Comment to Review Group on Intelligence and Communications Technologies
Regarding the Effects of Mass Surveillance
on the Practice of Journalism

October 4, 2013

Introduction

We are writing to the Review Group on Intelligence and Communications Technologies out of a concern about the impact of mass electronic surveillance on the practice of journalism.

We recognize that electronic surveillance plays a key role in law enforcement and national security. However, the tremendous power of Internet-era monitoring raises the most serious kinds of questions about freedom, power, and democracy. In particular, mass surveillance – the bulk interception and storage of citizens' communications and online activities – presents a grave threat to the effectiveness of an independent press.

Of course mass surveillance is of concern to people far removed from journalists and their sources. We are certain that others have made strong arguments about its effects on democracy, privacy, and American life generally. Our intention here is to clarify how such surveillance intersects the routine activities of journalists and their sources.

Put plainly, what the NSA is doing is incompatible with the existing law and policy protecting the confidentiality of journalist-source communications. This is not merely an incompatibility in spirit, but a series of specific and serious discrepancies between the activities of the intelligence community and existing law, policy, and practice in the rest of the government. Further, the climate of secrecy around mass surveillance activities is itself actively harmful to journalism, as sources cannot know when they might be monitored, or how intercepted information might be used against them.

In the sections of this comment we aim to document the following points:

1. The routine practice of journalism depends on sensitive discussions with sources. For this reason, existing law and policy guarantee the right of sources to have confidential discussions with reporters.

2. The NSA's domestic mass surveillance activities contradict this law and policy, specifically the policy laid out in the recent Department of Justice review.

3. Mass surveillance differs in character from individual surveillance, and raises greater issues.

4. It is not even possible for would-be sources to know, in general terms, how they might be monitored and how this might be used against them.

5. This state of affairs has already had a chilling effect on sources.

6. We propose two remedies. First, a principle of parity: journalist-source communications must be protected to the same standards regardless of how they might be obtained. Second, we need greater clarity around the interception, storage, and use of Americans' communications, as the confusing legal landscape chills journalists and sources alike.

1. Journalism depends on confidential discussions with sources

Journalism depends crucially on sources' willingness to talk. In turn, this often depends on the ability of the journalist to have confidential conversations with a source. These sensitive conversations convey critically important information unavailable through formal channels. These are not spectacular leaks of the Manning and Snowden kind, which are rare and unusual in journalism. Instead, we are speaking of the *routine* disclosure of ambiguously authorized material.

We say ambiguously authorized because the relations between sources and reporters are much more nuanced than simply "authorized" versus "leaked." Unofficial disclosure falls everywhere on the spectrum from "my boss told me to say this unofficially" to "I secretly gave damaging information to the press."

Most communications between journalists and their sources are never published. Conversations conducted "on background" or "off the record" provide critical context and leads for the reporter piecing together a story. Such private communication is not about getting the story, but getting the story right. In other cases multiple confidential conversations are required to establish trust before a source feels comfortable revealing information or going on the record with specific facts. Sources depend on the confidence of journalists all through the reporting process, even if nothing they say is published.

This manner of confidential information sharing is exceedingly common. It is well documented that such disclosures are a "daily occurrence" among government sources.[1] Further, leaks are more common from more senior staff. Congress leaks, but senior officials in the Executive branch are the most frequent leakers of all.[2] This may seem surprising, but this gray area is useful to government, journalists,

[1] The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information. p. 12. David Pozen, Harvard Law Review, forthcoming. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2223703

[2] Pozen, pp. 13-14.

and the public alike. Legal scholar David Pozen discusses this state of affairs at great length, and provides this illuminating example:

