International Journal of Communication 11(2017), 802-823 1932–8036/20170005

The Snowden Disclosures, Technical Standards, and the Making of Surveillance Infrastructures

MICHAEL ROGERS
Briar Project, UK

GRACE EDEN
University of Applied Sciences Western Switzerland HES-SO, Switzerland

The Snowden documents have revealed that intelligence agencies conduct large-scale digital surveillance by exploiting vulnerabilities in the hardware and software of communication infrastructures. These vulnerabilities have been characterized as "weaknesses," "flaws," "bugs," and "backdoors." Some of these result from errors in the design or implementation of systems, others from unanticipated uses of intended features. A particularly subtle kind of vulnerability arises from the manipulation of technical standards to render communication infrastructures susceptible to surveillance. Technical standards have a powerful influence on our digital environment: They shape the conditions under which digital citizenship is exercised. The Snowden revelations brought to the forefront the role of intelligence agencies in the standards-making process, lending new urgency to the debate over the adequacy and legitimacy of the current mechanisms used for negotiating standards. This article explores how influence is exercised in the production of standards and the implications this has for their trustworthiness and integrity.

Keywords: Snowden, standards, infrastructure, surveillance

In this article, we discuss the results of an exploratory study based on interviews conducted in 2015, two years after the Snowden disclosures, to understand how the Snowden documents have influenced attitudes to surveillance and privacy within certain standards organizations and associated institutions. We examine the social processes that produce technical standards, the role of standards in enabling or hindering surveillance, and the involvement of intelligence agencies in the negotiation and agreement of standards. Our aim is to bring to the attention of a communication studies audience a recent political turn in certain standards bodies, which is only the latest development in a long history of contention over the social and political effects of technical standards for communication infrastructures.

We begin by describing the role of technical standards within digital infrastructures and the general characteristics of the standards-making process, framed as a practice of negotiation and

Michael Rogers: Michael@briarproject.org
Grace Eden: grace.eden@hevs.ch
Date submitted: 2016–02–29

agreement. We then examine how intelligence agencies participate in standards making, the tensions such participation produces, and its implications for the trustworthiness and integrity of standards. Following this, we discuss the ways in which standards bodies and related institutions have responded to the Snowden disclosures, with a particular focus on organizations affected by the efforts of the U.S. National Security Agency (NSA) to influence and subvert technical standards, as revealed by the Snowden documents. Finally, we close with an exploration of possibilities for mitigating the influence of intelligence agencies on the standards-making process.

The Role of Standards

Standards can be defined as agreed characteristics that facilitate compatibility across products and processes within a particular domain (Nadvi & Wältring, 2004). Within the ICT domain, the organizations responsible for developing standards are a diverse collection of government institutions, nongovernmental organizations, industry consortia, academic institutions, professional associations, and loosely organized groups of individuals. Within each standards-making organization, working groups attempt to reach agreement on common solutions to technical challenges (Weiss & Cargill, 1992). When a standard is agreed on, it is specified in documents that establish uniform technical criteria, methods, processes, and practices.

Standards not only facilitate the technical coordination of geographically distributed systems, they also serve a political function. Coordinating transnational stakeholders in a process of negotiation and agreement through the development of common rules is a form of global governance (Nadvi, 2008). The resulting standards become normative documents that define the material conditions for global digital communication. Since there is no global government, global governance has been described as "an instance of governance in the absence of government" (Ruggie, 2014, p. 5). Standards are among the mechanisms by which this governance is achieved. Conformance to certain standards is often a basic condition of participation in international trade and communication, so there are strong economic and political incentives to conform, even in the absence of legal requirements (Russell, 2014). The American National Standards Institute (ANSI, 2010) describes this situation succinctly:

> Emerging economies understand that standards are synonymous with development and request standards-related technical assistance programs from donor countries. Increasingly our trading partners utilize such programs to influence the selection of standards by these economies and create favorable trade alliances. (p. 5)

Negotiation, Consensus, and Complexity

Standards are created through a diverse range of social processes. Russell (2014) distinguishes among de facto standards, which arise from common usage; de jure standards, which are mandated by law; and voluntary consensus standards, which are developed through a process of negotiation among certain interested parties. Participation in this process and adoption of the resulting standards are voluntary, which should be understood to mean an absence of legal requirements rather than an absence of economic or political pressures.

Camp and Vincent (2005) describe four models used to develop ICT standards, each of which has its own processes of negotiation and acceptance. The government model is a state-controlled process; the consortium model consists of members, usually corporations, who must pay a fee to participate; the professional association model includes members who share the same skills, knowledge, and practices; and the open model allows any individual to participate, with mechanisms for appointing members to coordination and oversight roles.

Each of these models has different degrees of transparency, accountability, and inclusiveness, but all involve a process of negotiation and consensus building through which participants in working groups exert their influence to reach agreement on specifications that reflect their specific interests (Weiss & Cargill, 1992). When standards are adopted voluntarily, once they are agreed on, consensus is vital to ensure their widespread implementation. During this process, participants with greater market power hold similarly greater influence over working groups. Weiss and Cargill (1992) note that negotiations within voluntary consortia are unequal interactions because of this influence based on market share, while Diffie and Landau (1998) observe that the purchasing power of governments can cause standards developed for government use to become de facto commercial standards.

As unequal participants compete to define standards, technological compromises emerge, which add complexity to standards. For instance, when working group participants propose competing solutions, it may be easier for them to agree on a standard that combines all the proposals rather than choosing any single proposal. This shifts the responsibility for selecting a solution onto those who implement the standard, which can lead to complex implementations that may not be interoperable. On its face this appears to be a failure of the standardization process, but this outcome may benefit certain participants—for example, by allowing an implementer with large market share to establish a de facto standard within the scope of the documented standard.

The voluntary consensus approach to standards making became the norm in the field of computer networking between the 1970s and 1990s, accompanied by an "ideology of open standards" (Russell, 2014, p. 21) that linked the open standards-making process with the ideals of participatory democracy, open markets, individual autonomy, and social progress. Telecommunications standards, in contrast, remain dominated by the International Telecommunications Union and associated organizations with strong historical links to national governments.

