Stream: Independent Submission
RFC: 9446
Category: Informational
Published: July 2023
ISSN: 2070-1721
Authors: S. Farrell
Trinity College, Dublin
F. Badii
Digital Medusa
B. Schneier
Harvard University
S. M. Bellovin
Columbia University

RFC 9446
Reflections on Ten Years Past the Snowden Revelations

Abstract

This memo contains the thoughts and recountings of events that transpired during and after the release of information about the United States National Security Agency (NSA) by Edward Snowden in 2013. There are four perspectives: that of someone who was involved with sifting through the information to responsibly inform the public, that of a security area director of the IETF, that of a human rights expert, and that of a computer science and affiliate law professor. The purpose of this memo is to provide some historical perspective, while at the same time offering a view as to what security and privacy challenges the technical community should consider. These essays do not represent a consensus view, but that of the individual authors.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9446.

Copyright Notice

Table of Contents

1. Introduction

On June 6th, 2013, an article appeared in *The Guardian* [Guard2013] that was the beginning of a series of what have come to be known as the Snowden revelations, describing certain activities of the United States National Security Agency (NSA). These activities included, amongst others: secret court orders; secret agreements for the receipt of so-called "meta-information" that includes source, destination, and timing of communications; and tapping of communications lines. The breathtaking scope of the operations shocked the Internet technical community and resulted in a sea change within the IETF, IAB, and other standards organizations.

Now that some years have passed, it seems appropriate to reflect on that period of time and to consider what effect the community's actions had, where security has improved, how the threat surface has evolved, what areas haven't improved, and where the community might invest future efforts.

Bruce Schneier begins this compendium of individual essays by bringing us back to 2013, recalling how it was for him and others to report what was happening, and the mindset of those involved. Next, Stephen Farrell reviews the technical community's reactions and in particular the reactions of the IETF community, technical advances, and where threats remain. Then Farzaneh Badii discusses the impact of those advances -- or lack thereof -- on human rights. Finally Steven M. Bellovin puts the Snowden revelations into an ever-evolving historical context of secrets and secret stealing that spans centuries, closing with some suggestions for IETF.

Readers are invited to consider what impact we as a community have had, what challenges remain, and what positive contribution the technical community can and should make to address security and privacy of citizens of the world.

-- Eliot Lear, Independent Submissions Editor for the RFC Series

2. Bruce Schneier: Snowden Ten Years Later

In 2013 and 2014, I wrote extensively about new revelations regarding NSA surveillance based on the documents provided by Edward Snowden. But I had a more personal involvement as well.

I wrote the essay below in September 2013. *The New Yorker* agreed to publish it, but *The Guardian* asked me not to. It was scared of UK law enforcement and worried that this essay would reflect badly on it. And given that the UK police would raid its offices in July 2014, it had legitimate cause to be worried.

Now, ten years later, I offer this as a time capsule of what those early months of Snowden were like.

> It's a surreal experience, paging through hundreds of top-secret NSA documents. You're peering into a forbidden world: strange, confusing, and fascinating all at the same time.
>
> I had flown down to Rio de Janeiro in late August at the request of Glenn Greenwald. He had been working on the Edward Snowden archive for a couple of months, and had a pile of more technical documents that he wanted help interpreting. According to Greenwald, Snowden also thought that bringing me down was a good idea.
>
> It made sense. I didn't know either of them, but I have been writing about cryptography, security, and privacy for decades. I could decipher some of the technical language that Greenwald had difficulty with, and understand the context and importance of various document. And I have long been publicly critical of the NSA's eavesdropping capabilities. My knowledge and expertise could help figure out which stories needed to be reported.

I thought about it a lot before agreeing. This was before David Miranda, Greenwald's partner, was detained at Heathrow airport by the UK authorities; but even without that, I knew there was a risk. I fly a lot -- a quarter of a million miles per year -- and being put on a TSA list, or being detained at the US border and having my electronics confiscated, would be a major problem. So would the FBI breaking into my home and seizing my personal electronics. But in the end, that made me more determined to do it.

I did spend some time on the phone with the attorneys recommended to me by the ACLU and the EFF. And I talked about it with my partner, especially when Miranda was detained three days before my departure. Both Greenwald and his employer, *The Guardian*, are careful about whom they show the documents to. They publish only those portions essential to getting the story out. It was important to them that I be a co-author, not a source. I didn't follow the legal reasoning, but the point is that *The Guardian* doesn't want to leak the documents to random people. It will, however, write stories in the public interest, and I would be allowed to review the documents as part of that process. So after a Skype conversation with someone at *The Guardian*, I signed a letter of engagement.

And then I flew to Brazil.

I saw only a tiny slice of the documents, and most of what I saw was surprisingly banal. The concerns of the top-secret world are largely tactical: system upgrades, operational problems owing to weather, delays because of work backlogs, and so on. I paged through weekly reports, presentation slides from status meetings, and general briefings to educate visitors. Management is management, even inside the NSA. Reading the documents, I felt as though I were sitting through some of those endless meetings.

The meeting presenters try to spice things up. Presentations regularly include intelligence success stories. There were details -- what had been found, and how, and where it helped -- and sometimes there were attaboys from "customers" who used the intelligence. I'm sure these are intended to remind NSA employees that they're doing good. It definitely had an effect on me. Those were all things I want the NSA to be doing.

There were so many code names. Everything has one: every program, every piece of equipment, every piece of software. Sometimes code names had their own code names. The biggest secrets seem to be the underlying real-world information: which particular company MONEYROCKET is; what software vulnerability EGOTISTICALGIRAFFE -- really, I am not making that one up -- is; how TURBINE works. Those secrets collectively have a code name -- ECI, for exceptionally compartmented information -- and almost never appear in the documents. Chatting with Snowden on an encrypted IM connection, I joked that the NSA cafeteria menu probably has code names for menu items. His response: "Trust me when I say you have no idea."

Those code names all come with logos, most of them amateurish and a lot of them dumb. Note to the NSA: take some of that more than ten-billion-dollar annual budget and hire yourself a design firm. Really; it'll pay off in morale.

> Once in a while, though, I would see something that made me stop, stand up, and pace around in circles. It wasn't that what I read was particularly exciting, or important. It was just that it was startling. It changed -- ever so slightly -- how I thought about the world.
>
> Greenwald said that that reaction was normal when people started reading through the documents.
>
> Intelligence professionals talk about how disorienting it is living on the inside. You read so much classified information about the world's geopolitical events that you start seeing the world differently. You become convinced that only the insiders know what's really going on, because the news media is so often wrong. Your family is ignorant. Your friends are ignorant. The world is ignorant. The only thing keeping you from ignorance is that constant stream of classified knowledge. It's hard not to feel superior, not to say things like "If you only knew what we know" all the time. I can understand how General Keith Alexander, the director of the NSA, comes across as so supercilious; I only saw a minute fraction of that secret world, and I started feeling it.
>
> It turned out to be a terrible week to visit Greenwald, as he was still dealing with the fallout from Miranda's detention. Two other journalists, one from *The Nation* and the other from *The Hindu*, were also in town working with him. A lot of my week involved Greenwald rushing into my hotel room, giving me a thumb drive of new stuff to look through, and rushing out again.
>
> A technician from *The Guardian* got a search capability working while I was there, and I spent some time with it. Question: when you're given the capability to search through a database of NSA secrets, what's the first thing you look for? Answer: your name.
>
> It wasn't there. Neither were any of the algorithm names I knew, not even algorithms I knew that the US government used.
>
> I tried to talk to Greenwald about his own operational security. It had been incredibly stupid for Miranda to be traveling with NSA documents on the thumb drive. Transferring files electronically is what encryption is for. I told Greenwald that he and Laura Poitras should be sending large encrypted files of dummy documents back and forth every day.
>
> Once, at Greenwald's home, I walked into the backyard and looked for TEMPEST receivers hiding in the trees. I didn't find any, but that doesn't mean they weren't there. Greenwald has a lot of dogs, but I don't think that would hinder professionals. I'm sure that a bunch of major governments have a complete copy of everything Greenwald has. Maybe the black bag teams bumped into each other in those early weeks.
>
> I started doubting my own security procedures. Reading about the NSA's hacking abilities will do that to you. Can it break the encryption on my hard drive? Probably not. Has the company that makes my encryption software deliberately weakened the implementation for it? Probably. Are NSA agents listening in on my calls back to the US? Very probably. Could agents take control of my computer over the Internet if they

wanted to? Definitely. In the end, I decided to do my best and stop worrying about it. It was the agency's documents, after all. And what I was working on would become public in a few weeks.