> Consider the recent news stories about the CIA's drone program targeting suspected al Qaeda militants in Yemen. The very existence of this program is classified. Relying on information provided by unnamed U.S. officials, the stories explain the basic purpose and nature of the program, and several report that all operations have been conducted with the consent of the Yemeni government. Let us assume that the President or his delegees authorized these communications with the press, whether proactively or in response to prior disclosures or discoveries by others. By revealing this information, the Administration keeps the American people minimally informed of its pursuits, characterizes them in a manner designed to build support, and signals its respect for international law and sovereignty (the detail about the host state's consent). At the same time, by revealing this information through a plant, the Administration manages to avoid engaging in any unstructured public conversation about issues that might implicate intelligence sources and methods, or violating any pledges it might have made to Yemeni leaders not to officially reveal their role in the drone strikes, lest this cause them political trouble at home.[3]

This analysis demonstrates the nuances of information sharing between sources and the press. While this example involves hypothetical Presidential authority, journalists depend on unofficial channels to cover all levels of government and many controversial topics entirely outside of government, such as business and medicine.

Simply put: a free press cannot function if journalists are not able to make guarantees of confidence to their sources. Private communications and disclosures are routine, not exceptional. Indeed, the ability to speak candidly with unofficial sources is foundational to the concept of an independent press.

The necessity of protecting the confidentiality of journalist-source communications has long been recognized by all branches of government. As the comment from the New York State Bar Association *et al.* documents, reporters' communications are privileged by statute or court ruling in 49 states.[4] Congress is currently considering a comprehensive media shield law that would require a judge to approve subpoenas

---

[3] Pozen, p. 38.

[4] See the contemporaneous comment to the Review Group from the Media Law Committee of the New York State Bar Association and the Communications and Media Law Committee of the New York City Bar Association for detailed discussion and references.

of journalist-source communications.[5] And in July, the Department of Justice issued new guidelines concerning the news media.[6]

After it was revealed that the Department had secretly subpoenaed the calling records for 20 AP phone lines – including the main House of Representatives press gallery line -- media industry uproar prompted a fresh look at DOJ procedures around investigations involving the news media. The President asked the Attorney General to conduct a review, and the July guidelines represent the result of this review. Below we will consider these guidelines in some detail.

2. NSA Surveillance programs contradict Department of Justice standards

In this section we will show how the NSA's surveillance regime contradicts recent Department of Justice policy regarding the confidentiality of journalist-source communications.

We consider the policies in the July 12, 2013 Department of Justice Report on Review of News Media Policies because they are remarkably relevant. First, they are very recent. This report was issued five weeks after the Snowden documents began to come to light. Second, this review was prompted by the unilateral executive seizure of reporters' call records, exactly the type of domestic records collected *en masse* by the NSA. Therefore, this document represents the Administration's current thinking on precisely those contemporary surveillance issues that pose the most serious threat to a vigorous free press.

There is an obvious objection to comparing these Department of Justice policies to NSA surveillance programs: they exist in very different legal and operational regimes. The Department of Justice guidelines concern civil and criminal investigations while the NSA is charged with foreign intelligence acquisition. On the face of it, these activities are in separate spheres.

But this distinction evaporates when examined from the perspective of a source to wishes to communicate with a journalist in confidence. Because chilling effects are our primary concern, it is precisely this source point of view which matters here.

The Department of Justice report recognizes the seriousness of intrusion into the work of journalism and states the basic remedy in its second paragraph:

---

[5] "Media shield act moves on to the full Senate," Washington Post, September 12, 2013.
http://articles.washingtonpost.com/2013-09-12/world/41994597_1_media-shield-law-press-freedom-confidential-sources

[6] Department of Justice Report on Review of News Media Policies, July 12, 2013.
http://www.justice.gov/iso/opa/resources/2202013712162851796893.pdf

> in light of the importance of the constitutionally protected newsgathering process, the Department views the use of tools to seek evidence from or involving the news media as an extraordinary measure. The Department's policy is to utilize such tools only as a last resort, after all reasonable alternative investigative steps have been taken, and when the information sought is essential to a successful investigation or prosecution.[7]

In contrast, recent revelations show that NSA collects information on essentially *all* journalist-source communications *in advance.* The collection of the telephone metadata of every American is the starkest example of this pre-emptive domestic mass surveillance. A person's call records, going back years, is profoundly revealing, and becomes even more so when combined with the calling records of everyone else. [8]

But this is hardly the only issue. The NSA records vast quantities of internet traffic with at least one end outside the U.S., that is, Americans' communications with people in other countries.[9] It can search this intercepted content for specific keywords.[10] It routinely engages in social network analysis of American citizens.[11] And because of the secrecy surrounding intelligence activities, we cannot assume that there are no further hidden domestic interception programs.

