Watchdogs Under Watch: Media in the Age of Cyber Surveillance

BY DON PODESTA

April 2015

rnw

CIMA
CENTER FOR INTERNATIONAL MEDIA ASSISTANCE

NED National Endowment for Democracy
Supporting freedom around the world

CIMA
CENTER FOR INTERNATIONAL MEDIA ASSISTANCE

ABOUT CIMA

The **Center for International Media Assistance (CIMA),** at the National Endowment for Democracy, works to strengthen the support, raise the visibility, and improve the effectiveness of independent media development throughout the world. The center provides information, builds networks, conducts research, and highlights the indispensable role independent media play in the creation and development of sustainable democracies. An important aspect of CIMA's work is to research ways to attract additional U.S. private sector interest in and support for international media development.

CIMA convenes working groups, discussions, and panels on a variety of topics in the field of media development and assistance. The center also issues reports and recommendations based on working group discussions and other investigations. These reports aim to provide policymakers, as well as donors and practitioners, with ideas for bolstering the effectiveness of media assistance.

Center for International Media Assistance
National Endowment for Democracy

1025 F STREET, N.W., 8TH FLOOR
WASHINGTON, DC 20004
PHONE: (202) 378-9700
FAX: (202) 378-9407
EMAIL: CIMA@ned.org
URL: http://cima.ned.org

Mark Nelson
SENIOR DIRECTOR

National Endowment for Democracy
Supporting freedom around the world

Watchdogs Under Watch: Media in the Age of Cyber Surveillance

APRIL 2015

CONTENTS

ABOUT THE AUTHOR

Don Podesta is the manager and editor at the Center for International Media Assistance at the National Endowment for Democracy. Previously he was an assistant managing editor at the *Washington Post,* where he also served as the paper's news editor and deputy foreign editor. From 1992 to 1994, he was the *Post*'s correspondent in South America, covering Peru's war against the Shining Path guerrilla movement; presidential elections in Bolivia, Chile, and Paraguay; the drug violence in Colombia; and several economic, social, and environmental issues in Brazil and Argentina. Before joining the *Post*, he worked as an editor or reporter for the *Washington Star,* the *Minneapolis Star,* the *Miami Herald* and the *Arizona Republic*.

Podesta holds a master's degree in international affairs from American University's School of International Service and a bachelor's degree in journalism from Arizona State University. He is the author of two other CIMA reports, *Soft Censorship: How Governments Around the Globe Use Money to Manipulate the Media* (2009) and *Business Journalism Thrives—Even Under Repressive Regimes* (2014).

ABOUT THIS REPORT

Watchdogs Under Watch: Media in the Age of Cyber Surveillance is a joint publication of **Radio Netherlands Worldwide (RNW)** and the **Center for International Media Assistance**.

RNW, the international broadcaster for the Netherlands, is a multimedia organization aimed at the support of free speech. It targets young people in countries where freedom of expression is severely restricted. RNW uses social media, online platforms, audio, and video to discuss sensitive issues.

rnw

The right to privacy is often understood as an essential requirement for the realization of the right to freedom of expression. Undue interference with individuals' privacy can both directly and indirectly limit the free development and exchange of ideas.

— FRANK LARUE, Report to the United Nations, 2013[1]

Big Brother is watching you.

— GEORGE ORWELL, *1984*
(Published in 1948)

Introduction

Electronic surveillance—of e-mail communications, telephone calls, visits to websites, online shopping, and even the physical whereabouts of individuals—is now pervasive the world over. This has enormous implications for privacy and for freedom of expression and association on the one hand and for national security and law enforcement on the other. Striking the right balance between these fundamental human rights and the need for governments to protect their citizens presents a daunting challenge for policy makers, civil society, news media, and, in the end, just about everybody.

For developing countries and those in the media development community, revelations beginning in 2013 about the extent of government surveillance of communications raise serious problems.

Some would argue that surveillance by Western governments that preach the gospel of free media smacks of hypocrisy and gives authoritarian governments cover to engage in similar action. Government surveillance makes it particularly difficult for civil society and media-support groups to do their work, especially where media institutions are weak and where freedom of expression is not ingrained in the local culture but rather is seen as a foreign concept. It especially damages Western government programs aimed at promoting Internet freedom worldwide.

The government of Pakistan, for example, is pushing "back against attempts to curb government surveillance. 'If the citizens of the United States of America cannot have these rights, how can you?' is an argument that rights advocates hear way too often," wrote Sana Saleem, a director of Bolo Bhi, an Internet rights group based in Pakistan, in a blog for the Committee to Protect Journalists one year after massive electronic surveillance by the U.S.'s National Security Agency (NSA) came to light. The Pakistani government, she wrote, "is seeking to replicate a NSA-like model in this country."[2]

Such challenges to freedom of expression and media development around the world require action by democratic governments, civil society, and media organizations. The aim of this briefing paper is to inventory the dilemmas that arise from the growth of electronic surveillance and consider the policy choices to try to address these dilemmas.