I wasn't sleeping well, either. A lot of it was the sheer magnitude of what I saw. It's not that any of it was a real surprise. Those of us in the information security community had long assumed that the NSA was doing things like this. But we never really sat down and figured out the details, and to have the details confirmed made a big difference. Maybe I can make it clearer with an analogy. Everyone knows that death is inevitable; there's absolutely no surprise about that. Yet it arrives as a surprise, because we spend most of our lives refusing to think about it. The NSA documents were a bit like that. Knowing that it is surely true that the NSA is eavesdropping on the world, and doing it in such a methodical and robust manner, is very different from coming face-to-face with the reality that it is and the details of how it is doing it.

I also found it incredibly difficult to keep the secrets. *The Guardian*'s process is slow and methodical. I move much faster. I drafted stories based on what I found. Then I wrote essays about those stories, and essays about the essays. Writing was therapy; I would wake up in the wee hours of the morning, and write an essay. But that put me at least three levels beyond what was published.

Now that my involvement is out, and my first essays are out, I feel a lot better. I'm sure it will get worse again when I find another monumental revelation; there are still more documents to go through.

I've heard it said that Snowden wants to damage America. I can say with certainty that he does not. So far, everyone involved in this incident has been incredibly careful about what is released to the public. There are many documents that could be immensely harmful to the US, and no one has any intention of releasing them. The documents the reporters release are carefully redacted. Greenwald and I repeatedly debated with *The Guardian* editors the newsworthiness of story ideas, stressing that we would not expose government secrets simply because they're interesting.

The NSA got incredibly lucky; this could have ended with a massive public dump like Chelsea Manning's State Department cables. I suppose it still could. Despite that, I can imagine how this feels to the NSA. It's used to keeping this stuff behind multiple levels of security: gates with alarms, armed guards, safe doors, and military-grade cryptography. It's not supposed to be on a bunch of thumb drives in Brazil, Germany, the UK, the US, and who knows where else, protected largely by some random people's opinions about what should or should not remain secret. This is easily the greatest intelligence failure in the history of ever. It's amazing that one person could have had so much access with so little accountability, and could sneak all of this data out without raising any alarms. The odds are close to zero that Snowden is the first person to do this; he's just the first person to make public that he did. It's a testament to General Alexander's power that he hasn't been forced to resign.

> It's not that we weren't being careful about security, it's that our standards of care are so different. From the NSA's point of view, we're all major security risks, myself included. I was taking notes about classified material, crumpling them up, and throwing them into the wastebasket. I was printing documents marked "TOP SECRET/COMINT/NOFORN" in a hotel lobby. And once, I took the wrong thumb drive with me to dinner, accidentally leaving the unencrypted one filled with top-secret documents in my hotel room. It was an honest mistake; they were both blue.
>
> If I were an NSA employee, the policy would be to fire me for that alone.
>
> Many have written about how being under constant surveillance changes a person. When you know you're being watched, you censor yourself. You become less open, less spontaneous. You look at what you write on your computer and dwell on what you've said on the telephone, wonder how it would sound taken out of context, from the perspective of a hypothetical observer. You're more likely to conform. You suppress your individuality. Even though I have worked in privacy for decades, and already knew a lot about the NSA and what it does, the change was palpable. That feeling hasn't faded. I am now more careful about what I say and write. I am less trusting of communications technology. I am less trusting of the computer industry.
>
> After much discussion, Greenwald and I agreed to write three stories together to start. All of those are still in progress. In addition, I wrote two commentaries on the Snowden documents that were recently made public. There's a lot more to come; even Greenwald hasn't looked through everything.
>
> Since my trip to Brazil (one month before), I've flown back to the US once and domestically seven times -- all without incident. I'm not on any list yet. At least, none that I know about.

As it happened, I didn't write much more with Greenwald or *The Guardian*. Those two had a falling out, and by the time everything settled and both began writing about the documents independently -- Greenwald at the newly formed website *The Intercept* -- I got cut out of the process somehow. I remember hearing that Greenwald was annoyed with me, but I never learned the reason. We haven't spoken since.

Still, I was happy with the one story I was part of: how the NSA hacks Tor. I consider it a personal success that I pushed *The Guardian* to publish NSA documents detailing QUANTUM. I don't think that would have gotten out any other way. And I still use those pages today when I teach cybersecurity to policymakers at the Harvard Kennedy School.

Other people wrote about the Snowden files, and wrote a lot. It was a slow trickle at first, and then a more consistent flow. Between Greenwald, Bart Gellman, and *The Guardian* reporters, there ended up being steady stream of news. (Bart brought in Ashkan Soltani to help him with the technical aspects, which was a great move on his part, even if it cost Ashkan a government job later.) More stories were covered by other publications.

It started getting weird. Both Greenwald and Gellman held documents back so they could publish them in their books. Jake Appelbaum, who had not yet been accused of sexual assault by multiple women, was working with Poitras. He partnered with *Der Spiegel* to release an implant catalog from the NSA's Tailored Access Operations group. To this day, I am convinced that the document was not in the Snowden archives: that Jake got it somehow, and it was released with the implication that it was from Edward Snowden. I thought it was important enough that I started writing about each item in that document in my blog: "NSA Exploit of the Week." That got my website blocked by the DoD: I keep a framed print of the censor's message on my wall.

Perhaps the most surreal document disclosures were when artists started writing fiction based on the documents. This was in 2016, when Laura Poitras built a secure room in New York to house the documents. By then, the documents were years out of date. And now they're over a decade out of date. (They were leaked in 2013, but most of them were from 2012 or before.)

I ended up being something of a public ambassador for the documents. When I got back from Rio, I gave talks at a private conference in Woods Hole, the Berkman Center at Harvard, something called the Congress on Privacy and Surveillance in Geneva, events at both CATO and New America in DC, an event at the University of Pennsylvania, an event at EPIC, a "Stop Watching Us" rally in DC, the RISCS conference in London, the ISF in Paris, and...then...at the IETF meeting in Vancouver in November 2013. (I remember little of this; I am reconstructing it all from my calendar.)

What struck me at the IETF was the indignation in the room, and the calls to action. And there was action, across many fronts. We technologists did a lot to help secure the Internet, for example.

The government didn't do its part, though. Despite the public outcry, investigations by Congress, pronouncements by President Obama, and federal court rulings, I don't think much has changed. The NSA canceled a program here and a program there, and it is now more public about defense. But I don't think it is any less aggressive about either bulk or targeted surveillance. Certainly its government authorities haven't been restricted in any way. And surveillance capitalism is still the business model of the Internet.

And Edward Snowden? We were in contact for a while on Signal. I visited him once in Moscow, in 2016. And I had him do a guest lecture to my class at Harvard for a few years, remotely by Jitsi. Afterwards, I would hold a session where I promised to answer every question he would evade or not answer, explain every response he did give, and be candid in a way that someone with an outstanding arrest warrant simply cannot. Sometimes I thought I could channel Snowden better than he could.

But now it's been a decade. Everything he knows is old and out of date. Everything we know is old and out of date. The NSA suffered an even worse leak of its secrets by the Russians, under the guise of the Shadow Brokers, in 2016 and 2017. The NSA has rebuilt. It again has capabilities we can only surmise.

3. Stephen Farrell: IETF and Internet Technical Community Reaction

In 2013, the IETF and, more broadly, the Internet technical, security, and privacy research communities, were surprised by the surveillance and attack efforts exposed by the Snowden revelations [Timeline]. While the potential for such was known, it was the scale and pervasiveness of the activities disclosed that was alarming and, I think it fair to say, quite annoying, for very many Internet engineers.

