KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

STRENGTHENING THE INTERNET AGAINST PERVASIVE ADVERSARIES: POLICY RESPONSES, IMPLICATIONS, AND OPPORTUNITIES

15 January 2014

Joseph Lorenzo Hall (joe@cdt.org), Chief Technologist;
W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT), 28 Feb–1 Mar 2014, London, UK

Abstract: This paper briefly discusses policy implications of, and opportunities in, efforts in standards-setting organizations to harden the Internet against pervasive attackers.

The Internet today seems very different from the Internet of a year ago. Revelations about pervasive monitoring and attacks by the US NSA and UK GCHQ have recalibrated our global threat model.[1] The efforts in response at the W3C and IETF focus on strengthening core Internet and Web functionality against this class of global attacker.

Efforts to strengthen the Internet do not occur in a vacuum. National and global policies helped to create the current Internet landscape and they will respond in the future and possibly shape it further. In this paper, we outline important policy issues for a strengthened Internet and Web. We also discuss how technologists can provide important input into the policy process.

I. Policy Implications Relevant to Internet and Web Standardization

There are at least two classes of policy issues that W3C and IETF should consider going forward: policy-based responses that may affect Internet and Web standards and policy implications of standards-setting activity itself. A comprehensive discussion of either of these classes is beyond the scope of this paper; instead, we hope to highlight for discussion issues we think are particularly important for Internet and Web standards.

A. Data Storage, Processing, and Routing Localization

One response to global intelligence revelations, notably in the EU and Brazil, is to attempt to increase national control over Internet and Web activity. This is currently popular in the form of mandates requiring data that is collected about or from a country's citizenry must be stored in data centers in-country — a practice referred to as "data localization."

---

[1] The threats involved with pervasive monitoring are in our opinion well described by the drafts: draft-barnes-pervasive-problem-00 and draft-farrell-perpass-attack-04.

We expect to see these kinds of measures evolve to encompass additional mandates beyond data localization. For example, routing mandates — measures to require or prohibit certain routes — could be attractive to policymakers who want to limit the scope of the network topology to which a pervasive attacker has access (e.g., do not route through the UK to avoid the TEMPORA cable taps of the GCHQ[2]). Another possibility, processing mandates, would require certain operations on data to occur within a nation's geographic boundaries (and presumably that country's legal jurisdiction and data protection framework).

If these efforts are successful, for protocol and API designers this means that standards may have to support these kinds of routing, storage and processing mandates. Despite the desire to be jurisdiction agnostic, global standard-setting organizations (SSOs) like the W3C and IETF may find that policies set by governments increasingly affect technical design decisions. These kinds of policies may conflict with fundamental principles of the Internet — for example, the end-to-end principle or principles of the Open Web. Encrypted traffic may need to support unencrypted routing policy metadata to obey routing mandates; server-side storage and computation may need to move to the client depending on the policy of the user's jurisdiction.

B. Dilution of W3C and IETF as Effective Standards Setting Organizations

The US National Institute of Standards and Technology (NIST) has had a particularly difficult time weathering critiques that it collaborates with the NSA to undermine security and cryptography standards. Many in the technical community know and deeply respect the computer security division at NIST, but the probable trapdoor in the Dual_EC_DRBG (NIST SP 800-90) and post-Snowden perceptions — e.g., that the standardization of SHA-3 was influenced to reduce its security level — have had serious reputational consequences for NIST. Indeed, some vendors — e.g., Silent Circle — have removed NIST cryptographic standards from their products or changed the default cipher suites to non-NIST standards, while others — e.g., RSA Security, Inc. — have had to publicly advise their customers not to use a particular encryption algorithm.

It would be prudent for the W3C and IETF to try to avoid similar controversies to the extent possible. The IETF in particular must work to ensure that it listens and responds to critiques from communities outside of the regular IETF membership (without compromising best current practice). We believe that it is in the broader public interest for W3C and IETF to work productively with external groups — civil society, policymakers, and academia.

C. Law Enforcement Interception and Wiretapping

Wiretapping laws exist 1) to discourage and punish unauthorized interception of communications content and metadata; and 2) to authorize law enforcement authorities, with cause and consistent with human rights and due process standards, to intercept communications signals in the process of investigating and prosecuting criminal activity. We have seen how technology has greatly reduced the barriers to — and cost of — performing surveillance. We know now that the amount and scale of signals interception currently occurring

[2] Ewen MacAskill, Julian Borger, Nick Hopkins, Nick Davies and James Ball, "GCHQ taps fibre-optic cables for secret access to world's communications," The Guardian (21 June 2014), *available at:* http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

on global networks is massive and far out of balance with the notion of surveillance being an occasional and last-resort law enforcement tool.