As far as we can determine, the intelligence community affords no special status to the journalistic communications swept up in these programs. Far from being a last resort, collecting journalistic records is standard practice.

It is true that statute, the rulings of the Foreign Intelligence Surveillance Court, Executive Order 12333, related memoranda, and internal compliance policies place restrictions on what the NSA can do with the data it collects. This thicket is not very reassuring for the source who worries about sanctions or prosecution. For someone who feels they need to have a private conversation, the damage is already done. The NSA already has their information and individual analysts can look at it without

---

[7] DoJ report, p. 1

[8] "Here's how phone metadata can reveal your affairs, abortions, and other secrets." Washington Post, August 27, 2013. http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/27/heres-how-phone-metadata-can-reveal-your-affairs-abortions-and-other-secrets/

[9] "How the NSA is still harvesting your online data." The Guardian, June 27, 2013. http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection

[10] "NSA. Said to Search Content of Messages to and From U.S." New York Times, August 8, 2013. http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html

[11] "NSA Gathers Data on Social Connections of U.S. Citizens," New York Times, September 28, 2013. http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html

judicial approval in each case.[12] And this information may be retained for years or further disseminated, which means the risk of disclosure will never diminish.

Contrariwise, the Department of Justice requires a multi-step review process before seeking to acquire such records:

> the Department would revise current policy to elevate the current approval requirements and require the approval of the Attorney General for all search warrants and court orders issued pursuant to l8 U.S.C. § 2703(d) directed at members of the news media.[13]

and

> The Department will create a standing News Media Review Committee, akin to its Capital Case Review Committee and State Secrets Review Committee, to advise the Attorney General and Deputy Attorney General when Department attorneys request authorization to seek media-related records in investigations into the unauthorized disclosure of information; when Department attorneys request authorization to seek media-related records in any law enforcement investigation without providing prior notice to the relevant member of the media; and when Department attorneys request authorization to seek testimony from a member of the media that would disclose the identity of a confidential source.[14]

Further, the guidelines specifically presume that the journalist in question must be notified:

> Advance notice will afford members of the news media the opportunity to engage with the Department regarding the proposed use of investigative

---

[12] The issue of access is complex and involves law, policy, and actual capability, but all three allow access without individual judicial oversight. For the legal regime see e.g. "Reauthorization of FISA Amendments Act," Congressional Research Service, p. 4. http://www.fas.org/sgp/crs/intel/R42725.pdf. As a matter of policy, FISC requires only a "reasonable, articulable suspicion" before domestic telephone metadata can be queried, i.e. analysts do not have to go back to the court. FISC docket 13-80, p. 7. http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf. But neither law nor policy answer the question of who actually has access. The 12 documented instances of misuse of such authority, several of which occurred at overseas facilities, suggest that a fair number of people have *de facto* access to this information. NSA Inspector General Response to Senator Grassley, September 11, 2013. http://www.grassley.senate.gov/judiciary/upload/NSA-Surveillance-09-11-13-response-from-IG-to-intentional-misuse-of-NSA-authority.pdf

[13] DoJ report, Section I

[14] DoJ report, Section II

> tools to obtain communications or business records, and also provide the news media with the opportunity to challenge the government's use of such tools in federal court. By strengthening the presumption in favor of notice, and providing that notice be deferred only where the Attorney General, after a review by a committee of senior Department officials, finds that notice would present a clear and substantial threat to the investigation, grave harm to national security, or imminent risk of death or serious bodily harm, the Department's new policy reflects the gravity of the decision to forgo negotiations with, or delay notification to, affected members of the news media.[15]

We are not aware of any provision under the current regime for the NSA to notify a source or journalist before examining their phone records or other private material. Further, the NSA may retain and disseminate warrantless intercepted communications *even of Americans* if these materials contain "evidence of a crime."