As for the IETF's reaction, informal meetings during the July 2013 IETF meeting in Berlin indicated that IETF participants considered that these revelations showed that we needed to do more to improve the security and privacy properties of IETF protocols, and to help ensure deployments made better use of the security and privacy mechanisms that already existed. In August, the IETF set up a new mailing list [Perpass], which became a useful venue for triaging proposals for work on these topics. At the November 2013 IETF meeting, there was a lively and very well attended plenary session [Plenary-video] on "hardening the Internet" against such attacks, followed by a "birds of a feather" session [Perpass-BoF] devoted to more detailed discussion of possible actions in terms of new working groups, protocols, and Best Current Practice (BCP) documents that could help improve matters. This was followed in February/March 2014 by a joint IAB/W3C workshop on "strengthening the Internet against pervasive monitoring" [STRINT] held in London and attended by 150 engineers (still the only IAB workshop in my experience where we needed a waiting list for people after capacity for the venue was reached!). The STRINT workshop report was eventually published as [RFC7687] in 2015, but in the meantime, work proceeded on a BCP document codifying that the IETF community considered that "pervasive monitoring is an attack" [RFC7258] (aka BCP 188). The IETF Last Call discussion for that short document included more than 1000 emails -- while there was broad agreement on the overall message, a number of IETF participants considered enshrining that message in the RFC Series and IETF processes controversial. In any case, the BCP was published in May 2014. The key statement on which rough consensus was reached is in the abstract of RFC 7258 and says "Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible." That document has since been referenced [Refs-to-7258] by many IETF working groups and RFCs as justifying additional work on security and privacy. Throughout that period and beyond, the repercussions of the Snowden revelations remained a major and ongoing agenda item for both of the IETF's main technical management bodies, the IAB and the IESG (on which I served at the time).

So far, I've only described the processes with which the IETF dealt with the attacks, but there was, of course, also much technical work started by IETF participants that was at least partly motivated by the Snowden revelations.

In November 2013, a working group was established to document better practices for using TLS in applications [UTA] so that deployments would be less at risk in the face of some of the attacks related to stripping TLS or having applications misuse TLS APIs or parameters. Similar work was done later to update recommendations for use of cryptography in other protocols in the CURDLE

Working Group [CURDLE]. The CURDLE Working Group was, to an extent, created to enable use of a set of new elliptic curves that had been documented by the IRTF Crypto Forum Research Group [CFRG]. That work in turn had been partly motivated by (perhaps ultimately unfounded) concerns about elliptic curves defined in NIST standards, following the DUAL_EC_DRBG debacle [Dual-EC] (described further below) where a NIST random number generator had been deliberately engineered to produce output that could be vulnerable to NSA attack.

Work to develop a new version of TLS was started in 2014, mainly due to concerns that TLS 1.2 and earlier version implementations had been shown to be vulnerable to a range of attacks over the years. The work to develop TLS 1.3 [RFC8446] also aimed to encrypt more of the handshake so as to expose less information to network observers -- a fairly direct result of the Snowden revelations. Work to further improve TLS in this respect continues today using the so-called Encrypted Client Hello (ECH) mechanism [TLS-ECH] to remove one of the last privacy leaks present in current TLS.

Work on ECH was enabled by significant developments to encrypt DNS traffic, using DNS over TLS (DoT) [RFC7858] or DNS Queries over HTTPS (DoH) [RFC8484], which also started as a result of the Snowden revelations. Prior to that, privacy hadn't really been considered when it came to DNS data or (more importantly) the act of accessing DNS data. The trend towards encrypting DNS traffic represents a significant change for the Internet, both in terms of reducing cleartext, but also in terms of moving points-of-control. The latter aspect was, and remains, controversial, but the IETF did its job of defining new protocols that can enable better DNS privacy. Work on HTTP version 2 [RFC9113] and QUIC [RFC9000] further demonstrates the trend in the IETF towards always encrypting protocols as the new norm, at least at and above the transport layer.

Of course, not all such initiatives bore fruit; for example, attempts to define a new MPLS encryption mechanism [MPLS-OPPORTUNISTIC-ENCRYPT] foundered due to a lack of interest and the existence of the already deployed IEEE Media Access Control Security (MACsec) scheme. But there has been a fairly clear trend towards trying to remove cleartext from the Internet as a precursor to provide improved privacy when considering network observers as attackers.

The IETF, of course, forms only one part of the broader Internet technical community, and there were many non-IETF activities triggered by the Snowden revelations, a number of which also eventually resulted in new IETF work to standardise better security and privacy mechanisms developed elsewhere.

In 2013, the web was largely unencrypted despite HTTPS being relatively usable, and that was partly due to problems using the Web PKI at scale. The Let's Encrypt initiative [LE] issued its first certificates in 2015 as part of its aim to try to move the web towards being fully encrypted, and it has been extremely successful in helping achieve that goal. Subsequently, the automation protocols developed for Let's Encrypt were standardised in the IETF's ACME Working Group [ACME].

In 2013, most email transport between mail servers was cleartext, directly enabling some of the attacks documented in the Snowden documents. Significant effort by major mail services and MTA software developers since then have resulted in more than 90% of email being encrypted between mail servers, and various IETF protocols have been defined in order to improve that situation, e.g., SMTP MTA Strict Transport Security (MTA-STS) [RFC8461].

Lastly, MAC addresses have historically been long-term fixed values visible to local networks (and beyond), which enabled some tracking attacks that were documented in the Snowden documents [Toronto]. Implementers, vendors, and the IEEE 802 standards group recognised this weakness and started work on MAC address randomisation that in turn led to the IETF's MADINAS Working Group [MADINAS], which aims to ensure randomised MAC addresses can be used on the Internet without causing unintentional harm. There is also a history of IETF work on deprecating MAC-address-based IPv6 interface identifiers and advocating pseudorandom identifiers and temporary addresses, some of which pre-dates Snowden [RFC7217] [RFC8064] [RFC8981].

In summary, the significantly large volume of technical work pursued in the IETF and elsewhere as a result of the Snowden revelations has focussed on two main things: decreasing the amount of plaintext that remains visible to network observers and secondly reducing the number of long-term identifiers that enable unexpected identification or re-identification of devices or users. This work is not by any means complete, nor is deployment universal, but significant progress has been made, and the work continues even if the level of annoyance at the attack has faded somewhat over time.

One should also note that there has been pushback against these improvements in security and privacy and the changes they cause for deployments. That has come from more or less two camps: those on whom these improvements force change tend to react badly, but later figure out how to adjust, and those who seemingly prefer not to strengthen security so as to, for example, continue to achieve what they call "visibility" even in the face of the many engineers who correctly argue that such an anti-encryption approach inevitably leads to worse security overall. The recurring nature of this kind of pushback is nicely illustrated by [RFC1984]. That informational document was published in 1996 as an IETF response to an early iteration of the perennial "encryption is bad" argument. In 2015, the unmodified 1996 text was upgraded to a BCP (BCP 200) as the underlying arguments have not changed, and will not change.

Looking back on all the above from a 2023 vantage point, I think that, as a community of Internet engineers, we got a lot right, but that today there's way more that needs to be done to better protect the security and privacy of people who use the Internet. In particular, we (the technical community) haven't done nearly as good a job at countering surveillance capitalism [Zubhoff2019], which has exploded in the last decade. In part, that's because many of the problems are outside of the scope of bodies such as the IETF. For example, intrusive backend sharing of people's data for advertising purposes can't really be mitigated via Internet protocols.

However, I also think that the real annoyance felt with respect to the Snowden revelations is (in general) not felt nearly as much when it comes to the legal but hugely privacy-invasive activities of major employers of Internet engineers.

It's noteworthy that RFC 7258 doesn't consider that bad actors are limited to governments, and personally, I think many advertising industry schemes for collecting data are egregious examples of pervasive monitoring and hence ought also be considered an attack on the Internet that ought be mitigated where possible. However, the Internet technical community clearly hasn't acted in that way over the last decade.

Perhaps that indicates that Internet engineers and the bodies in which they congregate need to place much more emphasis on standards for ethical behaviour than has been the case for the first half-century of the Internet. And while it would be good to see the current leaders of Internet bodies work to make progress in that regard, at the time of writing, it sadly seems more likely that government regulators will be the ones to try force better behaviour. That of course comes with a significant risk of having regulations that stymie the kind of permissionless innovation that characterised many earlier Internet successes.

So while we got a lot right in our reaction to Snowden's revelations, currently, we have a "worse" Internet. Nonetheless, I do still hope to see a sea change there, as the importance of real Internet security and privacy for people becomes utterly obvious to all, even the most hard-core capitalists and government signals intelligence agencies. That may seem naive, but I remain optimistic that, as a fact-based community, we (and eventually our employers) will recognise that the lesser risk is to honestly aim to provide the best security and privacy practically possible.

4. Farzaneh Badii: Did Snowden's Revelations Help with Protecting Human Rights on the Internet?

It is very difficult to empirically measure the effect of Snowden's revelations on human rights and the Internet. Anecdotally, we have been witnessing dominant regulatory and policy approaches that impact technologies and services that are at the core of protecting human rights on the Internet. (A range of European Union laws aims to address online safety or concentration of data. There are many more regulations that have an impact on the Internet [Masnick2023].) There has been little progress in fixing technical and policy issues that help enable human rights. The Snowden revelations did not revolutionize the Internet governance and technical approaches to support human rights such as freedom of expression, freedom of association and assembly, and privacy. It did not decrease the number of Internet shutdowns nor the eagerness of authoritarian (and even to some extent democratic) countries to territorialize the Internet. In some cases, the governments argued that they should have more data sovereignty or Internet sovereignty. Perhaps the revelations helped with the evolution of some technical and policy aspects.