Standards have been framed as public goods because they can be made available for anyone to use (Kindleberger, 1983). However, this conceptualization has been challenged by pointing to situations in which private consortia prioritize corporate over public interests; a limited range of actors are involved in standardization; license fees are charged for using standards; and standards organizations are accountable only to their members (Bunduchi, Williams, & Graham, 2004). These and other social traces embedded in the standards-making process ultimately manifest in the features and functionality incorporated in products and services. In the ICT domain, these traces affect how citizens' privacy and security are safeguarded or endangered in their everyday use of digital tools.

Empirical Study Methodology

For this research, we wanted to understand how issues of surveillance and privacy were negotiated within certain standards organizations and associated institutions, using the Snowden revelations as a focus for our inquiry. To achieve this, we conducted a semistructured interview study in which we discussed the role of standards in enabling or hindering surveillance; the relationship between standards organizations and intelligence agencies; individual and organizational attitudes to surveillance and privacy; and the effect, if any, of the Snowden leaks on these attitudes.

Data from eight interviews are included in this article. The interview subjects were participants in 11 standards-making bodies and associated institutions. Each of these organizations is involved in developing and coordinating the technical systems that make up the global communication infrastructure.[1] Six of the organizations are concerned with developing standards; one with certifying implementations; one with governance of infrastructure; and three with technical research. A brief overview of each organization is given in Table 1. It is important to note that there is cross-fertilization among these groups, with many participants attending working groups in multiple organizations. We focused on organizations whose work is relevant to the surveillance of communication, and especially organizations affected by the NSA's attempts to influence and subvert technical standards, as revealed by the Snowden documents. This places the United States at the center of our inquiry, as the documented instances of subversion affected both U.S. and global standards bodies, as we will describe.

Interviews were audio recorded and lasted between 60 and 90 minutes.[2] The audio was transcribed and analyzed using qualitative methods informed by thematic analysis (Guest, MacQueen, & Namey, 2012), with which themes are identified and coded across interviews. Through the identification of themes, concepts, practices, and activities, we analyzed the interview data to understand the ways in which the Snowden revelations have impacted these organizations.

We present findings from this study and discuss the implications for technological infrastructure and digital citizenship. Our findings are divided into four sections. First, we discuss how the characteristics of the standards-making process affect the susceptibility of technological infrastructures to surveillance. Next, we examine intelligence agency participation in standards making and the ways in which agencies influence technical standards. We then describe responses to the Snowden revelations that each interviewee has seen within the organizations in which he or she participates. Finally, we discuss possible ways to mitigate the influence of intelligence agencies on standards organizations.

1 A useful graphic that summarizes this ecology is available at https://www.icann.org/news/multimedia/78
2 One of the interviewees declined to be recorded.

Table 1. Organizations in Which Interviewees Participated.

Name of organization		Role	Structure	Scope
ETSI	European Telecommunications Standards Institute	Standards development	Nonprofit organization	Europe
GCF	Global Certification Forum	Standards compliance	Industry partnership	Global
IACR	International Association for Cryptologic Research	Professional association	Nonprofit organization	Global
ICANN	Internet Corporation for Assigned Names and Numbers	Infrastructure governance	Nonprofit organization	Global
IEEE	Institute of Electrical and Electronic Engineers	Standards development, professional association	Nonprofit organization	Global
IETF	Internet Engineering Task Force	Standards development	Individual participants	Global
IRTF	Internet Research Task Force	Research	Individual participants	Global
ISO	International Organization for Standardization	Standards development	Nongovernmental organization	Global
LMS	London Mathematical Society	Professional association	Nonprofit organization	UK
NIST	National Institute for Standards and Technology	Standards development	Government institution	U.S.
W3C	World Wide Web Consortium	Standards development	Industry consortium	Global

Consensus Standards, Complexity, and Surveillance

We described how complexity emerges in the standards-making process and why it is a key characteristic of voluntary consensus standards, arising from negotiation between participants with competing interests who need to reach technological compromises. Such an arrangement has specific effects with regard to surveillance, as described by two of our interviewees.

> Large companies want complex standards because it makes it harder for competitors to enter the market, but, of course, large complex standards are also good for the NSA because it means that nobody can actually implement them securely. So even if the standards themselves are secure, the implementations will not be. (ETSI, IACR, ISO, and NIST participant)

> I think there are people who actively push within the IETF to make sure that every standard has a dozen different options. . . . IPsec [Internet Protocol Security[3]] is a classic example of something that really should have been widely adopted a long time ago and was not . . . because everybody implemented a different set of the options and so they didn't interoperate very well, and the complexity I think really killed the hopes of broad adoption. I don't know whether that was a deliberate attempt to kill it by overloading it with features or whether that was actually people who were like, but my version really is better and it needs to be folded in too. (IETF and IRTF participant)

Whether complexity arises unintentionally as a by-product of negotiation, or is intentionally fostered by certain participants to advance their own interests, it can increase the susceptibility of communication systems to surveillance. For example, a standard that is implemented inaccurately or incompletely may be vulnerable to exploitation, whereas a standard with many incompatible implementations may not achieve wide adoption, which, in the case of cryptographic standards, would leave communication unprotected.

Intelligence Agency Participation in Standards Making

The Snowden files reveal intelligence agency interest in manipulating the standards-making process. According to documents leaked by Snowden, the NSA seeks to "influence policies, standards and specifications for commercial public key technologies"[4] (Perlroth, Larson, & Shane, 2013, para. 32). The agency "actively engages the U.S. and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make these systems exploitable through SIGINT [signals intelligence] collection" (Ball, Borger, & Greenwald, 2013, para. 18).

Leaked documents describe a specific instance of this manipulation: an NSA-engineered "backdoor"[5] in a 2006 cryptographic standard, which experts have identified as the Dual Elliptic Curve Deterministic Random Bit Generator, or Dual EC DRBG (Bernstein, Lange, & Niederhagen, 2015). The flawed algorithm was standardized by ANSI, and subsequently by NIST and ISO, and was implemented in Internet hardware and dozens of software libraries (Bernstein et al., 2015; Goodin, 2016). The backdoor allows the NSA to guess cryptographic keys used by devices that implement the standard, and thus to decrypt their communications.