This point is worth elaborating. The FISC approves so-called "minimization" procedures required under FISA section 702 that detail the procedures used to ensure that the "foreign intelligence surveillance" contemplated by FISA really is foreign. These minimization procedures govern the retention and use of information collected about Americans. The most recent publicly available minimization procedures order, from 2011, states that any domestic communication must be destroyed unless

> the communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such communication may be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with 50 U.S.C. l806(b) and l825(c), Executive Order No. 12333, and, where applicable, the crimes reporting procedures set out in the August l995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document.[16]

The two statutes mentioned in this section are brief and do not restrict the types of crimes that can be reported. That apparently falls to the 1995 MOU cited by the court, which specifically mentions many different types of crimes that may be reported by intelligence agencies to domestic federal law enforcement. These include "crimes involving intentional infliction or threat of death or serious physical harm," terrorism, and espionage, as one might expect. But the MOU also mentions

---

[15] DoJ report, Section III

[16] Minimization Procedures used by the NSA in Connection with Acquisitions of Foreign Intelligence Information. Section 5 (2). U.S. Foreign Intelligence Surveillance Court, October 31, 2011. http://www.dni.gov/files/documents/Minimization Procedures used by NSA in Connection with FISA SECT 702.pdf

many other types of crimes, including defrauding or bribing the government, perjury, counterfeiting, unauthorized computer access, drug offenses, money laundering, violations of environmental laws, and sanctions violations.[17]

In short, information originally collected through indiscriminate warrantless surveillance of an American journalist's American source can later be passed to federal law enforcement if it contains evidence of any of a large number of categories of crimes. Compare this to the exceptions for evidence of a crime in the Department of Justice procedures:

> (i) access to records will be limited to Department personnel who are working on the investigation and have a need to know the information; (ii) the records will be used solely in connection with the investigation and related judicial proceedings
>
> ...
>
> Under circumstances where the Deputy Attorney General finds that specific, identifiable records are evidence of a separate past or imminent crime involving (i) death; (ii) kidnapping; (iii) substantial bodily harm; (iv) conduct that constitutes a criminal offense that is a specified offense against a minor as defined in 42 U.S.C. § l69ll; or (v) incapacitation or destruction of critical infrastructure as defined in 42 U.S.C. § 5l95c(e), the Deputy Attorney General may authorize broader use of the information. [18]

This is a much narrower range of reportable offenses, which may be discovered only in the much narrower set of records already authorized in conjunction with a specific investigation.

The Department of Justice guidelines also dispense with the idea that personal data in the possession of third parties is not protected. The NSA and FISC make the converse argument, citing a 1979 Supreme Court decision holding that telephone dialing records are not protected because the caller disclosed the number to a third party.[19] The Department of Justice guidelines disagree:

> The Department will also make additional technical revisions to the Department's policies regarding news media subpoenas. Most significantly, to account for technological changes in news gathering, distribution, and publication, the Department's policies regarding the use of legal process to obtain information from, or records of, members of the news media will

---

[17] Memorandum of Understanding: Reporting of Information Concerning Federal Crimes. 1995, section VII. https://www.fas.org/irp/agency/doj/mou-crimes.pdf
[18] DoJ report, section VI
[19] FISC docket BR 13-109, Section II
http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf

> be revised to make clear that those policies apply to "communications records" or "business records" of members of the news media that are stored or maintained by third parties.[20]

We note that "business records" is precisely the language found in section 215 of the PATRIOT Act, which has been used to justify the mass seizure of phone records.