After Snowden's revelations 10 years ago, engineers and advocates at the IETF responded in a few ways. One prominent response was the issuance of a BCP document, "Pervasive Monitoring Is an Attack" [RFC7258] by Farrell and Tschofenig. The responses to the Snowden revelations did not mean that IETF had lost sight of issues such as privacy and surveillance. There were instances of resistance to surveillance in the past by engineers (we do not delve into how successful that was in protecting human rights). However, historically, many engineers believed that widespread and habitual surveillance was too expensive to be practical. The revelations proved them wrong.

Rights-centered activists were also involved with the IETF before the revelations. For example, staff from Center for Democracy and Technology (CDT) was undertaking work at the IETF (and was a member of the Internet Architecture Board) and held workshops about the challenges of creating privacy-protective protocols and systems. The technical shortcomings that were exploited by the National Security Agency to carry out mass-scale surveillance were recognized by the IETF before the Snowden revelations [Garfinkel1995] [RFC6462]. In 2012, Joy Liddicoat and Avri Doria wrote a report for the Internet Society that extensively discussed the processes and principles of human rights and Internet protocols [Doria2012].

Perhaps the Snowden revelations brought more attention to the IETF and its work as it related to important issues, such as privacy and freedom of expression. It might have also expedited and helped with more easily convening the Human Rights Protocol Considerations Research Group (HRPC) in the Internet Research Task Force (IRTF) in July 2015. The HRPC RG was originally co-chaired by Niels ten Oever (who worked at Article 19 at the time) and Internet governance activist Avri Doria. The charter of the HRPC RG states that the group was established: "to research whether standards and protocols can enable, strengthen or threaten human rights, as defined in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR)."

During the past decade, a few successful strides were made to create protocols that, when and if implemented, aim at protecting privacy of the users, as well as help with reducing pervasive surveillance. These efforts were in keeping with the consensus of the IETF found in RFC 7258. Sometimes these protocols have anti-censorship qualities as well. A few examples immediately come to mind: 1) the encryption of DNS queries (for example, DNS over HTTPS), 2) ACME protocol underpinning the Let's Encrypt initiative, and 3) Registration Data Access Protocol (RDAP) [RFC7480] [RFC7481] [RFC8056] [RFC9082] [RFC9083] [RFC9224]. (It is debatable that RDAP had anything to do with the Snowden revelations, but it is still a good example and is finally being implemented.)

The DNS Queries over HTTPS protocol aimed to encrypt DNS queries. Four years after RFC 7258, DoH was developed to tackle both active and passive monitoring of DNS queries. It is also a tool that can help with combatting censorship. Before the revelations, DNS query privacy would have been controversial due to being expensive or unnecessary, but the Snowden revelations made it more plausible. Let's Encrypt was not an Internet protocol, but it was an initiative that aimed to encrypt the web, and later on some of the automation protocols were standardized in the IETF ACME Working Group. RDAP could solve a long-term problem: redacting the domain name registrants' (and IP address holders') sensitive, personal data but at the same time enabling legitimate access to the information. As to the work of HRPC Research Group, it has so far issued [RFC8280] by ten Oever and Cath and a number of informational Internet-Drafts.

While we cannot really argue that all the movements and privacy-preserving protocols and initiatives that enable protecting human rights at the infrastructure layer solely or directly result from the Snowden revelations, I think it is safe to say that the revelations helped with expediting the resolution of some of the "technical" hesitations that had an effect on fixing Internet protocols that enabled protection of human rights.

Unfortunately, the Snowden revelations have not yet helped us meaningfully with adopting a human rights approach. We can't agree on prioritizing human rights in our Internet communities for a host of reasons. This could be due to: 1) human rights are sometimes in conflict with each other; 2) it is simply not possible to mitigate the human right violation through the Internet protocol; 3) it is not obvious for the engineers in advance how the Internet protocol contributes to enabling human rights protections, or precisely what they ought to do; 4) the protocol is already there, but market, law, and a host of other societal and political issues do not allow for widespread implementation.

IETF did not purposefully take a long time to adopt and implement protocols that enabled human rights. There were technical and political issues that created barriers. For example, as WHOIS was not capable of accommodating a tiered-access option, the IETF community attempted a few times before to create a protocol that would disclose the necessary information of IP holders and domain name registrants while at the same time protecting their data (Cross Registry Internet Service Protocol (CRISP) and later on Internet Registry Information Service (IRIS) are the examples). However, IRIS was technically very difficult to implement. It was not until RDAP was developed and the General Data Protection Regulation (GDPR) was enacted that Internet Corporation for Assigned Names and Numbers had to consider instructing registries and registrars to implement RDAP and its community had to come up with a privacy-compliant policy. Overall, a host of regulatory and market incentives can halt or slow down the implementation of human-rights-enabling protocols and implementation could depend on other organizations with their own political and stakeholder conflicts. Sometimes the protocol is available, but the regulatory framework and the market do not allow for implementation. Sometimes the surrounding context includes practical dimensions that are easy to overlook in a purely engineering-focused argument.

A curious example of this is sanctions regimes that target transactions involving economically valuable assets. As a result, sanctions might limit sanctioned nations' and entities' access to IPv4 resources (because the existence of a resale market for these addresses causes acquiring them to be interpreted as buying something of value), though the same consideration may not apply to IPv6 address resources. But IPv6 adoption itself depends on a host of complex factors that are by no means limited to technical comparisons of the properties of IPv4 and IPv6. Someone focused only on technical features of protocols may devise an elegant solution but be surprised both by deployment challenges and unintended downstream effects. Sometimes there are arguments over implementation of a protocol because as it is perceived, while it can protect freedom of expression and reduce surveillance, it can hamper other human rights. For instance, the technical community and some network operators still have doubts about the implementation of DNS over HTTPS, despite its potential to circumvent censorship and its ability to encrypt DNS queries. The arguments against implementation of DoH include protection of children online and lack of law enforcement access to data.

We must acknowledge that sometimes the technical solutions that we use that protect one right (for example, encryption to protect the right to privacy or to prevent surveillance) could potentially affect technical and policy solutions that try to protect other human rights (for example, encryption could prevent financial institutions from monitoring employees' network activities to detect fraudulent behavior). Acknowledging and identifying these conflicts can help

us come up with alternative techniques that could protect human rights while not hampering other technical solutions such as encryption. Where such alternative techniques are not possible, acknowledging the shortcoming could clarify and bring to light the trade-offs that we have accepted in our Internet system.

Ironically, we advocate for connectivity and believe expressing oneself on the Internet is a human right, but when a war erupts, we resort to tools that impact that very concept. For example, some believe that, by imposing sanctions on critical properties of the Internet, we can punish the perpetrators of a war. The Regional Internet Registries that are in charge of registration of IP addresses have shown resilience to these requests. However, some tech companies (for example, Cogent [Roth2022]) decided not to serve sanctioned countries and overcomplied with sanctions. Overcompliance with sanctions could hamper ordinary people's access to the Internet [Badii2023].

Perhaps we can solve some of these problems by undertaking a thorough impact assessment and contextualization to reveal how and why Internet protocols affect human rights (something Fidler and I argued for [Badii2021]). Contextualization and impact assessment can reveal how each Internet protocol or each line of code, in which systems, have an impact on which and whose human rights.

The HRPC RG (which I am a part of) and the larger human rights and policy analyst communities are still struggling to analyze legal, social, and market factors alongside the protocols to have a good understanding of what has an impact and what has to be changed. It is hard, but it is not impossible. If we thoroughly document and research the lifecycle of an Internet protocol and contextualize it, we might have a better understanding of which parts of the protocol to fix and how to fix them in order to protect human rights.

Overall, the revelations did, to some extent, contribute to the evolution of our ideas and perspectives. Our next step should be to undertake research on the impact of Internet systems (including Internet protocols) on human rights, promote the implementation of protocols good for human rights through policy and advocacy, and focus on which technical parts we can standardize to help with more widespread implementation of human-rights-enabling Internet protocols.

