Technologists’ Comment to the Director of National Intelligence Review Group on Intelligence and Communications Technology

4 October 2013

1 Introduction

We write to you as technologists with extensive experience in computer and network security, cryptography and the technology of security and privacy. Your panel, The Director of National Intelligence Review Group on Intelligence and Communications Technologies (“Review Group”), does not have a technologist as a member or official adviser. Accordingly, in this public comment we offer our technical perspective on the substance of your inquiry to better inform your work. After the text of our public comment, we include a list of technical questions we think are essential for the Review Group to seek answers to and incorporate into your analysis.

The Review Group must work from an informed basis on both legal and technical grounds to best fulfill your duties. An informed and competent technical understanding is critical to the oversight function of U.S. Government surveillance programs. A lack of technical understanding in existing oversight bodies has already resulted in substantial material defects in these programs. We believe that protecting sources and methods *by itself* is not a sufficient argument for withholding fundamental technical facts from the oversight process – particularly when those facts can be rationally discussed in an unclassified setting, without compromising sources and methods. Finally, we also write to emphasize that the recent revelations about NSA’s systematic subversion of encryption standards, protocols, software and hardware have a serious impact on the privacy and security of not only U.S. persons and businesses, but all persons and the growing global Internet environment.

2 Independent Technologist Input is Essential

The Review Group needs competent technical advice to do its job properly. The Review Group’s charge is:

> “to advise the President on how, in light of *advancements in technology*, the United States can *employ its technical collection capabilities* in a way that optimally protects our national security and advances our foreign policy while respecting our commitment to privacy and civil liberties, recognizing our need to maintain the public trust, and reducing the risk of unauthorized disclosure.”[1] (emphasis added)

This statement of your charge focuses on both the existing context of advancing technology and an understanding of the U.S.’ technical collection capabilities.

Advancements in technology have created a society that increasingly interacts with information systems to improve their lives. People engage in commerce, social activities, art, politics, business, and health care on scales previously unimaginable by leveraging instantaneous information availability. As these activities now create a vast digital paper trail of transactions and communications, there are significant privacy interests implicated at the moment information is collected and stored by

[1] Press Release, “Statement by the Press Secretary on the Review Group on Intelligence and Communications Technology,” The White House (August 27, 2013), *available at:* http://www.whitehouse.gov/the-press-office/2013/08/27/statement-press-secretary-review-group-intelligence-and-communications-t.

surveillance systems.[2] A technologist can situate advancements in modern technology, how they work, what is possible, how data moves through infrastructure, and how modern technology may implicate privacy and security.

A significantly more difficult challenge is understanding the government's technical collection capabilities. The NSA's surveillance system is broad and deep, encompassing all communication mediums, encrypted or not. What we have learned about this surveillance apparatus shows that it is complex, systemic and state-of-the-art. It encompasses vast collection, targeting, and processing systems as well as powerful technologies such as high-speed Internet filtering appliances, and intrusion techniques such as man-in-the-middle (MITM) attacks using fraudulent X.509 certificates, and the planting of backdoor mechanisms in software and hardware. Technologists have spent this past summer attempting to piece together the details of the NSA surveillance apparatus into a coherent picture with little success. The Review Group will not have much more success in achieving a comprehensive understanding of the surveillance programs without deep technical expertise.

Finally, it is critical that any technical advisors to the review group be independent, and not members of the intelligence community or closely aligned with intelligence community interests. Instead, such analysis demands open, transparent and independent technical input.

3 Technical Understanding is Critical for Oversight of Surveillance Programs

A thorough technical understanding of recently disclosed surveillance programs is critical to proper oversight of these programs, but this technical understanding seems to be lacking in current oversight mechanisms, especially the FISA court ("FISC"). Indeed, the need for more rigorous technical oversight is evident from FISC documents that have been declassified.[3] There are a number of examples where policy has had unintended technical harm.