The NSA's involvement in standards making is not in itself news: the agency has a dual responsibility for conducting foreign surveillance and securing domestic information systems, and its employees openly participate in standards bodies, ostensibly to serve the latter role. However, the Snowden documents confirm a longstanding suspicion that the NSA sometimes uses its information security mission as cover to advance its surveillance mission by subverting technical standards.

---

3 Internet Protocol Security is an encrypted and authenticated form of the Internet Protocol.

4 *Public key technologies* refers to a form of cryptography.

5 In cryptography, a *backdoor* is a vulnerability that can only be exploited by certain parties.

The NSA has participated in standards development since the first civilian encryption standards were published in the 1970s (Banisar & Schneier, 1999). Throughout the 1980s, the agency vied with the National Bureau of Standards (later NIST) for control of civilian cryptographic standards, with a 1989 memorandum of understanding between the two agencies giving the NSA an effective veto over NIST's work (Diffie & Landau, 1998).

In the early 1990s, the NSA allied its national security arguments with the law enforcement arguments of the Federal Bureau of Investigation (FBI) to promote policies and standards favorable to surveillance. The 1994 Communications Assistance for Law Enforcement Act required telephone companies to adopt standardized interfaces for "lawful intercept" surveillance; the law did not mandate a particular standard, but required industry to develop and implement one. Lawful intercept interfaces were built into equipment sold around the world, providing other governments with de facto wiretapping capabilities equivalent to those defined by U.S. law. The lawful intercept features in exported telecoms equipment were also exploited by the NSA for intelligence purposes (Bamford, 2015; Devereaux, Greenwald, & Poitras, 2014).

> For GSM and 3G, they provided lawful intercept interfaces, but of course we know from the Greek case in 2010[6] that actually one of those interfaces has been used by a third party, and we still don't know who this third party is—it could be organized crime, it could be another nation. (ETSI, IACR, ISO, and NIST participant)

> If you look at the quoted case about the Bahamas network,[7] it was exactly that lawful interception interface that apparently was abused [by the NSA] in order to take a full take on all the mobile calls in the Bahamas for a month or two. (IETF participant)

Historically, the NSA's overt influence on technical standards reached its peak in the 1990s, with Clipper, a proposed NIST standard for secure telephony using a secret NSA encryption algorithm. Clipper included a "key escrow" feature allowing calls to be decrypted for surveillance purposes. The proposal attracted widespread criticism on technical and political grounds, and was an embarrassing failure for the NSA and FBI. After legal restrictions on the export of cryptographic software were overturned in 1996, it appeared that the NSA's effort to control civilian cryptography was at an end. NIST organized a widely praised public competition to select a new Advanced Encryption Standard (AES), establishing its trustworthiness as a developer of robust and independent standards.

> Twenty years ago, NIST proposed an escrow standard . . . [which] was not good for their international reputation and to build trust into NIST because, of course, the keys would be held by the U.S. Government and not by any other government. But I think by organizing the AES competition in the late nineties, and more recently the SHA-3 competition, NIST has built up quite some credibility in having open standards and advocating strong security for everybody. (ETSI, IACR, ISO, and NIST participant)

---

6 Bamford (2015) argues that the third party was the NSA.

7 See Devereaux et al. (2014).

However, because of the Snowden disclosures, we now know that the NSA continued to use its relationship with NIST to influence cryptographic standards, exploiting the trust that NIST had earned. The NSA proposed Dual EC DRBG to ANSI, ISO, and NIST in parallel, using the ANSI standardization effort to argue for the algorithm's adoption by the other bodies. Documents released under the Freedom of Information Act show that NIST cryptographers did not fully understand the algorithm they were being asked to standardize and relied on the NSA's advice.[8]

The existence of a potential backdoor in Dual EC DRBG was recognized by participants in the ANSI working group as early as 2005 and was publicly revealed by academic cryptographers in 2007 (Bernstein et al., 2015). Even so, NIST did not revise its standard or openly investigate the issue until after the Snowden revelations, when it commissioned a study into how its internal processes has been manipulated (Cerf et al., 2014).

> It's kind of amazing how bold [the NSA was] because, in fact, they were caught and NIST didn't do anything. But, in 2007, they were caught in public, and so it shows how bold they are, that they actually dared to undermine public standards in the open view of everybody. (ETSI, IACR, ISO, and NIST participant)

> I do think that that particular NIST revelation did have a large impact on the standards groups that I follow, that the IETF was already talking about Snowden, but talked about it much more urgently . . . . after this NIST piece because it was actually subversion of a standards-setting organization and there was some remote possibility of that in W3C. (IETF and W3C participant)

There is also evidence that the NSA made several attempts to subvert an IETF standard. Between 2006 and 2010, four extensions were proposed to the Transport Layer Security protocol used to encrypt Web and e-mail traffic. Adoption of any of the extensions would have made exploitation of the Dual EC DRBG backdoor much easier (Checkoway et al., 2014). Three of the proposals were co-authored by NSA employees. Although none of the proposals became IETF standards, one was implemented in a software library sold by RSA Security.[9] Documents leaked by Snowden reveal that the NSA paid RSA $10 million to use Dual EC DRBG in the same library (Menn, 2013).

The subversion of two separate technical standards produced by different organizations, combined with a commercial contract to ensure the use of both subverted standards in a software library sold to third parties, demonstrates the sophistication of the NSA's strategy. Every stage of the process—from the initial proposal, through negotiation and consensus, to implementation and adoption—was influenced to produce the desired result: encryption products that were flawed in such a way as to enable decryption by the NSA.

---

8 See https://github.com/matthewdgreen/nistfoia and Cerf et al. (2014).

9 In software, a *library* is a component that can be reused in many different products.

The potential for standards to be subverted or compromised during the negotiation process has led to disagreement about whether intelligence agency employees should be allowed to participate in working groups. Having an employee of an intelligence agency in a leadership role is particularly controversial because these roles include extra responsibilities, such as consensus building, which can sway outcomes within the decision-making process.