Internet Users by Country (2014)

RANK	COUNTRY	COUNTRY'S SHARE OF WORLD INTERNET USERS	NUMBER OF INTERNET USERS
1	CHINA	21.97%	641.6 M
2	UNITED STATES	9.58%	279.8 M
3	INDIA	8.33%	243.2 M
4	JAPAN	3.74%	109.3 M
5	BRAZIL	3.69%	107.8 M
6	RUSSIA	2.89%	84.4 M
7	GERMANY	2.46%	71.7 M
8	NIGERIA	2.30%	67.1 M
9	UNITED KINGDOM	1.95%	57.1 M
10	FRANCE	1.90%	55.4 M
11	MEXICO	1.74%	50.9 M
12	SOUTH KOREA	1.55%	45.3 M
13	INDONESIA	1.45%	42.3 M
14	EGYPT	1.38%	40.3 M
15	VIETNAM	1.36%	39.8 M
16	PHILIPPINES	1.35%	39.5 M
17	ITALY	1.25%	36.6 M
18	TURKEY	1.21%	35.4 M
19	SPAIN	1.20%	35.0 M
20	CANADA	1.13%	33.0 M
21	POLAND	0.88%	25.7 M
22	COLOMBIA	0.88%	25.7 M
23	ARGENTINA	0.86%	25.0 M
24	SOUTH AFRICA	0.85%	25.0 M
25	IRAN	0.76%	22.2 M
26	AUSTRALIA	0.73%	21.2 M
27	MOROCCO	0.69%	20.2 M
28	PAKISTAN	0.69%	20.1 M
29	THAILAND	0.66%	19.4 M
30	SAUDI ARABIA	0.60%	17.4 M

0 100M 200M 300M 400M 500M 600M 700M 800M

Source: *http://www.internetlivestats.com/internet-users-by-country/*

The Spread of Cyber Surveillance

E-mails never die. Once sent, they live on—stored on a server somewhere or on the recipient's computer hard drive from where they can be retrieved. They also can be intercepted en route. Phone calls leave records that telecommunication companies keep and are sometimes required to share with government investigators or intelligence services. And of course phone calls, too, can be subject to eavesdropping in real time. Today's smartphones have geo-location capabilities and depend on communication with cellphone towers, whose locations are also known, making their users' whereabouts discoverable at all times.

Then there's "the Internet of things," the increasing digital connectivity of everything from smart watches and health-monitoring devices to kitchen refrigerators, all capturing and sending personal data across the Internet in order to serve up more information and facilitate transactions that consumers want. Of course this data, too, can be monitored.

So who wants all this information about individuals?

- Governments, especially intelligence services, the military, and law enforcement agencies.
- Private companies, including marketers of merchandise and services and providers of online communication platforms, including social media and e-mail.
- Hackers and cyber criminals.

This paper focuses on the first two—the behavior of governments and private companies in the realm of cyber surveillance and tracking. Addressing the third category—hackers and criminals—would require delving into issues such as identity theft and credit card fraud, which lie beyond the scope of this paper.

GOVERNMENT MONITORING

As the tools for tracking digital communications become more sophisticated, the consequences for citizens' privacy and freedom of expression become more critical. In late 2014 Freedom House reported that "more people were detained or prosecuted for their digital activities in the past year than ever before. Since May 2013, arrests for online communications were documented in 38 of the 65 countries studied in

China has more netizens than any other country in the world, and they know that their government monitors their communication. For example, users of the popular WeChat mobile messaging platform warn each other not to say certain things that would draw the attention of the Chinese Communist Party.... There is self-censorship all over China.

Freedom on the Net 2014, with social-media users identified as one of the main targets of government repression."[3]

That authoritarian governments in countries such as Iran and China monitor their citizens' activities on the Internet is well known, as are their motives. They may defend these practices as necessary to combat terrorism and crime and maintain social order, but such surveillance is also aimed at keeping themselves in power.

China has more netizens than any other country in the world, and they know that their government monitors their communication. For example, users of the popular WeChat mobile messaging platform warn each other not to say certain things that would draw the attention of the Chinese Communist Party, says Xia Yeliang, a former professor at Peking University and now a visiting fellow at the Cato Institute in Washington. There is, he says, "self-censorship all over China."

China also has more netizens in prison than any other country. The next most prolific jailer of bloggers is Vietnam. "Vietnamese activists have been the target of sophisticated cyberattacks," Freedom House says in its Internet freedom report. "In 2014, researchers found that a progovernment squad of hackers, active since 2009, targeted at least one civil society group and at least one news organization writing about Vietnam, as well as Vietnamese bloggers overseas. The malicious software used in the attacks was advanced enough to evade detection by almost all commercial antivirus programs, and sent from servers in locations around the world."[4]

Russia enacted a law in May 2014 requiring websites with more than 3,000 followers to register with the government as media outlets, making it nearly impossible for many bloggers to operate anonymously. Search engines and other Internet service providers must retain records of postings for six months. And under another law, Russian Internet service providers must install monitoring devices on their network that allow the FSB, successor to the Soviet KGB, to collect traffic directly.

However, democratic governments also engage in mass surveillance, which equally affects their citizens' rights to free expression and privacy. Why is this so in societies that espouse freedom of expression and association and access to information as values? For two closely related reasons:

- to prevent physical terrorist attacks, such as those that took place in New York on September 11, 2001, and in Paris in January of this year.
- to protect national infrastructure and electronic data from both physical and cyber attacks—not just from terrorists and criminals but also from foreign governments.

Governments see ensuring national security and the safety of their citizens as a paramount duty. In the 21st Century, the theater of operations for inter-state conflict and terrorism extends to cyberspace, which means that not engaging online is not an option for intelligence and law-enforcement agencies nor for the military.

Less than two weeks after the attacks on the satirical newspaper *Charlie Hebdo* and a kosher market in Paris, European leaders moved to tighten intelligence about travelers in the European Union's member states. Following a meeting of European foreign ministers and diplomats from Middle Eastern countries on January 19, Federica Mogherini, the EU's high representative for foreign affairs and security policy, said that the EU plans "to share information, intelligence, not only with the European Union but also with other countries around us."[5]

The extent of the U.S. government's massive data collection through the National Security Agency came to light in June 2013, revealed by NSA subcontractor Edward Snowden. The revelations became a scandal on a global scale and created a serious diplomatic problem for Washington when it became known that the private communications of foreign leaders in friendly countries from Brazil to Germany had been intercepted.