Technical details are important because they allow bodies charged with oversight to assess the level of intrusiveness and privacy risk of particular techniques and tools. For example, if the FISC had better understood how Multi-Communication Transactions (MCTs)[4] were being acquired, it could have probed into these acquisition techniques and proactively identified the risk that they posed, instead of having to rely on and react to the NSA's identification of its over-collection problem related to MCTs.

Moreover, without an understanding of the technical details of surveillance programs, the FISC has been forced to accept unsupported assertions that the government has made about those programs. For example, consider the government's assertion that "for technological reasons, NSA was not capable of breaking [Multi-Communication Transactions] down into their – and still is not capable – of breaking those down into their individual components."[5] Evaluating the purported inability to separate one embedded targeted communication in a package of many communications depends on understanding technical details of how the NSA implements the surveillance program in question. As technologists, it strikes us as highly unlikely that no reasonable solution exists to overcome the technical hurdle in this

[2] Justin Brookman and G.S. Hans, "Why Collection Matters: Surveillance as a De Facto Privacy Harm," Big Data: Making Ends Meet Conference, The Future of Privacy Forum/Stanford Law School Center for Internet and Society (2013), *available at:* http://www.futureofprivacy.org/wp-content/uploads/Brookman-Why-Collection-Matters.pdf.

[3] October 3, 2011 FISC Opinion, *available at:* https://www.eff.org/document/october-3-2011-fisc-opinion-holding-nsa-surveillance-unconstitutional; Documents governing the interpretation of section 215 of the PATRIOT ACT, *available at*: http://icontherecord.tumblr.com/.

[4] ODNI press conference, August 21, 2013. A transcribed discussion of MCTs appears here: https://www.eff.org/deeplinks/2013/08/intelligence-agency-attorney-explains-how-multi-communication-transactions-allowed.

[5] ODNI press conference, August 21, 2013. Audio recording, *available at:* https://www.eff.org/sites/default/files/odni-call-excerpt.mp3.

example.[6] It is deeply problematic that the court has no way to verify these types of assertions, and that the court is not provided an independent technologist or adviser outside of the intelligence community. Indeed, FISC Chief Judge Reggie Walton has admitted that "the FISC is forced to rely upon the accuracy of the information that is provided to the Court."[7]

There are many examples outside of NSA surveillance where a lack of full technical understanding has resulted in technical failures. The adoption of electronic voting systems after the 2000 Presidential Election did not proceed with significant technical input into the security of those systems, wasting billions of dollars on equipment that was obsolete by 2008.[8] Finally, technologists successfully argued in 2011-2012 that a set of bills designed to censor online copyright infringement would have grave consequences to the healthy operation of the Internet and online transactions.[9] We believe the vacuum of technical input in oversight of the NSA surveillance programs is a similar case, although much more complex.

In order to address this problem, we believe that at a minimum, a transparent adversarial process needs to take place within the FISC, and that the government's adversary as well as the court itself need to have independent technical experts on staff with all the requisite security clearances to be wholly read in to all of the technical details of the NSA surveillance programs. The Review Group must assess the FISC's technical expertise and request that outside, independent technologists who are not part of the intelligence community be incorporated into the FISC structure.

4 Protecting Sources and Methods By Itself is Not a Sufficient Argument to Withhold Technical Information from Oversight

Evidentiary justification must be provided to oversight bodies for claims that particular technical facts must be kept secret out of fear that they may reveal intelligence sources and methods. In many cases, such facts can be rationally discussed in an unclassified setting without compromising sources and methods.[10]

Given the clear public interest in adequate oversight of the surveillance programs that have come to light, the burden of proof must lie with the NSA and intelligence community to rigorously demonstrate the harm of reducing the classification level of materials (including declassification). The mere fact that materials contain technical details does not exempt them from this scrutiny.

While common sense suggests that the NSA has a justified interest in not revealing details about specific investigations – for example, the identities of targets under active investigation – the agency is clearly interested in keeping secret a much broader set of facts under the auspices of "sources and

[6] Alissa Cooper, "The NSA's Laziness Masquerading as Reasonableness," The Center for Democracy & Technology (September 11, 2013) *available at:* https://www.cdt.org/blogs/alissa-cooper/1109nsa%E2%80%99s-laziness-masquerading-reasonableness.