3. Mass surveillance raises issues beyond individual surveillance

Surveilling a number of individuals is hugely different in character from surveilling essentially everyone. The former is what law enforcement traditionally has done, while the latter is what the NSA is doing now.

FISC does not recognize this difference. *Smith v. Maryland*, decided by the Supreme Court in 1979, held that a single individual's calling records are not protected by the Fourth Amendment.[21] In its most recent ruling approving the collection of bulk call records FISC argued that this decision, when combined with various other precedent, implies that *all* individuals' calling records collected *en masse* are not protected:

> Put another way, where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*.[22]

We disagree in the strongest terms, for at least two reasons.

First, the surveillance of essentially everyone has effects far beyond the surveillance of journalists alone. This raises a new and hugely broader issue: the indiscriminate collection of information on the communications of *all possible sources.* In other words it is not enough to protect journalists. For a free press to function we must also protect the *means of communicating* with a journalist. At the present time, the NSA has made private electronic communication essentially impossible, at least in practical terms.

Second, the NSA is not simply investigating individuals one at a time, but simultaneously examining the relationships among many people.[23] Data on an entire society is vastly more than the sum of its parts. It is one thing to know who all of my contacts are. If you also know all of my contacts' contacts, social network

---

[20] DoJ report, section VII

[21] 442 U.S. 735 (1979)

[22] FISC docket BR 13-109, p. 9. http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf

[23] "NSA Gathers Data on Social Connections of U.S. Citizens," New York Times, September 28, 2013. http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html

analysis will reveal the deeper structure of my social groups, their communication patterns, and power structures.[24] Many other kinds of mass data analysis have been suggested for counter-terrorism application.[25]

These techniques draw on a fundamental concept from data mining: the detection of patterns across multiple records. Simultaneous analysis of many persons' records reveals an extraordinary amount that the isolated analysis of an individual's records does not. Indeed, the intelligence community would not bother with this kind of multiple-person analysis if it did not have the potential to yield valuable insights.

For these reasons, mass surveillance raises additional privacy issues that are of an entirely different and far more ominous character than those relating to individual surveillance. It will not be enough to implement intelligence law and policy parallel to current Department of Justice policy concerning journalist-source communications, because that policy has contemplated only the effects of *individual* surveillance. That policy does not speak to the blanket chilling effect of sources that we are beginning to see now.

4. Secret and confusing law

The source who wishes to communicate privately to a journalist faces very complex and confusing choices. Under the current regime it is unclear exactly how Americans are being monitored or what their legal rights may be.

We assert that citizens have the right to know under what conditions their private lives may be monitored, and how this information may be used against them. Specifically, citizens who do not know the bounds of surveillance cannot communicate confidently with journalists. But the public is currently in the dark for a variety of reasons.

First, much of the law is secret. The rulings of the Foreign Intelligence Surveillance Court are generally sealed, yet they contain key legal interpretations. For this reason we support proposals that require the Court to issue its opinions in redacted or summarized form.

Second, the law and procedure governing the acquisition, use, and sharing of surveillance information regarding U.S. citizens is fragmented and complex. It consists of a few statutes such as FISA and the PATRIOT Act, secret and now-public FISC rulings, and Executive instruments such as EO 12333 and the memoranda that implement it. Former assistant attorney general David Kris notes that "a good deal of foreign intelligence collection is regulated by the Fourth Amendment and

---

[24] See e.g. "Introduction to Social Network Methods," Hanneman and Riddle, 2005. http://faculty.ucr.edu/~hanneman/nettext/

[25] See e.g. "Knowledge Discovery for Counterterrorism and Law Enforcement," David Skillicorn, CRC Press, 2008

Executive Order 12333 and its subordinate procedures, but not in any meaningful way by statute."[26]

In particular, nowhere are the rules regarding sharing of (warrantless) surveillance information with domestic law enforcement agencies or criminal prosecutors clearly stated.