In Europe, reporting in *The Guardian* by Glenn Greenwald—one of the journalists to whom Snowden leaked the NSA documents—about the extent of data collection from private citizens and government leaders raised a storm of outrage, especially in Germany and France. "The most under-discussed aspect of the NSA story has long been its international scope. That all changed…as both Germany and France exploded with anger over new revelations about pervasive NSA surveillance on their population and democratically elected leaders," Greenwald wrote in *The Guardian*. "As was true for Brazil previously, reports about surveillance aimed at leaders are receiving most of the media attention, but what really originally drove the story there were revelations that the NSA is bulk-spying on millions and millions of innocent citizens in all of those nations."[6]

In the United Kingdom, a court ruled in December 2014 that mass surveillance of online and cellphone communications of the type the NSA carries out is legal.[7] Following the attack on *Charlie Hebdo,* Prime Minister David Cameron called for a ban on encrypted communications, saying, "In our country, do we want to allow a means of communication between people which […] we cannot read?"[8]

German Interior Minister Hans-Peter Friedrich, in an interview with the magazine *Der Spiegel* in 2013, argued in favor of Internet surveillance

The extent of the U.S. government's massive data collection through the National Security Agency came to light in June 2013, revealed by NSA subcontractor Edward Snowden. The revelations became a scandal on a global scale and created a serious diplomatic problem for Washington when it became known that the private communications of foreign leaders in friendly countries from Brazil to Germany had been intercepted.

The U.S. military now calls cyberspace the 'fifth domain' of warfare, and it views supremacy there as essential to its mission, just as it is in the other four: land, sea, air, and space.

— SHANE HARRIS
@War: The Rise of the Military-Internet Complex

by intelligence agencies. The German government has "to balance out a loss of control over the communication of criminals through new legal and technological means, Friedrich said. "Of course our intelligence agencies also have to be present on the Internet."[9]

This activity is not purely defensive in nature. The U.S. "military now calls cyberspace the 'fifth domain' of warfare, and it views supremacy there as essential to its mission, just as it is in the other four: land, sea, air, and space," writes Shane Harris in his book *@War: The Rise of the Military-Internet Complex*. "For more than a decade," Harris writes, "cyber espionage has been the single most productive means of gathering information about the country's adversaries—abroad and at home."[10]

In 2012, then-U.S. Defense Secretary Leon Panetta warned of a "cyber-Pearl Harbor that would cause physical destruction and the loss of life, an attack that would paralyze and shock the nation and create a profound new sense of vulnerability."[11]

Defending against such a cyberattack implies high levels of cyber vigilance and—along with preventing an offline, physical attack—serve as the government's justification for engaging in mass surveillance.

A report about "big data" issued by the White House in May 2014 puts it this way:

> Computational capabilities now make "finding a needle in a haystack" not only possible, but practical. In the past, searching large datasets required both rationally organized data and a specific research question, relying on choosing the right query to return the correct result. Big data analytics enable data scientists to amass lots of data, including unstructured data, and find anomalies or patterns. A key privacy challenge in this model of discovery is that ***in order to find the needle, you have to have a haystack***. To obtain certain insights, you need a certain quantity of data (emphasis added).[12]

Regardless of whether the intent is to improve security or to clamp down on dissent, the trend worldwide is toward more online surveillance. In 2014, Freedom House reported, 19 of the 65 countries it surveyed passed new laws "that increased surveillance or restricted user anonymity, including authoritarian countries where there is no judicial independence or credible legal recourse for users."[13]

THE CRUCIAL ROLE OF PRIVATE COMPANIES

Governments cannot do it alone. Most digital communications flow through and are stored on the servers of private corporations, particularly Internet giants such as Google and Facebook and telecommunications companies. Many of these companies operate globally but are based in the United States and are subject to U.S. laws as well as the laws of countries in which they do business. To the degree that they share data with governments—either in the United States or in other countries where they operate—these companies have a profound effect on the privacy of communications and therefore on freedom of expression and the flow of information worldwide.

The sheer size of the customer bases of just a handful of these Internet companies is an indicator of how much of the world's digital communication they control. Google carries anywhere from 25 percent of all Internet traffic in North America to 40 percent, depending on whose estimates you believe, and more than 400 million people use its e-mail service. Apple has sold in the neighborhood of 500 million iPhones. Yahoo claims 800 million active users monthly. In 2013, Microsoft reported that 420 million people were using its e-mail service, Outlook.[14]

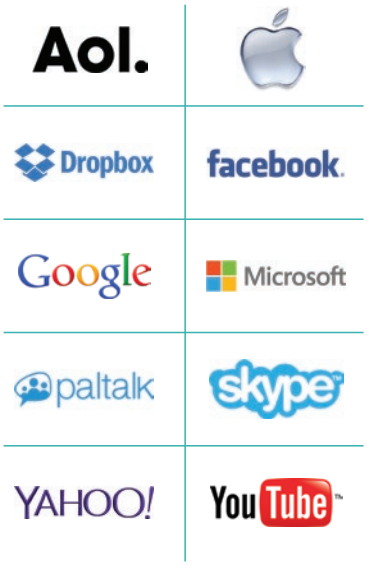
Aside from the fact that they are all American technology giants, what do these companies have in common? They and several others were recruited by the NSA for its Prism surveillance program, revealed by Snowden in 2013.