> The NSA people come to the ISO meetings, they participate to the IETF, they are even vice chairs of working groups, and so on. . . . and I think, in many cases, they participate there to improve security and to make sure that everything works well. But given what we learned about the BULLRUN program,[10] they also do it to actually make sure that things do not go well and actually some bad things happen. Of course, it's very hard in a complex world to decide in specific cases whether the intentions of these agencies are good or bad for any specific claim they make or any specific thing they do. (ETSI, IACR, ISO, and NIST participant)

It is clear that the intentions and methods of intelligence agencies remain problematic for the standards-making process. Yet there is no simple solution: even if intelligence agencies were excluded from direct participation, they could participate covertly via proxies or front organizations. The NSA works with numerous external contractors who could be tasked with participating on its behalf.

> I think if you would [exclude intelligence agencies from participation], then they would actually start acting through third parties. They would start a company or they would bribe somebody in a company or use somebody in a company and then you wouldn't know. So I think in some sense it's fine to have them participate. I understand the reservations of people if they take a more active role and whether we should let them be the chair or vice chair is another question. (ETSI, IACR, ISO, and NIST participant)

It might be argued, however, that the NSA's reputation for cryptographic expertise, its responsibility for securing domestic information systems, and its access to secret information lend authority to its arguments in working groups and allow it to propose features for which no public justification can be given. This appears to have been the case with Dual EC DRBG, where NIST's cryptographers deferred to the expertise of their NSA colleagues. Had the NSA been forced to hide its participation behind a third party, its contributions might have been subject to more critical scrutiny. We return to the issue of mitigating covert influence on standards making in the final section of the article.

Responses to the Snowden Revelations

The worldwide response to the Snowden disclosures has been enormous. Both the multifaceted nature of the attacks and their scale came as a shock to many technical experts, activists, journalists, and citizens. What had in the past been treated as hypotheticals were now documented facts. In this section

10 An NSA program revealed by Snowden that uses undisclosed techniques to defeat encryption.

we highlight how participants in standards organizations and related institutions have responded to the revelations.

Internet Engineering Task Force

The IETF has a long history of engaging with surveillance issues. In 1996, the organization's steering group published a statement supporting access to strong cryptography "for all Internet users in all countries," (IAB and IESG, 1996, p. 2) and in May 2000 the IETF declared that it would not develop standards for wiretapping.[11]

The first Snowden files were released in June 2013, and the following month a side meeting was organized at an IETF conference in Berlin to discuss the implications of the NSA's XKEYSCORE program. The result was the creation of a mailing list, *perpass* (short for *pervasive passive surveillance*),[12] in which IETF participants had a forum to discuss the ways in which this and other surveillance programs could be countered. The fruits of these discussions included the formation of new working groups to develop solutions for expanding encryption capabilities across the Internet.[13]

In November 2013, the IETF hosted a discussion of the implications of the Snowden leaks at a conference plenary in Vancouver.[14] The meeting attracted over one thousand participants who discussed surveillance, its relationship to technical infrastructure, and how the IETF should respond. It culminated in an agreement that led to the publication of *Pervasive Monitoring Is an Attack* in May 2014.[15] This is a "process" rather than a "technical" document, and thus has an impact on every strand of work the IETF does, including the development and revision of standards. Working groups must now consider pervasive monitoring alongside other security properties and provide guidance for how such attacks could be mitigated.

> The IETF has consensus on the fact that we should be mitigating this attack. We should be putting in place the technical mitigations that we know exist that can affect this and make the attack harder. They may not make it impossible but they can make it much more costly or make it very hard and we should do that. (IETF participant)

> A long time participant in the IETF . . . had a great way of expressing it. He said, "Listen, we've spent 20 years optimizing for bandwidth and for speed and it's time that we also started optimizing for privacy." . . . So now there is a growing awareness that this actually is one of the priorities and it's a priority that needs to be put on par with the traditional priorities of speed and cost. (IETF and IRTF participant)

---

11 https://tools.ietf.org/html/rfc2804

12 https://mailarchive.ietf.org/arch/search/?email_list=perpass

13 https://datatracker.ietf.org/wg/dprive/charter and https://datatracker.ietf.org/wg/tcpinc/charter

14 https://www.youtube.com/watch?v=oV71hhEpQ20

15 https://tools.ietf.org/html/rfc7258

More recently, the IETF published *Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement*[16]—an informational document that examines changing threat models as a result of the Snowden revelations.

> Whereas previously we would have assumed in our threat models that the attacker would try to be kind of parsimonious and attack the cheapest or the weakest link in the chain, these guys go for every link. . . . So we have to consider the threat model slightly differently and we have a bunch of people working on that. (IETF participant)

Technical standards specifically designed to hinder mass surveillance are also in development, using an approach called *opportunistic security*, in which encryption is automatically enabled whenever it is available.[17] It remains to be seen how complex these standards will be, and whether or not they will be widely adopted by industry.

In one sense, the IETF response to the Snowden revelations has been robust, reacting quickly and opening up channels of communication for its participants to discuss the issue though meetings, plenary sessions, and mailing lists. But the response has largely treated surveillance as a technical problem—one that is external to the IETF itself. The response to possible subversion of the IETF standards-making process has been less strong.

In 2013, following the Snowden revelations, an IETF and IRTF participant requested that an NSA employee be removed as cochair of the Crypto Forum Research Group (CFRG), an IRTF group that provides cryptographic advice on IETF standards.[18]

> We had a big fuss last year because one of the cochairs of CFRG was an NSA employee, but actually that's okay. I defended him to the death because if we start firing people because of who pays their salary, we're screwed. And as far as I know, he's a genuine guy who's doing the right things. He has since retired from NSA, and from being cochair of the group. But there was a big fuss on the CFRG mailing list about a year and a half ago. (IETF participant)

This quote is interesting on two levels. First, it expresses a particular view of how working groups operate, and second, it suggests that this view is a norm that must be upheld: Participants should not be judged by their affiliations, but by whether they are "a genuine guy." This reflects the official position of the IETF that individuals participate on their own behalf, rather than as representatives of organizations. However, when organizations are known to be paying individuals to influence and in some cases subvert standards, we must ask whether this view of working group dynamics remains tenable.