5. Steven M. Bellovin: Governments and Cryptography: The Crypto Wars

5.1. Historical Background

It's not a secret: many governments in the world don't like it when people encrypt their traffic. More precisely, they like strong cryptography for themselves but not for others, whether those others are private citizens or other countries. But the history is longer and more complex than that.

For much of written history, both governments and individuals used cryptography to protect their messages. To cite just one famous example, Julius Caesar is said to have encrypted messages by shifting letters in the alphabet by 3 [Kahn1996]. In modern parlance, 3 was the key, and each letter was encrypted with

C[i] = (P[i] + 3) mod 23

(The Latin alphabet of his time had only 23 letters.) Known Arabic writings on cryptanalysis go back to at least the 8th century; their sophistication shows that encryption was reasonably commonly used. In the 9th century, Abū Yūsuf Yaʻqūb ibn ʾIsḥāq aṣ-Ṣabbāḥ al-Kindī developed and wrote about frequency analysis as a way to crack ciphers [Borda2011] [Kahn1996].

In an era of minimal literacy, though, there wasn't that much use of encryption, simply because most people could neither read nor write. Governments used encryption for diplomatic messages, and cryptanalysts followed close behind. The famed Black Chambers of the Renaissance era read messages from many different governments, while early cryptographers devised stronger and stronger ciphers [Kahn1996]. In Elizabethan times in England, Sir Francis Walsingham's intelligence agency intercepted and decrypted messages from Mary, Queen of Scots; these messages formed some of the strongest evidence against her and eventually led to her execution [Kahn1996].

This pattern continued for centuries. In the United States, Thomas Jefferson invented the so-called wheel cipher in the late 18th century; it was reinvented about 100 years later by Étienne Bazeries and used as a standard American military cipher well into World War II [Kahn1996]. Jefferson and other statesmen of the late 18th and early 19th centuries regularly used cryptography when communicating with each other. An encrypted message was even part of the evidence introduced in Aaron Burr's 1807 trial for treason [Kerr2020] [Kahn1996]. Edgar Allan Poe claimed that he could cryptanalyze any message sent to him [Kahn1996].

The telegraph era upped the ante. In the US, just a year after Samuel Morse deployed his first telegraph line between Baltimore and Washington, his business partner, Francis Smith, published a codebook to help customers protect their traffic from prying eyes [Smith1845]. In 1870, Britain nationalized its domestic telegraph network; in response, Robert Slater published a more sophisticated codebook [Slater1870]. On the government side, Britain took advantage of its position as the central node in the world's international telegraphic networks to read a great deal of traffic passing through the country [Headrick1991] [Kennedy1971]. They used this ability strategically, too -- when war broke out in 1914, the British Navy cut Germany's undersea telegraph cables, forcing them to use radio; an intercept of the so-called Zimmermann telegram, when cryptanalyzed, arguably led to American entry into the war and thence to Germany's defeat. Once the US entered the war, it required users of international telegraph lines to deposit copies of the codebooks they used for compression, so that censors could check messages for prohibited content [Kahn1996].

In Victorian Britain, private citizens, often lovers, used encryption in newspapers' personal columns to communicate without their parents' knowledge. Charles Wheatstone and Charles Babbage used to solve these elementary ciphers routinely for their own amusement [Kahn1996].

This pattern continued for many years. Governments regularly used ciphers and codes, while other countries tried to break them; private individuals would sometimes use encryption but not often, and rarely well. But the two World Wars marked a sea change, one that would soon reverberate into the civilian world.

The first World War featured vast troop movements by all parties; this in turn required a lot of encrypted communications, often by telegraph or radio. These messages were often easily intercepted in bulk. Furthermore, the difficulty of encrypting large volumes of plaintext led to the development of a variety of mechanical encryption devices, including Germany's famed Enigma machine. World War II amplified both trends. It also gave rise to machine-assisted cryptanalysis, such as the United Kingdom's bombes (derived from an earlier Polish design) and Colossus machine, and the American's device for cracking Japan's PURPLE system. The US also used punch card-based tabulators to assist in breaking other Japanese codes, such as the Japanese Imperial Navy's JN-25 [Kahn1996] [Rowlett1998].

These developments set the stage for the postwar SIGINT (Signals Intelligence) environment. Many intragovernmental messages were sent by radio, making them easy to intercept; advanced cryptanalytic machines made cryptanalysis easier. Ciphers were getting stronger, though, and government SIGINT agencies did not want to give up their access to data. While there were undoubtedly many developments, two are well known.

The first involved CryptoAG, a Swedish (and later Swiss) manufacturer of encryption devices. The head of that company, Boris Hagelin, was a friend of William F. Friedman, a pioneering American cryptologist. During the 1950s, CryptoAG sold its devices to other governments; apparently at Friedman's behest, Hagelin weakened the encryption in a way that let the NSA read the traffic [Miller2020].

The story involving the British is less well-documented and less clear. When some of Britain's former colonies gained their independence, the British government gave them captured, war-surplus Enigma machines to protect their own traffic. Some authors contend that this was deceptive, in that these former colonies did not realize that the British could read Enigma-protected traffic; others claim that this was obvious but that these countries didn't care: Britain was no longer their enemy; it was neighboring countries they were worried about. Again, though, this concerned governmental use of encryption [Kahn1996] [Baldwin2022]. There was still little private use.

5.2. The Crypto Wars Begin

The modern era of conflict between an individual's desire for privacy and the government desires to read traffic began around 1972. The grain harvest in the USSR had failed; since relations between the Soviet Union and the United States were temporarily comparatively warm, the Soviet grain company -- an arm of the Soviet government, of course -- entered into negotiations with private American companies. Unknown to Americans at the time, Soviet intelligence was intercepting the phone calls of the American negotiating teams. In other words, private companies had to deal with state actors as a threat. Eventually, US intelligence learned of this and came to a realization: the private sector needed strong cryptography, too, to protect

American national interests [Broad1982] [Johnson1998]. This underscored the need for strong cryptography to protect American civilian traffic -- but the SIGINT people were unhappy at the thought of more encryption that they couldn't break.

Meanwhile, the US was concerned about protecting unclassified data [Landau2014]. In 1973 and again in 1974, the National Bureau of Standards (NBS) put out a call for a strong, modern encryption algorithm. IBM submitted Lucifer, an internally developed algorithm based on what has become known as a 16-round Feistel network. The original version used a long key. It seemed quite strong, so NBS sent it off to the NSA to get their take. The eventual design, which was adopted in 1976 as the Data Encryption Standard (DES), differed in some important ways from Lucifer. First, the so-called S-boxes, the source of the cryptologic strength of DES, were changed, and were now demonstrably not composed of random integers. Many researchers alleged that the S-boxes contained an NSA back door. It took nearly 20 years for the truth to come out: the S-boxes were in fact strengthened, not weakened. Most likely, IBM independently discovered the attack now known as differential cryptanalysis, though some scholars suspect that the NSA told them about it. The nonrandom S-boxes protected against this attack. The second change, though, was clearly insisted on by the NSA: the key size was shortened, from Lucifer's 112 bits to DES's 56 bits. We now know that the NSA wanted a 48-bit key size, while IBM wanted 64 bits; they compromised at 56 bits.

Whitfield Diffie and Martin Hellman, at Stanford University, wondered about the 56-bit keys. In 1979, they published a paper demonstrating that the US government, but few others, could afford to build a brute-force cracking machine, one that could try all 2^{56} possible keys to crack a message. NSA denied tampering with the design; a Senate investigating committee found that assertion to be correct, but did not discuss the shortened key length issue.

This, however, was not Diffie and Hellman's greatest contribution to cryptology. A few years earlier, they had published a paper inventing what is now known as public key cryptography. (In fact, public key encryption had been invented a few years earlier at UK Government Communications Headquarters (GCHQ), but they kept their discovery classified until 1997.) In 1978, Ronald Rivest, Adi Shamir, and Leonard Adleman devised the RSA algorithm, which made it usable. (An NSA employee, acting on his own, sent a letter warning that academic conferences on cryptology might violate US export laws.)

Around the same time, George Davida at the University of Wisconsin applied for a patent on a stream cipher; the NSA slapped a secrecy order on the application. This barred him from even talking about his invention. The publicity was devastating; the NSA had to back down.

The Crypto Wars had thus begun: civilians were inventing strong encryption systems, and the NSA was tampering with them or trying to suppress them. Bobby Inman, the then-director of the NSA, tried creating a voluntary review process for academic papers, but very few researchers were interested in participating [Landau1988].