Prism arose from an act of the U.S. Congress in 2007 that gave "the NSA license to demand access to huge volumes of data from US technology companies by broadly invoking the need to protect national security," Harris writes in *@War*.[15] Other tech firms who have participated in Prism include Facebook, AOL, Dropbox, PalTalk, Skype, and YouTube. *The Guardian* reported that a British intelligence agency, the Government Communications Headquarters (GCHQ) was also secretly collecting data from these companies.[16]

Prism isn't the NSA's only project involving U.S. technology companies. The agency also works with them to insert "backdoors" and vulnerabilities into their products so that potential obstacles to surveillance, such as encryption software, are removed or disabled.

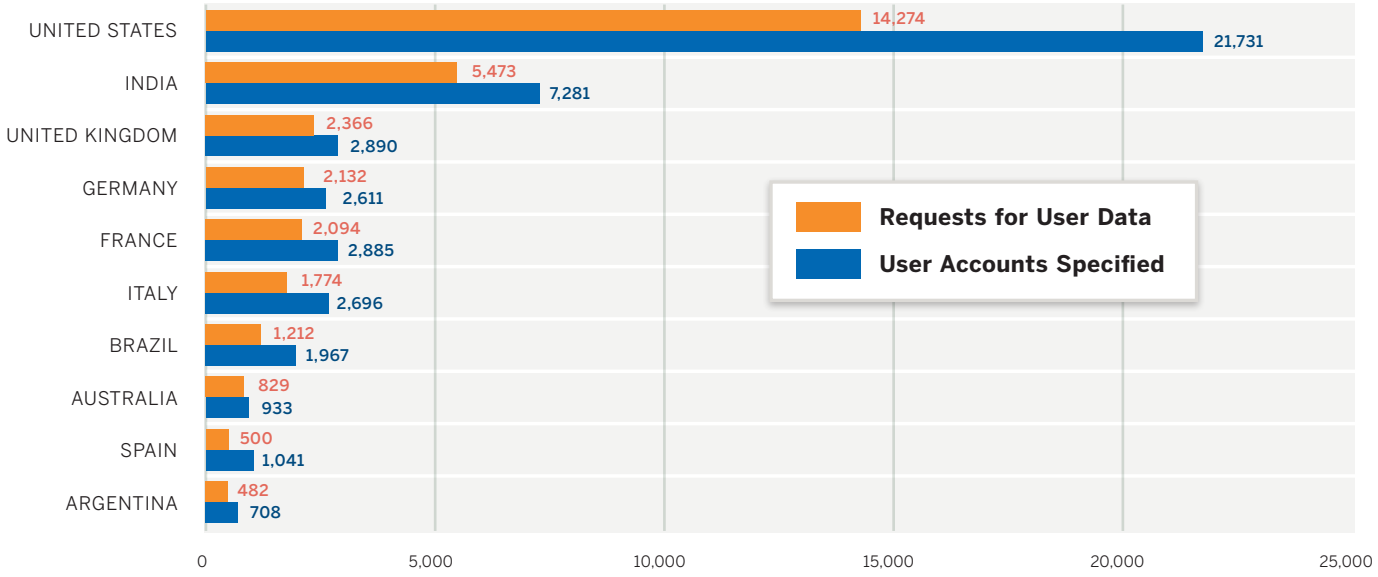
On the other hand, some of the big players on the Internet are trying to protect privacy in other ways. In 2008, Microsoft, Google, and Yahoo launched the Global Network Initiative (GNI) with the aim of assisting telecommunications and Internet companies support the rights to privacy and freedom of expression around the world. Since then, the

Prism arose from an act of the U.S. Congress in 2007 that gave "the NSA license to demand access to huge volumes of data from US technology companies by broadly invoking the need to protect national security,"