[7] Reggie Walton, reported in the Washington Post, August 15, 2013, *available at*: http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html.

[8] Douglas Jones, and Barbara Simons, Broken Ballots: Will Your Vote Count in the Electronic Age? CSLI Publications, 2012.

[9] 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, technical report (May 2011), *available at:* https://www.cdt.org/files/pdfs/Security-Concerns-DNS-Filtering-PIPA.pdf.

[10] Kenneth W. Dam, & Herbert S. Lin, (Eds.), Cryptography's role in securing the information society, National Academies Press (1996), available at: http://www.nap.edu/readingroom/books/crisis/. ("[classified] details, while necessarily important to policy makers who need to decide tomorrow what to do in a specific case, are not particularly relevant to the larger issues of why policy has the shape and texture that it does today nor to the general outline of how technology will and policy should evolve in the future.").

methods."[11] But this asserted need for more general secrecy regarding technical programs deserves close examination. A mere assertion without evidence that releasing information could harm investigations is simply not sufficient. Technical expertise, especially from scientists, is critical for conducting this analysis and accurately separating what needs to be kept secret from what can reasonably be made public. So far, to our knowledge, no such analysis exists.

5 NSA's Encryption Exploitation Efforts Undermine Security

The previous sections spoke mostly to the need for technical input and the necessary conditions for technical input to be of use in assessing surveillance activities. This section turns to the substance concerning recent highly technical revelations concerning encryption technology.

While many of the revelations over the past summer have implicated issues of law and policy, the reporting from early September focusing on the BULLRUN encryption exploitation program was staggering news for technologists.[12] Activities revealed in these disclosures fundamentally undermine general systems security in dangerous ways. In the NSA's dual role as both an information assurance and signals intelligence entity, clearly the signals intelligence mission has trumped information assurance.

First, it was revealed that the NSA has been working to subvert standards-setting efforts. In one case – the standard random number generator called "Dual_EC_DRBG" – it is widely acknowledged that the NSA planted a "trap door" in the algorithm that allows the agency to decrypt communications that use Dual_EC_DRBG.[13] This not only undermined the efforts of the National Institute of Standards and Technology (NIST) to produce secure cryptographic standards to protect sensitive information on digital systems, but also resulted in massive product recalls and expensive internal audits at businesses to determine if products they had relied on for strong security were in fact quite weak. For example, Dual_EC_DRBG was initially thought to be an obscure random number generator because it is particularly inefficient, but nonetheless it was recently revealed to be the default method of producing random numbers in the RSA Security, Inc. ("RSA") BSAFE cryptographic tools and libraries. BSAFE is a widely used cryptographic toolset and is certified for U.S. Government use. It is unclear how many individual products have been configured with this compromised default and how much encrypted data, communications, and transactions have unknowingly used this insecure cryptographic tool. NIST and RSA have initiated public recalls of the standard and the products that rely on BSAFE and have advised users that they more than likely contain a backdoor. This not only has worked to undermine NIST's credibility but also it has made it easier for those that would spy on business communications that rely on U.S. security tools.

Second, the NSA and its United Kingdom-equivalent, the GCHQ, have apparently engaged in subversion to undermine encryption online. The BULLRUN reporting indicates that NSA and/or GCHQ have hacked into Internet routers and targeted computers to surreptitiously gain access to communications before they are encrypted and to perform man-in-the-middle (MITM) attacks in order to eavesdrop on encrypted communications.[14] The GCHQ reportedly has placed "moles" in technology

[11] James Clapper, statement to Washington Post, published on August 29, 2013, *available at:* http://articles.washingtonpost.com/2013-08-29/world/41570439_1_intelligence-community-washington-post-gaps.