Taken together, mass surveillance plus secret and ambiguous laws give the appearance of an end run around Fourth Amendment privacy protections, particularly the Title III individualized warrant requirement. Whether or not this is true in fact in any particular case, the *appearance* will produce a chilling effect. There may *also* be systematic abuses, such as the DEA's "parallel construction" tactic which is currently under investigation by the Department of Justice.[27]

The result of all this secrecy and confusion has been predictable: sources have stopped talking to journalists.

5. Chilling Effects

Even before we began to learn the full extent of the NSA's mass surveillance activities, sources were wary of government intrusion into their communications. Responding to Department of Justice's secret seizure of Associated Press phone records, AP President Gary Pruitt spoke at the National Press Club in mid June:

> The actions of the DoJ against AP are already having an impact beyond the specifics of this particular case. Some of our longtime trusted sources have become nervous and anxious about talking to us, even on stories that aren't about national security. And in some cases, government employees that we once checked in with regularly will no longer speak to us by phone, and some are reluctant to meet in person.
>
> This chilling effect is not just at AP, it's happening at other news organizations as well. Journalists from other news organizations have personally told me it has intimidated sources from speaking to them.[28]

---

[26] "Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Approach," David Kris, May 20, 2103. http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-approach/

[27] "Justice Department reviewing DEA's shielding of sources." USA Today, August 5, 2013. http://www.usatoday.com/story/news/nation/2013/08/05/justice-dea-special-operations-shield/2620439/

[28] "AP Boss: sources won't talk anymore." Politico, June 19, 2013. http://www.politico.com/story/2013/06/ap-sources-93054.html

Imagine, then, the chilling effect of learning that the government has warrantless access to *all* calls made, not merely the calls through the 20 phone lines subpoenaed in this case. This is not a theoretical issue. We have already heard multiple reports from journalists that sources are refusing to speak, citing fears of surveillance.

In a forthcoming report of the Committee To Protect Journalists, former Washington Post executive editor Leonard Downie Jr. cites several journalists who have first-hand experience of these chilling effects.

> Numerous Washington-based journalists told me that officials are reluctant to discuss even unclassified information with them because they fear that leak investigations and government surveillance make it more difficult for reporters to protect them as sources. "I worry now about calling somebody because the contact can be found out through a check of phone records or e-mails," said veteran national security journalist R. Jeffrey Smith of the Center for Public Integrity, an influential nonprofit government accountability news organization in Washington. "It leaves a digital trail that makes it easier for the government to monitor those contacts," he said.
>
> "I think we have a real problem," said New York Times national security reporter Scott Shane. "Most people are deterred by those leaks prosecutions. They're scared to death. There's a gray zone between classified and unclassified information, and most sources were in that gray zone. Sources are now afraid to enter that gray zone. It's having a deterrent effect. If we consider aggressive press coverage of government activities being at the core of American democracy, this tips the balance heavily in favor of the government."[29]

There is no unilateral technical fix for communication security. Journalists can use encryption technologies such as PGP and OTR, but it is the sources who must encrypt. This requires sources to be both technically and operationally savvy, a high and unrealistic standard. Further, these tools do not provide anonymity, and the use of secure communications techniques can itself be revealing. We know that the NSA's XKeyScore system allows analysts to search specifically for encrypted communications.[30]

Despite all the advances in communications technology, it seems reporters will be forced to meet sources in parking garages as in days of old.

---

[29] The Obama Administration and the Press Leak investigations and surveillance in post-9/11 America. Committee to Project Journalists. Forthcoming.

[30] "NSA Targets Internet Users Who Search for 'Suspicious Stuff,' Newly Revealed Documents Show." Slate, July 31, 2013. http://www.slate.com/blogs/future_tense/2013/07/31/xkeyscore_nsa_targets_internet_users_who_search_for_suspicious_stuff.html

6. Recommendations

We do not pretend to know the full extent of the reforms that must be made. But we do understand the corrosive effects of the current secret mass surveillance regime on a free press. The government must take steps to rebuild confidence in the privacy of communications with journalists. We propose the following:

i) A principle of parity between intelligence and non-intelligence methods of obtaining journalist-source communications. We have reasonable assurances that the DoJ will not use its powers to interfere with the practice of journalism. We have no such assurances from the intelligence community.