Facebook Government Requests Report, July–Dec 2014

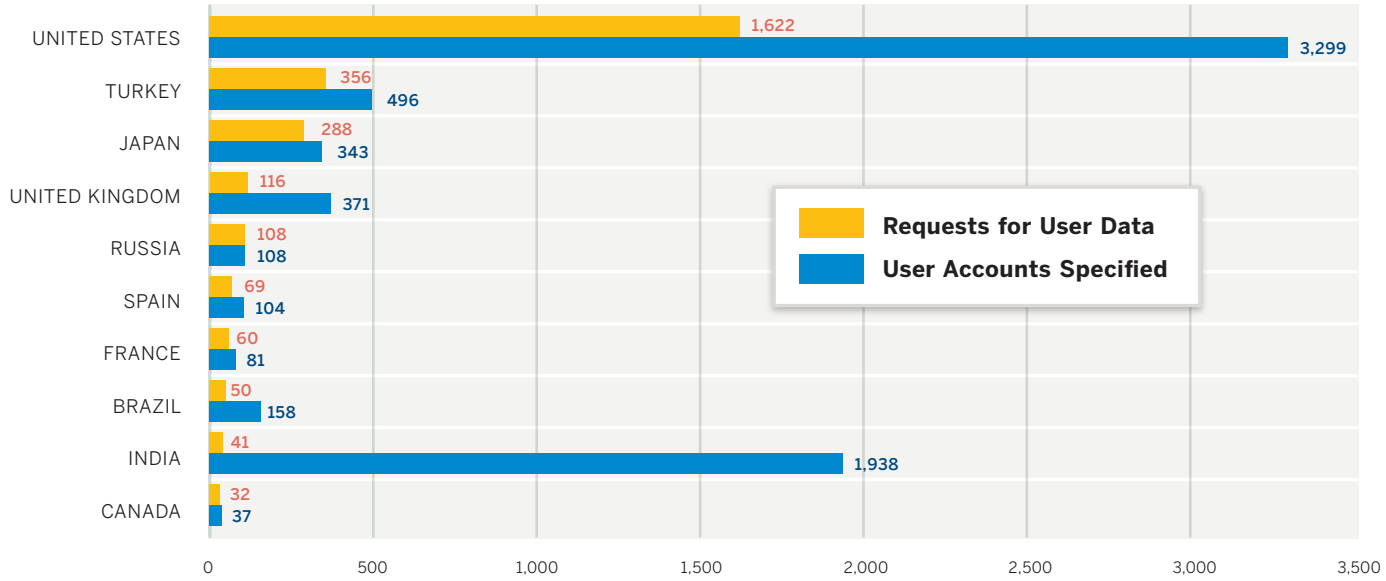
GOVERNMENT REQUESTS FOR INFORMATION ABOUT USER ACCOUNTS



Source: *https://govtrequests.facebook.com/*

Twitter Government Requests Report, July–Dec 2014

GOVERNMENT REQUESTS FOR INFORMATION ABOUT USER ACCOUNTS



Source: *https://transparency.twitter.com/information-requests/2014/jul-dec*

group has been joined by Facebook and several NGOs, press freedom organizations, and others and now has around three dozen members.

Google, Twitter, and Facebook issue periodic reports on the number of requests for information about their users and provide some level of detail, such as identifying the countries making the request and the percentage of requests with which they complied. Google's G-mail is encrypted, and the company stopped censoring its Chinese search engine in 2010. And Apple is engineering its smart phones so the government will be unable to extract data.

Still, Danny O'Brien, the Electronic Frontier Foundation's international director, argues that big Internet-based companies such as Google and Facebook actually decrease the security of the Internet because they create these "giant honeypots of data all in one place."[17]

Ironically, some of the NSA's surveillance activity is in conflict with other aspects of U.S. government policy. For example, the U.S. State Department has spent millions of dollars supporting TOR, a system developed by the U.S. Naval Research Laboratory that allows users to connect to the Internet anonymously. It is used by dissidents and activists in many parts of the world to avoid government surveillance. Yet among the NSA's activities were attempts to penetrate or disrupt TOR.[18]

Nor are U.S. companies the only ones involved in cyber surveillance. Development of surveillance technology starts with the Western democracies, moves to other democracies and allies, and then to the private sector, which sells it around the world, including to non-democracies. "It is significantly analogous to the weapons trade," says Craig Timberg, a *Washington Post* reporter who specializes in privacy, security, and surveillance.[19]

For example, in 2008, Iranian mobile phone operators bought technology used to track down dissidents from a Finnish-German consortium, Nokia-Siemens Networks. In Belarus, a system sold by Ericsson, a Swedish provider of telecommunications services, "was reported to have been put to similar use in the wake of postelection protests," Rebecca MacKinnon writes in her book, *Consent of the Networked: The Worldwide Struggle for Internet Freedom.*[20]

In both cases, it was legal to sell the technology used to spy on dissidents. In fact, the technology "is standard 'lawful intercept' required by law in Europe, so that police can track criminals," MacKinnon writes. "Unfortunately, with the same technology in the hands of a regime that defines 'crime' broadly to include political dissent and 'blasphemy,' the result is an efficient surveillance machine."[21]

Some argue that big Internet-based companies such as Google and Facebook actually decrease the security of the Internet because they create these "giant honeypots of data all in one place."

Cyber Surveillance and the Media

No citizen wants to be spied upon. But for journalists, being the object of secret surveillance presents an additional problem: Doing their jobs can put others in jeopardy. As the Committee to Protect Journalist puts it:

> Revelations about surveillance, intimidation, and exploitation of the press have raised unsettling questions about whether the U.S. and other Western democracies risk undermining journalists' ability to report in the digital age. They also give ammunition to repressive governments seeking to tighten restrictions on media and the Internet. When journalists believe they might be targeted by government hackers, pulled into a criminal investigation, or searched and interrogated about their work...their ability to inform the public erodes. If journalists cannot communicate in confidence with sources, they cannot do their jobs.[22]

In authoritarian countries, journalists can become "one-stop shopping" for governments to locate dissidents and activists. "We are remarkably valuable targets," says Washington Post reporter Timberg, "not so much for what we know but for who we know."

One of the biggest challenges presented by Internet and cellphone surveillance, says the EFF's Danny O'Brien, "is that the knowledge of surveillance has an effect. If you believe everything you do is unprotected or if your sources don't believe you can protect them, this has a chilling effect. Journalists are the canary in the coal mine for this. Journalists traditionally do things in a sneaky way...they snoop around. They're very suspicious individuals, but they're an important part of a free society."

Silvia Chocarro, a media consultant who worked on UNESCO's 2010 and 2012 reports on the safety of journalists and now a correspondent for Radio France International, agrees: "If journalists can't protect their sources, investigative journalism is finished."[23]

In authoritarian countries, journalists also must worry about protecting themselves, in addition to their sources. Not only can governments track their movements and communications within their countries' borders, but also internationally.

A case in point: An e-mail to a Chinese journalist based in the United States requesting an interview was politely declined, also by e-mail. But within minutes the journalist telephoned to say that an interview was indeed possible but that any further communication by e-mail was not. The interview took place in a public setting, away from the place of work of the writer who sought the interview.[24]

Similarly, Ethiopian Satellite Television, an Ethiopian exile media organization based in Alexandria, Virginia, has been hacked from abroad, most likely by the Ethiopian government, using commercial spyware, according to The Citizen Lab at the University of Toronto's Munk School of Global Affairs.[25]

The international trade in sophisticated spyware is mostly unregulated, which makes it readily available to governments and individual hackers alike. "We're finding this in repressive countries, and we're finding that it's being abused," Bill Marczak, one of the authors of the Citizen Lab's report, told the *Washington Post*. "This spyware has proliferated around the world...without any debate."[26]

Within the borders of certain countries both local media organizations and international ones must tread with care.

