This initial research only scratches the surface. For example, an April 2014 poll of 2,000 Americans on the impact of NSA revelations found that almost half—47 percent—had changed their approach to online activity in response to reports of NSA surveillance.

Survey participants reported thinking more carefully about where they go, what they say, and what they do online, and about a quarter are less inclined to use email. Other studies have

documented the real and projected economic costs of NSA surveillance to the US Internet industry (as high as US$180 million in lost sales for the cloud computing industry) as loss of trust in US-origin technologies and services drives business overseas. A report from Open Technology Institute released in July 2014 begins to catalogue some of these costs, as well as harm to Internet openness, US foreign policy interests, and cyber security.

Perhaps one of the biggest casualties of the Snowden revelations has been the US and UK's moral authority to criticize the surveillance abuses of other governments and lead by example.

A March 2014 Human Rights Watch report documented how the Ethiopian government uses surveillance to monitor opposition groups and journalists and silence dissenting voices. With unfettered access to mobile networks, security agencies regularly intercept calls and access phone records, which are then played during abusive interrogations, without any process or oversight.

A former Ethiopian opposition party member told Human Rights Watch: "One day they arrested me and they showed me everything. They showed me a list of all my phone calls and they played a conversation I had with my brother. They arrested me because we talked about politics on the phone. It was the first phone I ever owned, and I thought I could finally talk freely."

Earlier in 2014, the Ethiopian government arrested a group of bloggers who wrote on current events under a collective known as Zone 9. The Zone 9 bloggers now face politically motivated charges under Ethiopia's deeply flawed anti-terrorism law. The charges cite as evidence the fact that the bloggers traveled out of the country to receive training in encrypting their communications.

The Ethiopian state is not the US or the UK, but the US and UK statements and actions set a troubling precedent that undermine their credibility on rights and will be cited by many other governments. If the US, the UK, and their allies continue to argue, for example, that metadata deserves little privacy protection, then how can they effectively challenge Ethiopia when the government adopts the same legal argument? And if US and UK authorities continue to vilify and weaken broad use of encryption to protect ordinary

Internet users, how can their governments credibly condemn other governments that outlaw and punish use of encryption in the name of security?

International Standards for the Digital Age

The Snowden revelations have launched a global debate about modern surveillance, national security, and human rights. Privacy is now on the agenda of a range of states and international institutions for the first time.

Several major UN human rights institutions have begun to examine modern surveillance practices. In March 2014, the Human Rights Committee, an international expert body and authoritative interpreter of the International Covenant on Civil and Political Rights (ICCPR)—a global treaty to which the US is party—called on the US to ensure all surveillance is necessary and proportionate to achieving legitimate objectives regardless of the nationality or location of individuals who are affected.

In July 2014, the UN's top human rights official, then-High Commissioner for Human Rights Navi Pillay, issued a groundbreaking report on privacy in the digital age that directly challenges US and UK arguments for secret mass surveillance.

Pillay notably concluded that mass surveillance was "emerging as a dangerous habit rather than an exceptional measure." She said unchecked snooping could harm a range of human rights, including freedom of expression and association. The onus was on governments, she said, to demonstrate that their practices were necessary and proportionate to their security aims. In other words, spying on everyone because you can does not mean you should.

The high commissioner's report followed sustained action from privacy advocates and a group of countries, led by Germany and Brazil, to press the US and UK to stop mass surveillance and safeguard the privacy of people around the world. Stepping into the leadership vacuum, Germany and Brazil, along with Austria, Liechtenstein, Mexico, Norway, and Switzerland, led the passage of the December 2013 UN General Assembly resolution calling for the high commissioner's report.

In the face of inaction by the US, the UK, and their closest allies, these UN institutions have begun to lay out a principled approach to surveillance and human rights in the digital age, grounded in widely accepted standards of international human rights law.