16 https://tools.ietf.org/html/rfc7624

17 https://tools.ietf.org/html/rfc7435

18 https://www.ietf.org/mail-archive/web/cfrg/current/msg03554.html

One of our interviewees strongly criticized the response of the IETF and IRTF to the issue of intelligence agency involvement in working groups, and no longer takes part in either organization as a result.[19] The interviewee argued that the IETF's governance mechanisms had been appropriate when it was a small group of people who knew and trusted each other, and whose goals were aligned with those of the military research establishment that developed the early Internet. However, as the organization grew, it had continued to rely on the same core group of individuals to steer it while regarding itself as an open, transparent, and nonhierarchical organization. This left the IETF unable to address the question of whether its core participants could be trusted.

Freeman (1972) argues that all social groups contain informal structures of this kind, but groups that perceive themselves as "structureless" cannot recognize, and therefore challenge, their informal structures. While the IETF has some formal rules and structures, it describes itself as a "loosely self-organized group of people" (Hoffman, 2012, Section 2, para. 1) and emphasizes "rough consensus" (Clark, 1992, p. 543) and "personal judgment" (Hoffman, 2012, Section A.3, para. 1) as its governing principles.[20] It is perhaps significant that the issue of an NSA employee cochairing a working group was settled informally.

Internet Research Task Force

The IRTF investigates key research themes that may contribute to the development of future IETF standards. Because of this, there is crossover between participants in these organizations. The IRTF has recently formed the Human Rights Protocol Considerations Research Group (HRPC),[21] which is developing a glossary document that maps technical terms to human rights terms with the aim of linking concepts across these two domains. The group has also developed a methodology document that provides guidance for how to analyze the corpus of Internet standards produced by the IETF within a human rights context.

> At the IETF meetings, we have HRPC meetings and when they were first proposed, my biggest fear was that they were just going to be like yes, you can have a room, go off and do your thing and everyone can ignore you now. . . . But in practice, what's actually happened is that a lot of people have come to it and said we want to talk about this. We want to build this discussion. So, in some ways, whether the documents end up being concretely useful or not, having a place to have the discussion I think has raised the awareness of the issue within the IETF and is helping to build consensus around the idea that these things are related. (IETF and IRTF participant)

Although the creation of the HRPC was not a direct response to the Snowden revelations, the disclosures have increased interest in the group. Connecting human rights activists and standards

19 This interviewee did not wish to be directly quoted.

20 See Clark (1992) and https://www.ietf.org/tao.html, para. 257

21 https://irtf.org/hrpc

developers holds great promise in beginning to frame technical standards in terms of their social impacts and consequences. In future, the IETF may even embed this work directly into standards development.

The IRTF has also made efforts to decrease its historic reliance on NIST for cryptographic advice by inviting academic cryptographers to participate in the IRTF to create an alternative pool of expertise.

London Mathematical Society

The close relationship between other academic communities and intelligence agencies has caused similar concern, as was raised in the interviews.

> It just began with reading the newspapers, and when the Snowden revelations first came out, I was very interested and read about them, and then, quite slowly in fact, it dawned on me that the mathematical community was actually somehow involved in these things, because GCHQ [Government Communications Headquarters[22]] and the NSA have always employed a lot of mathematicians. (LMS participant)

After this, the interviewee started to engage the UK mathematical community's professional association, the London Mathematical Society (LMS), in a dialogue about the issue.

> For a start, very nearly every mathematician I've discussed this with has similar opinions to me. They are extremely uncomfortable with what we now know that GCHQ and the NSA are doing. That's at the level of individuals. I think institutions respond in a much different way because there's this illusion that it's possible for an institution to be neutral. Let's say you're head of a university department and some opportunity comes up to collaborate with GCHQ, you might like to imagine that you're just a neutral conduit of information and you pass that information on to your department. (LMS participant)

This disconnection between the technical details of research and its potential social impact exists not only in the mathematical community but also within the larger ICT research community, where a kind of cognitive dissonance occurs in which the actions of researchers are not associated with the resultant consequences (Eden, Jirotka, & Stahl, 2014). The debate continues within the LMS.

International Association for Cryptologic Research

Another professional association, the International Association for Cryptologic Research (IACR), has responded to the Snowden disclosures with the release of the Copenhagen Declaration,[23] which states that the association's members reject the compromise of cryptographic standards and that research should be undertaken to protect personal privacy against governmental and corporate overreach. However, members of the IACR who work for intelligence agencies did not engage in the debate that led

22 Government Communications Headquarters is the UK's signals intelligence agency.

23 https://www.iacr.org/misc/statement-May2014.html

to the declaration. An interviewee told us that whenever there are discussions about surveillance issues, these members sit in silence, which can lead to tensions within the community.

Internet Corporation for Assigned Names and Numbers

The Snowden revelations have brought into focus issues of Internet governance, with a renewed effort to move beyond ICANN's historic operational control by the U.S. government (Bradshaw et al., 2015; Gibbs, 2013). A full discussion of Internet governance post-Snowden is beyond the scope of this article, but one interviewee highlighted ICANN's data retention agreement, instituted in 2013, as especially contentious in light of the Snowden disclosures. The agreement concerns access to information about the owners of domain names. At issue is ICANN's request that registrars hold their customers' personal data in escrow for 18 months. The data are escrowed with Iron Mountain, a U.S. defense contractor.

> The whole point of that escrow requirement, nominally it's to protect users just in case your registrar turns out to be a fly-by-night. . . . So they need some data, but the kind of level of data they're asking these guys to retain is much more of a surveillance measure than it is reasonable. (ICANN and IEEE participant)

The European Data Protection Supervisor wrote to ICANN expressing concern over the data escrow requirements, noting that the practice was illegal in the European Union. The issue remains unresolved.