Radio Netherlands Worldwide (RNW), which partnered with CIMA to produce this paper, runs a program in Saudi Arabia that uses Google Hangout to deal with social issues that cannot be discussed in the mainstream Saudi media. It is a discussion program, combined with video clips and guest appearances by people from civil society and, when possible, government representatives. But it steers clear of national politics. "It's an editorial choice not to go Saudi bashing," says Jannie Schipper, RNW's producer-editor in charge of Saudi content.[27]

In order to avoid the risk of government monitoring, many of the program's guests appear anonymously, either kept off camera or given false names. Publishing content that the Saudi authorities object to can have severe consequences, as demonstrated by the sentence of 10 years

In authoritarian countries, journalists also must worry about protecting themselves, in addition to their sources. Not only can governments track their movements and communications within their countries' borders, but also internationally.

© Photo courtesy of RNW

RNW staff protest for the release of imprisoned al-Jazeera journalists.

More than 1 in 3 writers

in Free countries [as characterized by Freedom House]...said that they had avoided writing or speaking on a particular topic, or had seriously considered it, due to concerns about surveillance.

in prison and 1,000 lashes for Raif Badawi, the Saudi blogger who dared to criticize Saudi Arabia's clerics.

"Sometimes it's hard to convince people to take any security measures, either because they have already been harassed anyway," Schipper said, or because they think they're too low profile to be noticed.

Writers in general—not only members of the news media—report feeling the chilling effects of surveillance since the reports of the NSA's data collection practices came to light.

"Surveillance conducted by government authorities induces self-censorship by writers around the world," according to a survey of writers by PEN International released in January. "More than 1 in 3 writers in Free countries [as characterized by Freedom House]...said that they had avoided writing or speaking on a particular topic, or had seriously considered it, due to concerns about surveillance."[28]

SURVEILLANCE WITHOUT INTERCEPTION

Governments do not need to resort to secret electronic interception of private communications in real time to track individuals. In the "Information Age," the data is hiding in plain sight. Smart phones come loaded with applications that send out information about their users, especially their physical location. Even simple cellphones must exchange signals with transmission towers, whose locations are known. Facial-recognition software can be used to identify dissidents participating in protests from images captured on video or in photographs.

"There's so much information out there that you can construct an iron-clad case against any journalist, using 'evidence' such as who you're friends with on Facebook, who you follow on Twitter, who is on your contacts list on your phone," says Courtney Radsch, advocacy director for the Committee to Protect Journalists (CPJ). Cyber surveillance, she says, has "completely undermined the ability of journalists around the world to do their work."[29]

Citizens, including journalists and bloggers, are reluctant to give up their electronic gadgets, which means they are willingly trading convenience for privacy.

For international media organizations, which must communicate with their correspondents all over the world, who in turn must communicate with their sources, this presents a major challenge. Bernadette van Dijck, RNW's senior adviser and strategist for business intelligence, says: "We are acting in a global communication world, and at RNW we focus on countries where freedom of the press and freedom of expression are severely restricted...so we operate in cyberspace and especially on social media to stretch that space for free speech."[30]

Under the auspices of Radio Free Asia, the Open Technology Fund is working to open that space for free speech by developing communications technology and platforms that are secure, easy to use, and portable. "When we fund a tool, we require that it be useable by anyone in the world for free," says Libby Liu, president of RFA and strategic and operations director of the OTF.

After the Saffron Revolution in Burma of 2007, many of RFA's sources there "were thrown in prison for talking to us" during the pro-democracy protests, Liu says. "I don't want any more of those lives lost on our watch."

"We are acting in a global communication world, and at RNW we focus on countries where freedom of the press and freedom of expression are severely restricted...so we operate in cyberspace and especially on social media to stretch that space for free speech."

— BERNADETTE VAN DIJCK, RNW senior adviser and strategist for business intelligence

"There are a lot of people who do good in the world, and if you don't protect their work...you're just making a target list. You don't want to hurt the people you're trying to help."

— LIBBY LIU, president of Radio Free Asia and strategic and operations director of the Open Technology Fund

"There are a lot of people who do good in the world," Liu says, "and if you don't protect their work...you're just making a target list. You don't want to hurt the people you're trying to help."

Another—and perhaps easier—way for governments to track the movements of journalists and their interactions with sources doesn't involve directly intercepting communications electronically. Instead, they can go to intermediaries, such as Internet and telecommunications companies. In the case of the U.S. Justice Department's seizure of the Associated Press's telephone records in 2013, the investigators pursuing a leak case went to the phone company, not to the AP.

"It used to be that reporters were once able to protect their sources by refusing to testify in court," says Trevor Timm, co-founder and the executive director of the Freedom of the Press Foundation. Now, he says, the authorities can get what they want from telephone call records or direct electronic surveillance "and never have to go to the reporter in the first place."[31]

Freedom of expression and journalism NGOs work to protect journalists from the dangers of surveillance by stressing good "digital hygiene," such as maintaining strong computer passwords and using encryption in electronic communications. These have been detailed on their websites and in their handbooks and reports and do not need to be recounted here. The larger question is what can be done on a societal level to protect freedom of expression and privacy in the face of the growing sophistication of the digital tools for surveillance of citizens, including journalists.

The Dilemma: Security and Freedom of Expression

The world's governments are not about to stop using the electronic tools available to them to protect their citizens from terrorists, criminals, and potential foreign enemies. Where, then, does that leave privacy and the right to freedom of expression?

As difficult as reconciling these seemingly contradictory imperatives may be, it is far more likely to be addressed in open, democratic societies than in closed or restricted ones. The foundational documents of nearly every country—including authoritarian ones—refer to the right to freedom of expression. And most countries are signatories to various international covenants on human rights, which include freedom of expression. But not every national government pays heed to such language in their constitutions and international covenants. Perhaps the best place to begin is in those countries that attempt to do so.