Several critical themes emerging from this work directly challenge the defenses of mass surveillance:

- **Surveillance harms a range of rights beyond privacy, including freedom of expression, association, and movement, as well as the right to counsel.** If individuals cannot go online without fear of undue monitoring, the power of digital technologies to enable rights will be deeply undermined. Journalists cannot protect their sources, lawyers cannot ensure the confidentiality of their communications with clients, and human rights defenders cannot do their work safely.
- **States have obligations to safeguard the privacy rights of users outside their borders.** In our globally networked age, it is untenable to argue that the right to privacy stops at the border while surveillance is borderless.
- **Mass surveillance is by nature indiscriminate and it is presumptively illegal.** Article 17 of the ICCPR requires that any interference with privacy be proportionate and narrowly tailored. Just because mass surveillance and bulk data collection might yield some information that may one day be useful, it cannot justify the invasion of everyone's privacy.
- **States should recognize that privacy and other rights are harmed when they collect private data, regardless of whether that data is used.** Knowing that the government can acquire data about your communications and online activities can chill freedom of expression and association, even if the data collected is never misused. States should impose meaningful limits on when data can be collected, as well as on how data may be used and how long it is retained.
- **States should increase transparency and oversight over surveillance and intelligence gathering powers.** There are legitimate reasons for secrecy when addressing national security threats. But such powers must be subject to oversight to prevent overreach and abuse, including through judicial and parliamentary bodies.
- **The private sector has a responsibility to respect rights when asked to facilitate surveillance or data collection.** Where Internet or telecommunications

companies turn over user data or assist with surveillance without adequate safeguards, they risk complicity in resulting violations.

The Way Ahead

While the Snowden controversy has focused on the US and UK, as noted above, there is no reason to assume that other governments' laws or practices are better. Most privacy regimes were put in place during the Internet's infancy, before social media or smart phones existed, and they are now falling short in providing meaningful protection for rights. And, of course, there are those governments like Ethiopia, China, and Russia who routinely engage in abusive surveillance as a matter of policy and design.

Thanks to Brazil and Germany, there is international momentum to develop norms and guidance and establish institutions to ensure that privacy still has meaning in the digital age. As part of this effort in the coming months, Human Rights Watch will support the creation of a new special rapporteur on the right to privacy at the UN Human Rights Council—an independent expert tasked with scrutinizing state surveillance practices in a sustained and systematic way.

At time of writing, however, there is still a desire to secure buy-in from the US and UK as mass surveillance debates play out at these international venues. The instinct to treat the US and UK with diplomatic kid gloves is not surprising, given their technological capacity and political power. But ultimately, this approach may be counterproductive. In the short term, they are more likely to play the role of spoilers rather than promoters of principled standards. This was certainly true during the debate that led to the December 2013 UN General Assembly resolution on privacy in the digital age, when the US and UK pushed, somewhat successfully, to water down the text behind the scenes, and again in November 2014, with respect to the follow-on resolution on the same topic.

Of course, we must continue to press for reforms in the US and UK and urge these governments to extend privacy protections to those outside their borders. But we should not allow political paralysis in the US and UK to hamper development of international privacy norms. A process of broad international engagement, including with strategic allies, can facilitate the US and UK's eventual acceptance and internalization of strong international

standards over time. When other nations and international institutions lead by example and establish strong human rights standards, they will bring the US and UK along.

Global norm development is just a first step, however. The Snowden revelations have shown how far security agencies are liable to go when they are allowed to operate with inadequate oversight and accountability. As new surveillance capabilities develop and states grapple with renewed security threats—whether terrorism and violent extremism or cyber attacks—sustained public scrutiny and national implementation of global norms are needed. The Pillay report has provided much-needed guidance. The onus is now on parliaments and legislatures around the world to examine surveillance practices and assess their costs and tangible benefits more closely and publicly within a human rights frame.

Surveillance must remain on the human rights agenda, nationally and globally. Otherwise, we risk transforming the Internet into every government's all-seeing panopticon.

Cynthia Wong is senior researcher on the Internet and human rights at Human Rights Watch