There were few major public battles during the 1980s because there were few new major use cases for civilian cryptography during that time. There was one notable incident, though: Shamir, Amos Fiat, and Uriel Feige invented zero-knowledge proofs and applied for a US patent. In response, the US Army slapped a secrecy order on the patent. After a great deal of public

outrage and intervention by, of all organizations, the NSA, the order was lifted on very narrow grounds: the inventors were not American, and they had been discussing their work all over the world [Landau1988].

In the 1990s, though, everything changed.

5.3. The Battle Is Joined

There were three major developments in cryptography in the early 1990s. First, Phil Zimmermann released PGP (Pretty Good Privacy), a package to encrypt email messages. In 1993, AT&T planned to release the TSD-3600, an easy-to-use phone encryptor aimed at business travelers. Shortly after that, the Netscape Communications Corporation released SSL (Secure Socket Layer) as a way to enable web-based commerce using their browser and web server. All of these were seen as threats by the NSA and the FBI.

PGP was, at least arguably, covered by what was known as ITAR, the International Trafficking in Arms Regulations -- under American law, encryption software was regarded as a weapon, so exports required a license. It was also alleged to infringe the patents on the RSA algorithm. Needless to say, both issues were problematic for what was intended to be open source software. Eventually, the criminal investigation into Zimmermann's role in the spread of PGP overseas was dropped, but the threat of such investigations remained to deter others [Levy2001].

The TSD-3600 was another matter. AT&T was a major corporation that did not want to pick a fight with the US government, but international business travelers were seen as a major market for the device. At the government's "request", the DES chip was replaced with what was known as the Clipper chip. The Clipper chip used Skipjack, a cipher with 80-bit keys; it was thus much stronger against brute-force attacks than DES. However, it provided "key escrow". Without going into any details, the key escrow mechanism allowed US government eavesdroppers to consult a pair of (presumably secure) internal databases and decrypt all communications protected by the chip. The Clipper chip proved to be extremely unpopular with industry; that AT&T Bell Labs' Matt Blaze found a weakness in the design [Blaze1994], one that let you use Skipjack without the key escrow feature, didn't help its reputation.

The third major development, SSL, was even trickier. SSL was aimed at e-commerce, and of course Netscape wanted to be able to sell its products outside the US. That would require an export license, so they made a deal with the government: non-American users would receive a version that used 40-bit keys, a key length far shorter than what the NSA had agreed to 20 years earlier. (To get ahead of the story: there was a compromise mode of operation, wherein an export-grade browser could use strong encryption when talking to a financial institution. This hybrid mode led to cryptographic weaknesses discovered some 20 years later [Adrian2015].)

Technologists and American industry pushed back. The IETF adopted the Danvers Doctrine, described in [RFC3365]:

> At the 32cd [sic] IETF held in Danvers, Massachusetts during April of 1995 the IESG asked the plenary for a consensus on the strength of security that should be provided by IETF standards. Although the immediate issue before the IETF was whether or not to support "export" grade security (which is to say weak security) in standards the question raised the generic issue of security in general.
>
> The overwhelming consensus was that the IETF should standardize on the use of the best security available, regardless of national policies. This consensus is often referred to as the "Danvers Doctrine".

Then American companies started losing business to their overseas competitors, who did not have to comply with US export laws. All of this led to what seemed like a happy conclusion: the US government drastically loosened its export rules for cryptographic software. All was well -- or so it seemed...

5.4. The Hidden Battle

Strong cryptography was here to stay, and it was no longer an American monopoly, if indeed it ever was. The Information Assurance Directorate of the NSA, the part of the agency that is supposed to protect US data, was pleased by the spread of strong cryptography. When the Advanced Encryption Standard (AES) competition was held, there were no allegations of malign NSA interference; in fact, the winning entry was devised by two Europeans, Joan Daemen and Vincent Rijmen. But the NSA and its SIGINT needs did not go away -- the agency merely adopted other techniques.

I have often noted that one doesn't go through strong security, one goes around it. When strong encryption became more common and much more necessary, the NSA started going around it, by targeting computers and the software that they run. And it seems clear that they believe that AES is quite strong; they've even endorsed its use for protecting TOP SECRET information. But there was an asterisk attached to that endorsement: AES is suitable if and only if properly used and implemented. Therein lies the rub.

The first apparent attempt to tamper with outside cryptographic mechanisms was discovered in 2007, when two Microsoft researchers, Dan Shumow and Niels Ferguson, noted an odd property of a NIST-standardized random number generator, DUAL_EC_DRBG. (The NBS had been renamed to NIST, the National Institute of Standards and Technology.) Random numbers are vital for cryptography, but Shumow and Ferguson showed that if certain constants in DUAL_EC_DRBG were chosen in a particular way with a known-but-hidden other number, whoever knew that number could predict all future random numbers from a system given a few sample bytes to start from [Kostyuk2022]. These sample bytes could come from known keys, nonces, or anything else. Where did the constants in DUAL_EC_DRBG come from and how were they chosen or generated? No one who knows is talking. But although cryptographers and security specialists were very suspicious -- Bruce Schneier wrote in 2007, before more facts came out, that "both NIST and the NSA have some explaining to do"; I assigned my students reading on the topic -- the issue didn't really get any traction until six years later, when among the papers that Edward

Snowden disclosed was the information that the NSA had indeed tampered with a major cryptographic standard, though published reports did not specifically name DUAL_EC_DRBG or explain what the purpose was.

The revelations didn't stop there. There have been allegations that the NSA paid some companies to use DUAL_EC_DRBG in their products. Some people have claimed that there were attempts to modify some IETF standards to make enough random bytes visible, to aid in exploiting the random number generator. A major vendor of networking gear, Juniper, did use DUAL_EC_DRBG in some of its products, but with different constants [Checkoway2016]. Where did these come from? Were they from the NSA or some other government? Could their source tree have been hacked by an intelligence agency? There was a different hack of their code at around the same time [Moore2015]. No one is talking.

The Snowden revelations also included data suggesting that the NSA had a worldwide eavesdropping network and a group that tried very specific, targeted hacks on very specific targets' systems. In retrospect, neither is surprising: "spies gonna spy". The NSA's business is signals intelligence; of course they're going to try to intercept traffic. Indeed, the DUAL_EC_DRBG tampering is useless to anyone who has not collected messages to decrypt. And targeted hacks are a natural way around strong encryption: collect the data before it is encrypted or after it is decrypted, and don't worry about the strength of the algorithms.

The privacy community, worldwide, was appalled, though perhaps they shouldn't have been. It calls to mind the line that Claude Rains' character uttered in the movie Casablanca [Curtiz]: "I'm shocked, shocked to find that gambling is going on in here." The immediate and continuing reaction was to deploy more encryption. The standards have long existed; what was missing was adoption. One barrier was the difficulty and expense of getting certificates to use with TLS, the successor to SSL; that void was filled by Let's Encrypt [LE], which made free certificates easy to get online. Today, most HTTP traffic is encrypted, so much so that Google's search engine down-ranks sites that do not use it. Major email providers uniformly use TLS to protect all traffic. Wi-Fi, though a local area issue, now uses much stronger encryption. (It's important to remember that security and insecurity have economic components. Security doesn't have to be perfect to be very useful, if it raises the attackers' costs by enough.)

The news on the software side is less good. Not a day goes by when one does not read of organizations being hit by ransomware. It goes without saying that any threat actor capable of encrypting disks is also capable of stealing the information on them; indeed, that is a frequent accompanying activity, since the threat of disclosure is another incentive to pay for those sites that do have good enough backups. Major vendors have put a lot of effort into securing their software, but bugs and operational errors by end-user sites persist.

5.5. Whither the IETF?

Signal intelligence agencies, not just the NSA, but its peers around the globe -- most major countries have their own -- are not going to go away. The challenges that have beset the NSA are common to all such agencies, and their solutions are likely the same. The question is what should be done to protect individual privacy. A number of strong democracies, such as Australia and the

United Kingdom, are, in a resumption of the Crypto Wars, moving to restrict encryption. Spurred on by complaints from the FBI and other law enforcement agencies, the US Congress frequently considers bills to do the same.

The IETF has long had a commitment to strong, ubiquitous encryption. This is a good thing. It needs to continue, with cryptography and other security features designed into protocols from the beginning. But there is also a need for maintenance. Parameters such as key lengths and modulus sizes age; a value that is acceptable today may not be 10 years hence. (We've already seen apparent problems from 1024-bit moduli specified in an RFC, an RFC that was not modified when technology improved enough that attacking encryption based on them had become feasible [Adrian2015].) The IETF can do nothing about the code that vendors ship or that sites use, but it can alert the world that it thinks things have changed.