> In terms of what the attitude is or was, remembering that the Internet came out of DARPA [U.S. Defense Advanced Research Projects Agency] and there's still a huge U.S. military interest in it, I think there is kind of *sous-entendu*, an understanding that surveillance is part of the U.S.'s interest in this stuff, but nobody talks about it. It's not really talked about at ICANN. (ICANN and IEEE participant)

Since our interviews took place, ICANN has formed a working group to consider whether the existing policies for managing information about domain name owners should be replaced.[24]

Institute of Electrical and Electronic Engineers

The availability of information about domain name owners will affect a growing number of people with the rise of Internet-connected consumer devices—the so-called Internet of things. When one of our interviewees raised this issue in an IEEE working group, the concerns were dismissed in the session, but privately acknowledged by several participants. This illustrates how concerns about the social effects of technical decisions can be excluded from working group discussions unless an effort is made to include them explicitly within the working group's remit.

---

24 http://whois.icann.org/sites/default/files/files/final-issue-report-next-generation-rds-07oct15-en.pdf

Global Certification Forum

The GCF certifies implementations of mobile communication standards produced by the 3rd Generation Partnership Project (3GPP). Within this certification organization, the Snowden revelations have not been discussed.

> I wonder a little bit myself because it's not openly discussed. . . . But I think the level of awareness or willingness to have a look and say this is what has happened since Snowden—that has to have an impact on us, let's tighten up our security testing or something, [but] I don't see that happening yet on a grand scale. . . . So I don't think it has changed much so far at least. (GCF participant)

Because mobile communications standards fall within the telecommunications domain, where designing systems to support "lawful intercept" surveillance is an industry norm, there is limited scope for developing systems that protect against surveillance.

> 3GPP consists of network manufacturers and network operators who are bound by the laws of governments, and laws of nations that require lawful intercept. So even if they wanted to develop something like end-to-end encryption, they can certainly do that but then governments would not allow end-to-end encryption in networks to be used because then that would break their lawful intercept. (GCF participant)

Requirements for lawful intercept access have not been challenged by the telecommunications industry despite the abuse of these capabilities revealed by Snowden. At the time of writing, the 3GPP is in the process of standardizing an encrypted telephony protocol developed by GCHQ. Like the Clipper proposal from the 1990s, the protocol enables calls to be decrypted for surveillance purposes (Murdoch, 2016).

World Wide Web Consortium

The W3C does not have a stated policy on surveillance or privacy, but a number of W3C standards explicitly address privacy issues (Doty, 2015), and the organization's director has been an outspoken critic of NSA surveillance (Warr, 2013).

The Snowden revelations had an impact on the already-established Tracking Protection working group,[25] which aims to increase individuals' privacy and control when browsing websites. The group's Do Not Track standard focuses on enabling the expression of privacy preferences, thus making it possible to block or accept tracking elements in Web browsing sessions. The Do Not Track discussions began in 2011, and the Snowden revelations have affected the group's work. Interestingly, the working group lost participation because the civil society organizations involved wanted to focus their resources on the implications of the Snowden disclosures, and many left the group to do so.

25 https://www.w3.org/2011/tracking-protection

Although Do Not Track would eventually protect consumers, it would be a voluntary implementation on the part of advertisers and other companies that track website visitors. Many browsers have a Do Not Track option available, but this merely asks websites not to track visitors who enable the option. Whether the request is honored or not is up to the companies who do the tracking. This example demonstrates the effects of market influence and voluntarism: without voluntary adoption of this standard by advertisers, which would go against their commercial interests, the standard is ineffective. Only if the standard were to become a legal requirement could privacy advocates ensure that it would function in all circumstances. We may conclude from this that when the technical features of the Internet and World Wide Web have a direct impact on citizen privacy and security, the voluntary approach to standards negotiation and adoption may not be adequate for addressing the concerns of wider society.

National Institute of Standards and Technology

When evidence of a backdoor in Dual EC DRBG was published in September 2013, NIST released a statement saying that it "would not deliberately weaken a cryptographic standard" (NIST, 2013, para. 2). However, in the same statement it reminded the public that "NIST is required by statute to consult with the NSA" (NIST, 2013, para. 4). NIST subsequently invited a committee of external experts to investigate how the flawed standard came to be published despite the recognized possibility of a backdoor (Cerf et al., 2014). The Snowden revelations were cited in several of the committee members' individual reports as being the catalyst for the NIST review.

The committee recommended that NIST review its relationship with the NSA and request changes from the U.S. government as necessary to ensure its independence. The memorandum of understanding between the two agencies is currently under review, but no statutory changes have been proposed (NIST, 2015). Another recommendation was that NIST should increase its cryptographic expertise and seek advice from outside experts to reduce its dependence on the NSA.

> I think, in general, the people of NIST were quite shocked by this, and they tried to get their act together and build again trust in the community, but I think it's going to be a long-term process. And, of course, the fact remains that NSA has hundreds and hundreds of cryptographers and has access to literature from decades old, and they collaborate also with other agencies and, of course, NIST has maybe a handful of cryptographers and even if they double this to 10 or 15, they still will be, in terms of expertise and track record, running behind in some areas. (ETSI, IACR, ISO, and NIST participant)

In response to the committee's findings, NIST increased its annual budget for cryptographic work by $6 million (NIST, 2015). The NSA program for subverting cryptographic standards and implementations has an annual budget of more than $250 million (Perlroth et al., 2013).

The NIST standard describing Dual EC DRBG was finally revised in June 2015 to remove the flawed algorithm, 10 years after participants in the ANSI working group first recognized the possibility of a

backdoor. An implementation of the standard in hardware sold by Juniper Networks was withdrawn in January 2016 after the backdoor was found to have been taken over by an unknown party (Goodin, 2016).

Mitigating the Influence of Intelligence Agencies

The Snowden revelations have drawn renewed attention to the role of intelligence agencies in the standards-making process, and cast doubt on the adequacy of current mechanisms for ensuring the integrity and trustworthiness of standards. Our interviewees described various measures that standards bodies are exploring that might help to mitigate this influence.