[12] Nicole Perlroth, Jeff Larson, & Scott Shane, "N.S.A. Able to Foil Basic Safeguards of Privacy on Web," The New York Times, A1 (September 5, 2013), *available at:* http://www.nytimes.com/2013/09/06/us/nsa-foils-much-Internet-encryption.html?hp.

[13] Kim Zetter, "How a Crypto 'Backdoor' Pitted the Tech World Against the NSA," Wired.com Threat Level (September 24, 2013), *available at:* http://www.wired.com/threatlevel/2013/09/nsa-backdoor/all/.

[14] See, *Id.*, Perlroth, fn. 12: ("The N.S.A. hacked into target computers to snare messages before they were encrypted."); See, Ryan Gallagher, "New Snowden Documents Show NSA Deemed Google Networks a 'Target'," Slate FutureTense (September 9, 2013), *available at:*

and Internet companies to provide covert access to technical information, simultaneously undermining due process and industry efforts to better protect the privacy of users.[15] To perform MITM attacks, the NSA has reportedly deployed fraudulent X.509 certificates for destinations on the Internet, and it is unclear if this is done with cooperation, by subversion or by legally compelling certificate authorities to issue these certificates.[16] However it has been accomplished, these actions by the NSA severely undermine the Public Key Infrastructure that is used to secure the Internet. This comes at a critical time in the evolution of Internet security: new industries like health care are just starting to put more trust into the security of online systems. It would be disastrous if the NSA's efforts undermined this growing trust in online security.

Finally, the NSA has reportedly worked to covertly and overtly plant backdoors in software and hardware products, undermining the security and privacy of vast swaths of Internet users in an indiscriminate, dragnet manner. Technologists have already commented extensively about why generic backdoors in endpoint systems are unwise and simply will not work.[17] That is, the NSA assumes that it can exploit these weaknesses and gain exclusive access to the content of communications. The reality is that backdoors and covert access mechanisms are fragile and often exploitable by organized criminals, hackers, and the military and intelligence services of other governments, and they can be easily bypassed by using non-vulnerable communication methods.[18] The revelation of these backdoors has already had a negative effect on commerce in the United States, as businesses and users worldwide with a need for secure communications are likely to look outside of the United States for products and services.

6 Our Commitments to Privacy and Civil Liberties Require Recognizing the Interests of Non-U.S. Persons in Online Environments

Part of the Review Group's charge is to evaluate the extent to which the NSA surveillance programs respect "our commitment to privacy and civil liberties." In an increasingly global information environment, these commitments undoubtedly extend to non-U.S. persons. The United Nation's Human Rights Council has resolved that, "the same rights that people have offline must also be

http://www.slate.com/blogs/future_tense/2013/09/09/shifting_shadow_stormbrew_flying_pig_new_snowden_documents_show_nsa_deemed.html, ("The document illustrates with a diagram how [either NSA or GCHQ] appears to have hacked into a target's Internet router and covertly redirected targeted Google traffic using a fake security certificate so it could intercept the information in unencrypted format."). A U.S. Government agency hacking into computers overseas may be illegal: the definition of "protected computer" in the Computer Fraud and Abuse Act covers foreign computers: "the term 'protected computer' means a computer [...] which is used in or affecting interstate or foreign commerce or communication, *including a computer located outside the United States* that is used in a manner that affects interstate or foreign commerce or communication of the United States" 18 USC §1030(e)(2)(B) (emphasis added).

[15] James Ball, Julian Borger, and Glenn Greenwald, "Revealed: how US and UK spy agencies defeat Internet privacy and security," The Guardian (September 5, 2013), available at: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security, ("The GCHQ team was, according to an internal document, 'responsible for identifying, recruiting and running covert agents in the global telecommunications industry.'").

[16] Christopher Soghoian and Sid Stamm, Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL, Financial Cryptography and Data Security '11 March 2011, *available at* http://files.cloudprivacy.net/ssl-mitm.pdf.