One approach might be for civil society, political leaders, and citizens in general who care about privacy and freedom of expression to press for a set of standards, which perhaps could be applicable internationally. In balancing the need for national security with the right to privacy, governments should consider:

- Transparency
- Oversight
- Proportionality

Governments should make clear to their citizenry why surveillance is necessary, under what circumstances it is employed, and what are its limits under the law.

TRANSPARENCY

Governments should make clear to their citizenry why surveillance is necessary, under what circumstances it is employed, and what are its limits under the law. They should also explain what mechanisms are in place for oversight of surveillance methods and how they are implemented.

Internet corporations should make clear their policies on cooperation with government requests for data about their users and continue to publish periodic reports detailing the number and source of the requests and report the responses to those government requests.

"There are principles governments are sworn to uphold... Just because the restrictions [such as against warrantless searches] are old school, doesn't mean they don't apply in the Internet age."

— QUINN MCKEW, deputy executive director of Article 19

There were some incremental steps toward more transparency in early 2015. In February, the British court that oversees intelligence agencies ruled that GCHQ had acted unlawfully in its collection of electronic data in the past because its inadequate oversight violated European human rights law. It was the first time the tribunal had ruled against British intelligence agencies.

However, the tribunal ruled earlier that by making public safeguards in place, GHCQ was now operating within the law and the surveillance could continue, which the agency was quick to point out in reaction to the February ruling. In a statement, CHCQ said, "We are pleased that the court has once again ruled that the U.K.'s bulk interception regime is fully lawful...much of GCHQ's work must remain secret. But we are working with the rest of government to improve public understanding about what we do."[32]

In the United States, the Office of the Director of National Intelligence released its report on signal intelligence reform. Among the changes in policy is a requirement that information about "non-U.S. persons" be deleted in five years if the information has no legitimate intelligence purpose.[33]

OVERSIGHT AND ACCOUNTABILITY

There is an important difference between targeted surveillance and mass surveillance. A law enforcement agency's work to watch out for a specific criminal or terrorism suspect is qualitatively different from collecting everything about everybody and sorting out what is useful later.

While the speed of electronic communications in the 21st Century and the wide range of terrorism threats might make the notion of seeking a court order to allow surveillance of suspects seem quaint, surveillance of citizens and their communications must be within the law, and there must be legal oversight of such surveillance.

"There are principles governments are sworn to uphold," says Quinn McKew, deputy executive director of Article 19. "Just because the restrictions [such as against warrantless searches] are old school, doesn't mean they don't apply in the Internet age."[34]

Oversight courts or agencies should ensure that any surveillance is applicable under the law as intended and that certain laws, such as anti-terrorism statutes, are not being invoked to allow the use of surveillance for other purposes, such as to suppress dissent.

Eduardo Bertoni, former special rapporteur for freedom of expression under the Inter-American Commission for Human Rights, says the objective of a law aimed at curbing child pornography or sex trafficking "can be legitimate, but once you open the door for that you could monitor everything."[35]

As CPJ Executive Director Joel Simon put it in January during a talk on the occasion of the release of his book, *The New Censorship: Inside the Global Battle for Media Freedom,* "There needs to be some framework for what kind of surveillance is legitimate."

Accountability should also apply to the private sector. Other companies should follow the example of Google, Yahoo, Microsoft, and Facebook and join the GNI. The GNI itself should redouble its efforts in supporting human rights, privacy, and free expression internationally.

PROPORTIONALITY

When considering the role of cyber surveillance in national security it is worth asking: What is it that we're trying to secure to begin with and at what cost?

While governments must protect their citizens, that is but one duty among many. Upholding the laws of the nation and protecting citizens' rights are also important duties of governments.

"We take it as a given that we have to protect citizens," says CPJ's Courtney Radsch. "But [what happened on] 9/11 was not for lack of signals intelligence. It was about the failure to connect the dots." In fact, she argues, there is so much data available now that governments lack the ability to deal with it and that more data could actually make it more difficult to analyze it and use it to prevent a terrorist attack.

Trevor Timm of the Freedom of the Press Foundation points to "overclassification"—there are too many secrets, in his opinion. "The best thing the government can do is concentrate on classifying secrets that are truly worthy of being secret," he says. "Prioritize what information you want to protect most rather than assuming everyone is a criminal or a leaker."

"The best thing the government can do is concentrate on classifying secrets that are truly worthy of being secret… Prioritize what information you want to protect most rather than assuming everyone is a criminal or a leaker."

— TREVOR TIMM, Freedom of the Press Foundation

Conclusion

The fundamental problem with cyber surveillance, even for the most well-intentioned governments, is that laws have not evolved with the technology. Governments must enforce the laws that exist and apply them to the modern age. And they should consider that just because technology makes surveillance possible doesn't mean it makes it necessary or justifiable in all cases.

The best one can hope for is international adoption of a set of standards, and the use of those standards by international monitoring organizations to apply pressure on authoritarian governments to meet them.

"Cellphones are mini surveillance devices that are tracking our every move," Timm says. "But just because our cellphones have GPS capability doesn't mean...everyone else has the right to know what you're doing."

These, however, are considerations for countries with rule of law and accountable, open governments. For citizens of nations with authoritarian rulers, securing protection against surveillance is much more problematic and the consequences of running afoul of the authorities who conduct such surveillance much more severe. The best one can hope for is international adoption of a set of standards, as outlined above, and the use of those standards by international monitoring organizations to apply pressure on authoritarian governments to meet them.