Open and Transparent Processes

The concepts of openness and transparency are accepted by some participants in standards bodies as sufficient protection against intelligence agency influence. An open standards-making process is one in which anyone can participate, all documents related to the negotiation process are published, and the standard itself is publicly available. Proponents of the open model argue that since everyone is aware that participants may seek to further their own interests, attempts to influence decision making can be recognized and countered.

> The way we work is just open, and if we're open, that means we don't fire people because they change affiliation or because of a given affiliation. We look at their arguments and we look at what their output is, examine it as the best we can and that's the only defense we have. (IETF participant)

> The main way to defend against that is openness and transparency . . . to have more people who have the right politics involved and engaged and getting into these arguments, going forward and saying, I hear that you want to propose this particular way to solve this problem, but it's going to cause these other issues down the line and it's going to leave us open to these other concerns and we really need to stop it. (IETF and IRTF participant)

One of our interviewees drew an analogy between intelligence agency subversion of standards and attempts by companies to insert patented technologies into standards to charge license fees later, a practice known as *submarining*:

> We've had to deal with patents for decades, and from the point of view of the standards process, subverting it for national government purposes on the quiet is kind of like trying to do a submarine, get your patent into the standard. . . . We do everything in the open and so therefore everybody just needs to examine what's being suggested and think about who is the person suggesting it and they might be suspicious of that and if they are, they themselves will go off and do more examination. (IETF participant)

A question left unanswered by these descriptions of ideal transparent processes is who specifically is responsible for critically examining the contributions of working group participants. If the IETF's claim that participants are not representatives of organizations is accepted, then no participant has a special responsibility to perform such scrutiny—unless it is the working group chairs, whose own affiliations are excluded from consideration. This seems a weak position from which to resist deliberate subversion of standards.

Competitions

Other interviewees argued for a different kind of open process: public competitions, in which entrants submit proposals to meet a published set of criteria, the proposals are evaluated in public by a panel of judges, and the winning proposal is standardized. By selecting a single winner, this model can avoid the complexity that arises when trying to reconcile competing proposals. NIST has used this model to develop some of its cryptographic standards, and because of the transparency of the process, these standards have remained trusted even after the Dual EC DRBG revelations.

> We have in crypto something which is I think pretty unique. You can compare it a bit to the Olympic Games for cryptographers. So if NIST wants a specific standard in an area, they actually invite everybody to submit their candidates . . . there is a four-year-long competition and in the end, NIST selects a winner. So they also have to motivate why they select certain algorithms. So I think this is actually the best way to develop standards because it's open and transparent, and also NIST enforces to submitters that if their algorithm is selected, it will be available for free to everybody. (ETSI, IACR, ISO, and NIST participant)

The NIST Committee of Visitors report (Cerf et al., 2014) recommends that NIST host more open cryptographic competitions that engage academics and industry worldwide in the peer-reviewed selection of standards. It is worth bearing in mind, however, that the trust NIST earned in the past through its use of competitions might have contributed to the acceptance of Dual EC DRBG, which was developed using a less transparent process. For competitions to be fully effective in mitigating the subversion of standards, they should be clearly distinguished from standards developed by other means.

Although competitions have been successful in cryptography, they may not be suitable for all fields. They require criteria that can be agreed on in advance by all entrants, as well as the possibility for less powerful participants to produce entries of comparable quality to their dominant rivals. Where these conditions are not met, some participants may prefer an unequal negotiation process rather than a winner-takes-all contest.

Explicit Inclusion of Political Concerns in Standards

The IRTF's Human Rights Protocol Considerations research group is making a fundamental response to the issue of intelligence agency influence on standards, as well as other technological threats to individual rights, by exploring whether human rights can be explicitly recognized as criteria that

technical standards must meet. A draft standard under development by the group contains "a proposal for guidelines for human rights considerations, similar to the work done on the guidelines for privacy considerations" (ten Oever & Cath, 2016, p. 1) that is already part of the IETF standards process.

The ongoing struggle over Internet governance suggests, however, that the inclusion of political concerns in the process is not by itself sufficient to ensure that those concerns are addressed. Continued participation in the standards-making process by civil society groups will also be needed to ensure that human rights remain an active focus of debate rather than receiving only superficial acknowledgment. At the time of this writing, neither the open process favored by the IETF and IRTF nor the more restricted models used by ISO, ETSI, and others makes any provision for ensuring this kind of participation.

Conclusion

The Snowden revelations have profound implications for the design of communication infrastructures, in which the technical issues cannot be separated from questions of commercial and political influence, global governance, and human rights. Various actors intervene in the standards-making process for various purposes, and disentangling the links between these actors, their objectives, and the technical capabilities codified in a standard can be extraordinarily difficult. Thankfully, there is growing recognition of these issues within the standards-making community. This is reflected in the work of the IRTF on translating human rights considerations into criteria for standards development; in the debate within the IETF over intelligence agency participation in working groups; and in the NIST Committee of Visitors's recommendations for the development of a more independent and transparent process. On the other hand, in the telecommunications industry we see little debate over these issues and a continued acceptance of surveillance as an industry norm.

In each of these cases, the adequacy of current processes for developing standards has been cast into doubt. We ask the question: What if standards for digital communication were developed and defined within legal frameworks as they are in other domains such as food, building, and product safety? What if technical standards were legally required to include elements in their specifications that defend and uphold the principles of human rights, security, and privacy? When government agencies are willing to exploit the social vulnerabilities found in institutional processes just as readily as the technical vulnerabilities found in software and hardware, these questions become increasingly urgent.

References

ANSI (American National Standards Institute). (2010). *United States standards strategy*. New York, NY: Author.

Ball, J., Borger, J., & Greenwald, G. (2013, September 6). Revealed: How US and UK spy agencies defeat Internet privacy and security. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

Bamford, J. (2015, September 29). A death in Athens: Did a rogue NSA operation cause the death of a Greek telecom employee? *The Intercept*. Retrieved from https://theintercept.com/2015/09/28/death-athens-rogue-nsa-operation

Banisar, D., & Schneier, B. (1999). *The electronic privacy papers: Documents on the battle for privacy in the age of surveillance*. New York, NY: Wiley.