The natural response from the W3C and IETF is to be more careful (for example, to encrypt traffic or protect client-side data). Enabling encryption for future protocol revisions and securing Web interactions will make signals interception much more difficult. A natural reaction from policymakers and law enforcement is to argue that this will aid criminals. Should SSOs consider *not* strengthening the Internet and Web in light of these arguments? No.

We agree with the following statement from draft-farrell-perpass-attack-04: “we cannot defend against the most nefarious actors while allowing monitoring by other actors no matter how benevolent some might consider them to be, since the actions required are indistinguishable from other attacks.” RFC 2804 further supports “freedom from security loopholes.”

SSOs need to be prepared for the argument that strengthening communications security by default will “help the bad guys.” As Internet technologies further diffuse into global society and commerce, it seems rather obvious to technologists that underlying mechanisms must be sound and resilient. The overwhelming balance of value is undoubtedly on the side of securing communications; we need to be able to cleanly articulate and demonstrate that value.

Another consequence of strengthening the Internet is that governments will have to legally obtain through the front door (“downstream” collection by court order) what they had been getting through the back door (“upstream” collection by tapping cables). Service providers that store content in the clear will see more court orders for that content. Some of them will be periodic bulk data requests (e.g., like the daily national telephone calling metadata the NSA receives every day). Some service providers — such as those that are part of the Global Network Initiative — publish periodic reports of the number of law enforcement requests they receive, so this shift from the back door to the front door will be observable. Conduits for end-to-end secure communications that don’t at any time have access to keying material will not be able to meaningfully respond to such requests. However, jurisdictions that have aggressive wiretap-assistance laws that cover Internet technologies — like the UK’s Regulation of Investigatory Powers Act (RIPA) — may demand that software developers build in backdoors, even those developers headquartered in other countries.

D. Control of Illegal, Annoying, or Malicious Content

In a more secure Internet and Web, some methods of controlling and gatekeeping content become impossible or very difficult.[3] How do you bulk-filter spam if all email is end-to-end encrypted? How do you leverage choke points to scan traffic for malware, IP exfiltration, and obscenity? We are eager to learn more at the upcoming workshop about the effects of strengthening the Internet on these types of service.

E. Encryption as a Controlled Export Technology, Subject to IPRs

Some methods used to harden communications move the resulting software into the realm of export-controlled technologies (and possibly patent-controlled). Again, here we are eager to learn more at the workshop about how this might affect code contributors and standards design.

[3] We don’t think it is appropriate for these to reside on public networks, but they are important on private networks.

F. Is There a Need for More Standardization of Anonymity Primitives?

It would seem there are many standards for cryptography and authentication methods, but not many for anonymization techniques. To eventually support users in incredibly hostile network environments, it would seem natural to develop standards for basic reusable methods to anonymize Internet activity — e.g. onion routing as implemented in the Tor software.

II. Opportunities for Technologists' Input into Policy Processes

Finally, in addition to policy implications for standards, there are also important opportunities. It's increasingly important that technologists provide input into the policy process and remain aware of actions by policymakers that might affect their work. For example, in the context of pervasive monitoring, CDT and the Electronic Frontier Foundation (EFF) organized a group of 47 leading technologists from around the world to submit comments last October to President Obama's NSA Review Group.[4] Signatories included many technologists that work regularly within the W3C and IETF.

In our comments we argued that technical expertise is essential for properly understanding the implications of the NSA's surveillance program. We highlighted cases where clearly a lack of technical expertise had lead to massive over-collection of personal data. Finally, we argued that if the US were to truly honor its commitments to civil liberties and privacy, it must recognize the digital rights of non-US persons on the Internet.

When the NSA Review Group's report was released in December, its recommendations included powerful statements siding with technical expertise and strong security. It recognized that the secret Foreign Intelligence Surveillance Court must have technical expertise and that the US should not stockpile software vulnerabilities or undermine encryption and security standards. It further emphasized that an increasingly global Internet environment demands the US rethink how it surveils foreign nationals. The final conclusions of the NSA Review Group report explicitly supported the 47 Technologists' comment. A similar effort focused on DNSSEC was persuasive to the Obama Administration regarding Web-blocking legislation in 2012.[5]

Accessible technical analyses are very persuasive in policy discussions, and we encourage W3C and IETF members to identify opportunities to meaningfully participate. There are a number of NGOs — like CDT — that can help navigate these processes.

III. Conclusion

We look forward to discussing these issues and more at the workshop in London.

[4] Technologists' Comment to the Director of National Intelligence Review Group on Intelligence and Communications Technology, Center for Democracy & Technology (4 October 2013), *available at:* https://www.cdt.org/files/pdfs/nsa-review-panel-tech-comment.pdf.

[5] Steve Crocker, David Dagon, Dan Kaminsky, Danny McPherson, and Paul Vixie, Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the PROTECT IP Bill, (May 2011), *available at:* https://www.cdt.org/files/pdfs/Security-Concerns-DNS-Filtering-PIPA.pdf.