Cryptoagility is of increasing importance. In the next very few years, we will have so-called post-quantum algorithms. Both protocols and key lengths will need to change, perhaps drastically. Is the IETF ready? What will happen to, say, DNSSEC if key lengths become drastically longer? Backwards compatibility will remain important, but that, of course, opens the door to other attacks. We've long thought about them; we need to be sure that our mechanisms work -- we've been surprised in the past [BellovinRescorla2006].

We also need to worry more about metadata. General Michael Hayden, former director of both the NSA and the CIA, once remarked, "We kill people based on metadata" [Ferran2014]. But caution is necessary; attempts to hide metadata can have side effects. To give a trivial example, Tor is quite strong, but if your exit node is in a different country than you are in, web sites that use IP geolocation may present their content in a language foreign to you. Some sites even block connections from known Tor exit nodes. More generally, many attempts to hide metadata involve trusting a different party; that party may turn out to be untrustworthy or it may itself become a target of attack. As another prominent IETFer has remarked, "Insecurity is like entropy; you can't destroy it, but you can move it around." The IETF has done a lot; it needs to do more. And remember that the risk here is not just governments acting directly, it's also private companies that collect the data and sell it to all comers.

Finally, the IETF must remember that its middle name is "Engineering". To me, one of the attributes of engineering is the art of picking the right solution in an over-constrained environment. Intelligence agencies won't go away, nor will national restrictions on cryptography. We have to pick the right path while staying true to our principles.

6. Security Considerations

Each or any of the authors may have forgotten or omitted things or gotten things wrong. We're sorry if that's the case, but that's in the nature of a look-back such as this. Such flaws almost certainly won't worsen security or privacy, though.

7. IANA Considerations

This document has no IANA actions.

8. Informative References

[ACME] IETF, "Automated Certificate Management Environment (acme)", <https://datatracker.ietf.org/wg/acme/about/>.

[Adrian2015] Adrian, D., Bhargavan, K., Durumeric, Z., Gaudry, P., Green, M., Halderman, J. A., Heninger, N., Springhall, D., Thomé, E., Valenta, L., VanderSloot, B., Wustrow, E., Zanella-Béguelin, S., and P. Zimmermann, "Imperfect Forward Secrecy: How Diffie-Hellman Fails in Practice", CCS '15: Proceedings of the 22th ACM Conference on Computer and Communications Security, October 2015, <https://dl.acm.org/doi/10.1145/2810103.2813707>.

[Badii2021] Badiei, F., Fidler, B., and The Pennsylvania State University Press, "The Would-Be Technocracy: Evaluating Efforts to Direct and Control Social Change with Internet Protocol Design", Journal of Information Policy, vol. 11, pp. 376-402, DOI 10.5325/jinfopoli.11.2021.0376, December 2021, <https://doi.org/10.5325/jinfopoli.11.2021.0376>.

[Badii2023] Badiei, F., "Sanctions and the Internet", Digital Medusa, 2023, <https://digitalmedusa.org/wp-content/uploads/2023/05/SanctionsandtheInternet-DigitalMedusa.pdf>.

[Baldwin2022] Baldwin, M., "Did Britain sell Enigmas postwar?", Dr. Enigma, March 2022, <https://drenigma.org/2022/03/02/did-britain-sell-enigmas-postwar/>.

[BellovinRescorla2006] Bellovin, S. M. and E. K. Rescorla, "Deploying a New Hash Algorithm", Proceedings of NDSS '06, February 2006, <https://www.cs.columbia.edu/~smb/papers/new-hash.pdf>.

[Blaze1994] Blaze, M., "Protocol Failure in the Escrowed Encryption Standard", CCS '94: Proceedings of Second ACM Conference on Computer and Communications Security, 1994, <https://dl.acm.org/doi/10.1145/191177.191193>.

[Borda2011] Borda, M., "Fundamentals in Information Theory and Coding", Springer-Berlin, May 2011.

[Broad1982] Broad, W. J., "Evading the Soviet Ear at Glen Cove", Science, 217:4563, pp. 910-911, September 1982, <https://www.science.org/doi/abs/10.1126/science.217.4563.910>.

[CFRG] IRTF, "Crypto Forum (cfrg)", <https://datatracker.ietf.org/rg/cfrg/about/>.

[Checkoway2016]
Checkoway, S., Maskiewicz, J., Garman, C., Fried, J., Cohney, S., Green, M., Heninger, N., Weinmann, R. P., Rescorla, E., and Hovav Shacham, "A Systematic Analysis of the Juniper Dual EC Incident", CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pp. 468-479, October 2016, <https://dl.acm.org/citation.cfm?id=2978395>.

[CURDLE] IETF, "CURves, Deprecating and a Little more Encryption (curdle)", <https://datatracker.ietf.org/wg/curdle/about/>.

[Curtiz] Curtiz, M., Epstein, J. J., Epstein, P. G., and H. Koch, "Casablanca", Warner Bros. Pictures, November 1942.

[Doria2012] Liddicoat, J. and A. Doria, "Human Rights and Internet Protocols: Comparing Processes and Principles", The Internet Society, December 2012, <https://www.internetsociety.org/resources/doc/2012/human-rights-and-internet-protocols-comparing-processes-and-principles/>.

[Dual-EC] Bernstein, D., Lange, T., and R. Niederhagen, "Dual EC: A Standardized Back Door", July 2016, <https://eprint.iacr.org/2015/767.pdf>.

[Ferran2014] Ferran, L., "Ex-NSA Chief: "We Kill People Based on Metadata"", ABC News, May 2014, <https://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata>.

[Garfinkel1995] Garfinkel, S., "PGP: Pretty Good Privacy", O'Reilly and Associates, January 1995.

[Guard2013] Greenwald, G., "NSA collecting phone records of millions of Verizon customers daily", The Guardian, June 2013.

[Headrick1991] Headrick, D. R., "The Invisible Weapon: Telecommunications and International Politics, 1851-1945", Oxford University Press, 1991.

[Johnson1998] Johnson, T. R., "American Cryptology During the Cold War, 1945-1989; Book III: Retrenchment and Reform, 1972-1980", Center for Cryptologic History, NSA, 1998, <https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/cryptologic-histories/cold_war_iii.pdf>.

[Kahn1996] Kahn, D., "The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet", 2nd Edition, Scribner, 1996.

[Kennedy1971] Kennedy, P. M., "Imperial cable communications and strategy, 1870-1914", English Historical Review, 86:341, pp. 728-752, Oxford University Press, October 1971, <https://www.jstor.org/stable/563928>.

[Kerr2020] Kerr, O. S., "Decryption Originalism: The Lessons of Burr", Harvard Law Review, 134:905, January 2021, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3533069>.

[Kostyuk2022] Kostyuk, N. and S. Landau, "Dueling over DUAL_EC_DRBG: The Consequences of Corrupting a Cryptographic Standardization Process", Harvard National Security Journal, 13:2, pp. 224-284, June 2022, <https://www.harvardnsj.org/wp-content/uploads/sites/13/2022/06/Vol13Iss2_Kostyuk-Landau_Dual-EC-DRGB.pdf>.

[Landau1988] Landau, S., "Zero Knowledge and the Department of Defense", Notices of the American Mathematical Society, 35:1, pp. 5-12, January 1988, <https://privacyink.org/pdf/Zero_Knowledge.pdf>.

[Landau2014] Landau, S., "Under the Radar: NSA's Efforts to Secure Private-Sector Telecommunications Infrastructure", Journal of National Security Law & Policy, 7:3, September 2014, <https://jnslp.com/wp-content/uploads/2015/03/NSA%E2%80%99s-Efforts-to-Secure-Private-Sector-Telecommunications-Infrastructure_2.pdf>.

[LE] Aas, J., Barnes, R., Case, B., Durumeric, Z., Eckersley, P., Flores-López, A., Halderman, A., Hoffman-Andrews, J., Kasten, J., Rescorla, E., Schoen, S. D., and B. Warren, "Let's Encrypt: An Automated Certificate Authority to Encrypt the Entire Web", CCS '19: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, November 2019, <https://dl.acm.org/doi/pdf/10.1145/3319535.3363192>.

[Levy2001] Levy, S., "Crypto: How the Code Rebels Beat the Government-Saving Privacy in the Digital Age", Penguin Publishing Group, January 2001.

[MADINAS] IETF, "MAC Address Device Identification for Network and Application Services (madinas)", <https://datatracker.ietf.org/wg/madinas/about>.