Bernstein, D. J., Lange, T., & Niederhagen, R. (2015). Dual EC: A standardized back door. *IACR Cryptology ePrint Archive*. Retrieved from http://eprint.iacr.org/2015/767

Bradshaw, S., DeNardis, L., Hampson, F. O., Jardine, E., & Raymond, M. (2015). The emergence of contention in global Internet governance. *Global Commission on Internet Governance* (Paper series, 17). Waterloo, Canada: Centre for International Governance Innovation.

Bunduchi, R., Williams, R., & Graham, I. (2004, August 25). *Between public and private—the nature of today's standards*. Workshop on Standards, Democracy and the Public Interest, Paris, France.

Camp, L. J., & Vincent, C. (2005). Looking to the Internet for models of governance. *Ethics and Information Technology*, *6*(3), 161–173. doi:10.1007/s10676-004-3250-3

Cerf, V., Felten, E., Lipner, S., Preneel, B., Richey, E., Rivest, R., & Schrotter, F. (2014). *NIST cryptographic standards and guidelines development process: Report and recommendations of the Visiting Committee on Advanced Technology of the National Institute of Standards and Technology*. Gaithersburg, MD: National Institute of Standards and Technology.

Checkoway, S., Niederhagen, R., Everspaugh, A., Green, M., Lange, T., Ristenpart, T., . . . Fredrikson, M. (2014, August). On the practical exploitability of Dual EC in TLS implementations. *23rd USENIX Security Symposium (USENIX Security 14),* 319–335. San Diego, CA: USENIX Association.

Clark, D. (1992). A cloudy crystal ball—visions of the future. *Proceedings of the 24th Internet Engineering Task Force*, 539–543. IETF. Retrieved from https://www.ietf.org/proceedings/24.pdf

Devereaux, R., Greenwald, G., & Poitras, L. (2014, May 19). Data pirates of the Caribbean: The NSA is recording every cell phone call in the Bahamas. *The Intercept*. Retrieved from https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas

Diffie, W., & Landau, S. (1998). *Privacy on the line: The politics of wiretapping and encryption*. Cambridge, MA: MIT Press.

Doty, N. (2015, May 21). *Reviewing for privacy in Internet and Web standard-setting*. Paper presented at the International Workshop on Privacy Engineering, San Jose, CA.

Eden, G., Jirotka, M., & Stahl, B. (2014). *Responsible research and innovation in ICT: Summary of key issues, recommendations, challenges and enablers* (EPSRC Technical Report). Retrieved from https://drive.switch.ch/index.php/s/e2huVHGb3h9mCc1

Freeman, J. (1972). The tyranny of structurelessness. *Berkeley Journal of Sociology*, *17*(1972–73), 151–165.

Gibbs, S. (2013, November 21). ICANN chief: Shift away from US "is the way forward." *The Guardian*. Retrieved from https://www.theguardian.com/technology/2013/nov/21/icann-internet-governance-solution-us-nsa-brazil-argentina

Goodin, D. (2016, January 10). Juniper drops NSA-developed code following new backdoor revelations. *Ars Technica*. Retrieved from http://arstechnica.co.uk/security/2016/01/juniper-drops-nsa-developed-code-following-new-backdoor-revelations

Guest, G., MacQueen, K. M., & Namey, E. (2012). *Applied thematic analysis*. Thousand Oaks, CA: SAGE Publications.

Hoffman, P. (Ed.). (2012). The tao of IETF: A novice's guide to the Internet Engineering Task Force. IETF. Retrieved from https://www.ietf.org/tao.html

IAB (Internet Architecture Board) and IESG (Internet Engineering Steering Group). (1996). IAB and IESG statement on cryptographic technology and the Internet. IETF. Retrieved from https://tools.ietf.org/html/bcp200

Kindleberger, C. P. (1983). Standards as public, collective, and private goods. *Kyklos*, *36*, 377–397.

Menn, J. (2013, December 20). Exclusive: Secret contract tied NSA and security industry pioneer. *Reuters*. Retrieved from http://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220

Murdoch, S. J. (2016). Insecure by design: Protocols for encrypted phone calls. *IEEE Computer Magazine*, *49*(3), 25–33.

Nadvi, K. (2008). Global standards, global governance and the organisation of global value chains. *Journal of Economic Geography*, *8*, 323–343.

Nadvi, K., & Wältring, F. (2004). Making sense of global standards. In H. Schmitz (Ed.), *Local enterprises in the global economy* (pp. 53–94). Cheltenham, UK: Edward Elgar.

NIST (National Institute of Standards and Technology). (2013). Cryptographic standards statement. Retrieved from http://www.nist.gov/director/cybersecuritystatement-091013.cfm

NIST (National Institute of Standards and Technology). (2015). *NIST cryptographic standards and guidelines: A report to the NIST Visiting Committee on Advanced Technology regarding recommendations to improve NIST's approach*. Gaithersburg, MD: Author.

Perlroth, N., Larson, J., & Shane, S. (2013, September 5). N.S.A. able to foil basic safeguards of privacy on Web. *The New York Times*. Retrieved from http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html

Ruggie, J. G. (2014). Global governance and "new governance theory": Lessons from business and human rights. *Global Governance*, *20*, 5–17.

Russell, A. M. (2014). *Open standards and the digital age: History, ideology, and networks*. Cambridge, UK: Cambridge University Press.

ten Oever, N., & Cath, C. (2016, August 27). Research into human rights protocol considerations, draft-tenoever-hrpc-research-05. Retrieved from https://www.ietf.org/archive/id/draft-tenoever-hrpc-research-05.txt

Warr, P. (2013, June 10). Tim Berners-Lee calls NSA surveillance an "intrusion on basic human rights." *Wired*. Retrieved from http://www.wired.co.uk/article/berners-lee-nsa-prism

Weiss, M., & Cargill, C. (1992). Consortia in the standards development process. *Journal of the American Society for Information Science*, *43*(8), 559–565.