For RNW's Bernadette van Dijck, the challenge for international broadcasters is how to strike a balance between open debate and the safety of the people they work with in authoritarian countries: "We are operating within this battlefield or whatever you may call it...with these dilemmas every day."

Endnotes

[1] Frank LaRue, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,* April 17, 2013, 7. *http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf*

[2] Sana Saleem, "A year after Snowden revelations, damage persists to freedom of expression in Pakistan," Committee to Protect Journalists, June 16, 2014, *https://cpj.org/blog/2014/06/a-year-after-snowden-revelations-damage-persists-t.php#more*

[3] Freedom House, *Freedom of the Net 2014,* 7.

[4] Xia Yeliang, remarks at a panel discussion to launch Freedom House's special report: The Politburo's Predicament: Confronting the Limits of Chinese Communist Party Repression, Washington, DC, January 13, 2015.

[5] Michael Birnbaum, "In E.U. a drive to share data," *The Washington Post,* January 20, 2015, Page A1.

[6] Glenn Greenwald, "As Europe erupts over US spying, NSA chief says government must stop media," *The Guardian,* October 25, 2013, *http://www.theguardian.com/commentisfree/2013/oct/25/europe-erupts-nsa-spying-chief-government*

[7] Mark Scott, "British Court Rules in Favor of Electronic Surveillance, *New York Times,* Dec. 5, 2014, *http://www.nytimes.com/2014/12/06/world/europe/british-court-says-governments-electronic-surveillance-is-legal.html*

[8] Andrew Griffin, "WhatsApp and iMessage could be banned under new surveillance plans," *The Independent,* January 12, 2015, *http://www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-and-snapchat-could-be-banned-under-new-surveillance-plans-9973035.html*

[9] "Der Spiegel: Germany to expand Internet Surveillance," *Deutsche Welle,* June 16, 2013, *http://www.dw.de/der-spiegel-germany-to-expand-internet-surveillance/a-16885711*

[10] Shane Harris, *@War: The Rise of the Military-Internet Complex,* (Houghton Mifflin Harcourt, Boston, New York, 2014) xxi.

[11] Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times,* October 12, 2012, *http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0*

[12] Executive office of the President, *Big Data: Seizing Opportunities, Preserving Values,* May 2014, 6, *http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf*

[13] *Freedom of the Net 2014,* 6.

[14] It is difficult to find independent statistics for users of the big Internet companies, as most of the data is held and released by the companies themselves. The information in this paragraph is summarized in Harris (p. 44) and has been checked against these other sources:

http://www.forbes.com/sites/markrogowsky/2014/03/25/without-much-fanfare-apple-has-sold-its-500-millionth-iphone/

http://www.businessinsider.com/yahoo-just-passed-800-million-monthly-active-users-worldwide-2013-9

http://www.forbes.com/sites/timworstall/2013/08/17/fascinating-number-google-is-now-40-of-the-internet/

http://www.cnet.com/news/google-sets-internet-record-with-25-percent-of-u-s-traffic/

[15] Harris, 44.

[16] Greenwald, "NSA Prism program taps in to user data of Apple, Google and others," *The Guardian,* June 7, 2013, *http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data*

[17] Danny O'Brien, interview with author, January 6, 2015.

[18] Harris, 84–86.

[19] Craig Timberg, interview with author, November 24, 2014.

[20] Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom,* (Basic Books, New York, 2012) 56.

[21] Ibid.

[22] Committee to Protect Journalists, Right to Report in the Digital Age advocacy campaign, *http://www.cpj.org/campaigns/digital-freedom/right-to-report-journalists-surveillance-prosecution.php*

[23] Silvia Chocarro, interview with author, January 16, 2015.

[24] Author's personal experience. Date of interview withheld for security reasons.

[25] Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, "Hacking Team and the Targeting of Ethiopian Journalists," *The Citizen Lab,* February 2014, *https://citizenlab.org/wp-content/uploads/2015/01/Hacking-Team-and-the-Targeting-of-Ethiopian-Journalists31.pdf*

[26] Timberg, "Foreign regimes use spyware against journalists, even in U.S.," *Washington Post,* February 12, 2014 *http://www.washingtonpost.com/business/technology/foreign-regimes-use-spyware-against-journalists-even-in-us/2014/02/12/9501a20e-9043-11e3-84e1-27626c5ef5fb_story.html*

[27] Jannie Schipper, interview with author, December 30, 2014.

[28] PEN International, *Global Chilling: The Impact of Mass Surveillance on International Writers,* January 5, 2015, 5, *http://www.pen.org/sites/default/files/globalchilling_2015.pdf*

[29] Courtney Radsch, interview with author, December 15, 2014.

[30] Bernadette van Dijck, interview with author, December 18, 2014.

[31] Trevor Timm, interview with author, January 7, 2015.

[32] Mark Scott, British Court Says Spying on Data Was Illegal," the *New York Times,* February 6, 2015, *http://www.nytimes.com/2015/02/07/world/europe/electronic-surveillance-by-spy-agencies-was-illegal-british-court-says.html?rref=world/europe&module=Ribbon&version=context&region=Header&action=click&contentCollection=Europe&pgtype=article*

[33] *http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties*

[34] Quinn McKew, interview with author, January 8, 2015.

[35] Eduardo Bertoni, interview with author, December 19, 2014.

Center for International Media Assistance

NATIONAL ENDOWMENT FOR DEMOCRACY
1025 F STREET, N.W., 8TH FLOOR
WASHINGTON, DC 20004

PHONE: (202) 378-9700
EMAIL: CIMA@ned.org
URL: http://cima.ned.org

rnw

CIMA
CENTER FOR INTERNATIONAL MEDIA ASSISTANCE

NED
National Endowment for Democracy
Supporting freedom around the world