[17] Ben Adida, Collin Anderson, Annie I. Anton, Matt Blaze, Roger Dingledine, Edward W. Felten, Matthew D. Green, J. Alex Halderman, David R. Jefferson, Cullen Jennings, Susan Landau, Navroop Mitter, Peter G. Neumann, Eric Rescorla, Fred B. Schneider, Bruce Schneier, Hovav Shacham, Micah Sherr, David Wagner, Philip Zimmermann, CALEA II: Risks of Wiretap Modifications to Endpoints, technical report (May 17, 2013), *available at:* https://www.cdt.org/files/pdfs/CALEAII-techreport.pdf.

[18] Stephanie K. Pell, Jonesing for a Privacy Mandate, Getting a Technology Fix – Doctrine to Follow, North Carolina Journal of Law and Technology, **14**:2, p. 46 (Spring 2013), *available at:* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2262397. ("When compromised, an encrypted communications system with a law enforcement back door is far more likely to result in the catastrophic loss of communications confidentiality than a system that never has access to the unencrypted communications of its users.")

protected online."[19] If U.S. providers of services must ignore the rights of non-U.S. persons due to domestic surveillance obligations, the free flow of information that Internet activities depend upon on will stagnate. On the contrary, if jurisdictions accept – as the United States does at the UN – that all users have some rights to privacy regardless of the user's location, this sets a necessary condition for people of the world to feel comfortable engaging in cross-border Internet activities, upon which the promise of a global connected society rests.

Included in the list of technical questions provided below are questions that the Review Board should ask about how technical parameters are used to determine the "foreignness" of a target. The questions are included because the legal structures that gave rise to NSA surveillance make a distinction between U.S. persons and non-U.S. persons, and therefore part of the public debate about the NSA's activities has turned on issues of foreignness. The inclusion of the foreignness questions below is not meant to imply an endorsement of the disparate treatment that U.S. persons and non-U.S. persons have received under U.S. law.

7 Conclusion

We appreciate the opportunity to provide input to the Review Group as you work to complete your charge. The Review Group must have deep, competent technical expertise. You must also have access to granular technical details to do this work and you must be able to properly situate the technical reality you find behind the veil of secrecy surrounding the surveillance programs. You must recognize that current NSA surveillance activities make everyone less secure and call into question the extent to which human rights translate into the online environment. We are available to provide further input and expertise as needed.

Signed (Affiliations are for identification purposes only):

Ben Adida

Ross Anderson, University of Cambridge

Dan Auerbach, The Electronic Frontier Foundation

Brian Behlendorf, Board Member at EFF, Mozilla, and Benetech

Steven M. Bellovin, Columbia University

Matt Blaze, University of Pennsylvania

Scott Bradner, Harvard University

Eric Burger, Georgetown University

L. Jean Camp, Indiana University

Stephen Checkoway, Johns Hopkins University

Nicolas Christin, Carnegie Mellon University

Alissa Cooper, Center for Democracy & Technology

[19] U.N. Human Rights Council, "Resolution 20: The promotion, protection and enjoyment of human rights on the Internet," A/HRC/20/L.13 (29 June 2012), *available at:* http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G12/147/10/PDF/G1214710.pdf.