Perhaps the most critical missing element is the regulation of intelligence sharing, especially with domestic law enforcement. It must not be possible to circumvent individual warrant requirements through intelligence methods, as it currently appears to be.

The nature of mass surveillance requires additional assurances. Just as it is not possible to get a Title III warrant to search *all* people, it should not be possible to apply broad searches or data mining to intercepted bulk material. It is essential that sources know that their communications cannot be invaded without *individual* judicial review.

We realize that the details of such reform will be complex. However we stand by the principle of parity as fundamental: there must be one set of rules, and those rules must protect journalist-source communications. Given the recent loss of public confidence, it is likely that these rules will not be credible if they are not enshrined in law.

ii) Clarity around the interception and storage of Americans' communications.

Our right of private communication cannot be ambiguous. Americans must know how their communications and data are being collected, and for what purposes. The recent voluntary declassifications and disclosures are a good step. Are there are other surveillance programs that might cause public uproar if they were widely understood? Such sensitivity is itself the best possible argument that these programs need to be publicly discussed.

Such a discussion cannot proceed without also addressing the issue of effectiveness. Are these programs effective and necessary to guarantee our safety? We have heard very little about the use of this private information for its putative purpose of counter-terrorism. General Alexander has stated that

these programs have stopped "over 50" plots.[31] However, this number has been questioned on the grounds that the only plots specifically discussed relied on individual surveillance, not mass surveillance[32,33] and a previous government accounting of foiled terrorist plots proved to be inflated.[34]

Ultimately, the government must clearly explain the current conditions under which information gleaned under surveillance of any kind can be used against someone, especially for administrative sanction or criminal prosecution – and provide legal remedy if these conditions are violated. This must include surveillance performed by the intelligence community.

The underlying principles here are clarity and credibility. The existing surveillance regime lacks both.

Mass surveillance is a serious threat to the constitutionally protected function of a free press, and therefore to democracy itself, because it impinges on the ability and confidence of *every possible source* who might talk to a journalist. We need clear, public law which protects ordinary citizens from unaccountable intrusions into their private communications, no matter how those communications were obtained. We need a full accounting of what has been done and what is being done, and why, and whether it is necessary and effective. We have heard many assurances from the government that there is no abuse; but we do not need assurances, we need rights.

---

[31] "N.S.A. Chief Says Surveillance Has Stopped Dozens of Plots." New York Times, June 18, 2013. http://www.nytimes.com/2013/06/19/us/politics/nsa-chief-says-surveillance-has-stopped-dozens-of-plots.html

[32] "Is NSA exaggerating its surveillance successes?" Christian Science Monitor, June 18, 2013. http://www.csmonitor.com/USA/DC-Decoder/2013/0618/Is-NSA-exaggerating-its-surveillance-successes

[33] "Defenders of NSA Surveillance Omit Most of Mumbai Plotter's Story." ProPublica, June 12, 2013. http://www.propublica.org/article/defenders-of-nsa-surveillance-web-omit-most-of-mumbai-plotters-story

[34] "Fact-Check: How the NYPD Overstated Its Counterterrorism Record." ProPublica, July 10, 2012.

Signed,

Emily Bell
Director
Tow Center for Digital Journalism
Columbia University Graduate School of Journalism

Ethan Zuckerman
Director
Center for Civic Media
Massachusetts Institute of Technology Media Lab

Jonathan Stray
Fellow in Computational Journalism
Tow Center for Digital Journalism
Columbia University Graduate School of Journalism

Shelia Coronel
Director
Toni Stabile Center for Investigative Journalism
Columbia University Graduate School of Journalism

Michael Schudson
Professor
Columbia University Graduate School of Journalism