[Masnick2023] Masnick, M., "The Unintended Consequences of Internet Regulation", Copia, April 2023, <https://copia.is/library/unintended-consequences/>.

[Miller2020] Miller, G., "The intelligence coup of the century", The Washington Post, February 2020, <https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/>.

[Moore2015] Moore, H. D., "CVE-2015-7755: Juniper ScreenOS Authentication Backdoor", Rapid7, December 2015, <https://www.rapid7.com/blog/post/2015/12/20/cve-2015-7755-juniper-screenos-authentication-backdoor/>.

[MPLS-OPPORTUNISTIC-ENCRYPT] Farrel, A. and S. Farrell, "Opportunistic Security in MPLS Networks", Work in Progress, Internet-Draft, draft-ietf-mpls-opportunistic-encrypt-03, 28 March 2017, <https://datatracker.ietf.org/doc/html/draft-ietf-mpls-opportunistic-encrypt-03>.

[Perpass] IETF, "perpass mailing list", <https://mailarchive.ietf.org/arch/browse/perpass/>.

[Perpass-BoF] IETF, "perpass BoF -- Handling Pervasive Monitoring in the IETF", IETF 88 Proceedings, November 2013, <https://www.ietf.org/proceedings/88/perpass.html>.

[Plenary-video] "IETF 88 Technical Plenary: Hardening The Internet", YouTube video, 2:37:28, posted by "IETF - Internet Engineering Task Force", November 2013, <https://www.youtube.com/watch?v=oV71hhEpQ20&pp=ygUQaWV0ZiA4OCBwbGVuYXJ5IA%3D%3D>.

[Refs-to-7258] IETF, "References to RFC7258", <https://datatracker.ietf.org/doc/rfc7258/referencedby/>.

[RFC1984] IAB and IESG, "IAB and IESG Statement on Cryptographic Technology and the Internet", BCP 200, RFC 1984, DOI 10.17487/RFC1984, August 1996, <https://www.rfc-editor.org/info/rfc1984>.

[RFC3365] Schiller, J., "Strong Security Requirements for Internet Engineering Task Force Standard Protocols", BCP 61, RFC 3365, DOI 10.17487/RFC3365, August 2002, <https://www.rfc-editor.org/info/rfc3365>.

[RFC6462] Cooper, A., "Report from the Internet Privacy Workshop", RFC 6462, DOI 10.17487/RFC6462, January 2012, <https://www.rfc-editor.org/info/rfc6462>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/info/rfc7217>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <https://www.rfc-editor.org/info/rfc7258>.

[RFC7480] Newton, A., Ellacott, B., and N. Kong, "HTTP Usage in the Registration Data Access Protocol (RDAP)", STD 95, RFC 7480, DOI 10.17487/RFC7480, March 2015, <https://www.rfc-editor.org/info/rfc7480>.

[RFC7481] Hollenbeck, S. and N. Kong, "Security Services for the Registration Data Access Protocol (RDAP)", STD 95, RFC 7481, DOI 10.17487/RFC7481, March 2015, <https://www.rfc-editor.org/info/rfc7481>.

[RFC7687] Farrell, S., Wenning, R., Bos, B., Blanchet, M., and H. Tschofenig, "Report from the Strengthening the Internet (STRINT) Workshop", RFC 7687, DOI 10.17487/RFC7687, December 2015, <https://www.rfc-editor.org/info/rfc7687>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/info/rfc7858>.

[RFC8056] Gould, J., "Extensible Provisioning Protocol (EPP) and Registration Data Access Protocol (RDAP) Status Mapping", RFC 8056, DOI 10.17487/RFC8056, January 2017, <https://www.rfc-editor.org/info/rfc8056>.

[RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017, <https://www.rfc-editor.org/info/rfc8064>.

[RFC8280] ten Oever, N. and C. Cath, "Research into Human Rights Protocol Considerations", RFC 8280, DOI 10.17487/RFC8280, October 2017, <https://www.rfc-editor.org/info/rfc8280>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC8461] Margolis, D., Risher, M., Ramakrishnan, B., Brotman, A., and J. Jones, "SMTP MTA Strict Transport Security (MTA-STS)", RFC 8461, DOI 10.17487/RFC8461, September 2018, <https://www.rfc-editor.org/info/rfc8461>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/info/rfc8484>.

[RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <https://www.rfc-editor.org/info/rfc8981>.

[RFC9000] Iyengar, J., Ed. and M. Thomson, Ed., "QUIC: A UDP-Based Multiplexed and Secure Transport", RFC 9000, DOI 10.17487/RFC9000, May 2021, <https://www.rfc-editor.org/info/rfc9000>.

[RFC9082] Hollenbeck, S. and A. Newton, "Registration Data Access Protocol (RDAP) Query Format", STD 95, RFC 9082, DOI 10.17487/RFC9082, June 2021, <https://www.rfc-editor.org/info/rfc9082>.

[RFC9083] Hollenbeck, S. and A. Newton, "JSON Responses for the Registration Data Access Protocol (RDAP)", STD 95, RFC 9083, DOI 10.17487/RFC9083, June 2021, <https://www.rfc-editor.org/info/rfc9083>.

[RFC9113] Thomson, M., Ed. and C. Benfield, Ed., "HTTP/2", RFC 9113, DOI 10.17487/RFC9113, June 2022, <https://www.rfc-editor.org/info/rfc9113>.

[RFC9224] Blanchet, M., "Finding the Authoritative Registration Data Access Protocol (RDAP) Service", STD 95, RFC 9224, DOI 10.17487/RFC9224, March 2022, <https://www.rfc-editor.org/info/rfc9224>.

[Roth2022] Roth, E., "Internet backbone provider shuts off service in Russia", The Verge, March 2022, <https://www.theverge.com/2022/3/5/22962822/internet-backbone-provider-cogent-shuts-off-service-russia>.

[Rowlett1998] Rowlett, F. B., "The Story of Magic, Memoirs of an American Cryptologic Pioneer", Aegean Park Press, 1998.

[Slater1870] Slater, R., "Telegraphic Code, to Ensure Secresy in the Transmission of Telegrams", First Edition, W.R. Gray, 1870, <https://books.google.com/books?id=MJYBAAAAQAAJ>.

[Smith1845] Smith, F. O., "The Secret Corresponding Vocabulary: Adapted for Use to Morse's Electro-Magnetic Telegraph, and Also in Conducting Written Correspondence, Transmitted by the Mails, or Otherwise", Thurston, Isley & Company, 1845, <https://books.google.com/books?id=Z45clCxsF7EC>.

[STRINT] W3C and IAB, "A W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT)", March 2014, <https://www.w3.org/2014/strint/>.

[Timeline] Wikipedia, "Global surveillance disclosures (2013-present)", July 2023, <https://en.wikipedia.org/w/index.php?title=Global_surveillance_disclosures_(2013%E2%80%93present)&oldid=1161557819>.

[TLS-ECH] Rescorla, E., Oku, K., Sullivan, N., and C. A. Wood, "TLS Encrypted Client Hello", Work in Progress, Internet-Draft, draft-ietf-tls-esni-16, 6 April 2023, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-esni-16>.

[Toronto] Memmott, M., "Canada Used Airport Wi-Fi To Track Travelers, Snowden Leak Alleges", NPR, January 2014, <https://www.npr.org/sections/thetwo-way/2014/01/31/269418375/airport-wi-fi-used-to-track-travelers-snowden-leak-alleges>.

[UTA] IETF, "Using TLS in Applications (uta)", <https://datatracker.ietf.org/wg/uta/about>.

[Zubhoff2019] Zuboff, S., "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power", PublicAffairs, ISBN 9781781256855, January 2019.

Acknowledgments

Susan Landau added many valuable comments to Steve Bellovin's essay.

We thank Carsten Bormann, Brian Carpenter, Wendy Grossman, Kathleen Moriarty, Jan Schaumann, Seth David Schoen, and Paul Wouters for comments and review of this text, though that of course doesn't mean that they necessarily agree with the text.

This document was created at the behest of Eliot Lear, who also cat herded and did some editing.

Authors' Addresses

Stephen Farrell
Trinity College, Dublin
Ireland
Email: stephen.farrell@cs.tcd.ie

Farzaneh Badii
Digital Medusa
Email: farzaneh.badii@gmail.com

Bruce Schneier
Harvard University
United States of America
Email: schneier@schneier.com

Steven M. Bellovin
Columbia University
United States of America
Email: smb@cs.columbia.edu