Lorrie Faith Cranor, Carnegie Mellon University

Nick Doty, University of California, Berkeley/World Wide Web Consortium

Jeremy Epstein, SRI International

David Evans, University of Virginia

David Farber, Carnegie Mellon University/University of Pennsylvania

Stephen Farrell, Trinity College Dublin

Joan Feigenbaum, Yale University

Edward W. Felten, Princeton University

Bryan Ford, Yale University

Daniel Kahn Gillmor

Matthew D. Green, Johns Hopkins University

J. Alex Halderman, University of Michigan

Joseph Lorenzo Hall, Center for Democracy & Technology

James Hendler, Rensselaer Polytechnic Institute

Nadia Heninger, University of Pennsylvania

David Jefferson, Lawrence Livermore National Laboratory

Micah Lee, Electronic Frontier Foundation

Morgan Marquis-Boire, Citizen Lab, University of Toronto

Siobhan MacDermott, AVG Technologies

Jonathan Mayer, Stanford University

Sascha Meinrath, Open Technology Institute, New America Foundation

Peter G. Neumann, SRI International

M. Chris Riley, Mozilla

Phillip Rogaway, University of California, Davis

Runa A. Sandvik, Independent Researcher

Bruce Schneier, BT

Jeffrey I. Schiller, Massachusetts Institute of Technology

Seth David Schoen, Electronic Frontier Foundation

Micah Sherr, Georgetown University

Christopher Soghoian, American Civil Liberties Union

Ashkan Soltani, Independent Researcher

Brad Templeton, Electronic Frontier Foundation/Singularity University

Dan S. Wallach, Rice University

Nicholas Weaver, International Computer Science Institute

Philip Zimmermann, Silent Circle LLC

Technical Questions About NSA Surveillance

The following is a list of technical questions we feel are important for the Review Group to answer. While we recognize that it may not be possible to disclose all of the technical detail involved in responding to these questions, we think it is essential that the Review Group seeks answers to these questions to technically inform this inquiry and any subsequent recommendations.

1. Reporting has indicated that the NSA acquires private encryption keys. This appears to include in some cases obtaining the private key corresponding to an X.509 certificate, allowing real-time decryption – a passive man-in-the-middle (MITM) attack – of any TLS session protected by that certificate. In another case, the NSA was able to create a fraudulent X.509 certificate that appeared to be valid for Google websites in Brazil, indicating that the agency had either compelled a Certificate Authority to issue a fraudulent X.509 certificate against keying material the NSA created, or that the NSA has obtained the signing keys from one or more Certificate Authorities, allowing the NSA to freely issue its own fraudulent X.509 certificates.
    a. What process is used to acquire these keys?
    b. Is there any hacking of remote servers (obtaining keying material surreptitiously or covertly without authorization or notice of the key holder) or other information systems that takes place to accomplish the acquisition of keying material? Where hacking into systems occurs to obtain keying material, are any of the compromised information systems "used in a manner that affects interstate or foreign commerce or communication of the United States?"[20]
    c. Does the NSA place operatives, analysts, or agents inside U.S. Companies to facilitate surreptitious or covert access to keying material? Does it do so outside the United States? Does it cooperate with the UK's GCHQ in doing this?
2. Across all NSA surveillance programs, how are they audited for precision, accuracy, legal compliance, and benefit of the program?
    a. To what extent do programs feed back information on false positives and false negatives to improve targeting (or similar) logic?
    b. If a particular selector is deemed to be ineffective at predicting relevant activity, is it dropped from the analyst toolkit? Is that data no longer acquired at all?
    c. Predicting rare events – such as earthquakes or terrorist bombings – is known to be a hard problem in machine learning and artificial intelligence. Models for these events can be unscientific or they can be predictive and falsifiable. Does the NSA ensure that only predictive modeling occurs? How are models evaluated if not based on their predictive power?
    d. Evaluating the benefit of anti-terrorist programs is a hard problem. What is the NSA's detailed methodology for measuring this? Are outside economists and experts consulted?
3. How can the public be assured that the vast quantity of information the NSA collects is kept safely? Notably:
    a. Given the need to "connect the dots" easily and analyze the vast quantities of information acquired in NSA's surveillance mission, what mechanisms exist to make sure this surveillance data is technically maintained in a highly-secure manner that

[20] See discussion of the CFAA's definition of "protected computer" at fn. 14.

minimizes the risk of a data breach?

b. To what extent and to what purpose is information on ordinary U.S persons collected? To train algorithms? As "background" data from which suspicious connections should stand out, and hence used on an ongoing basis?

4. We would like to suggest that the Review Group request some specific types of materials (we recognize that these materials may not be publicly disclosable at this time; we believe they are critical for the Review Group to gain a proper understanding of the scope and extent of the NSA surveillance program). Specifically, the Review Group should:

   a. Request and obtain a pseudonymized sample (or even fictitious but comprehensive examples) of every type of communication and signals data that the NSA collects under each of the surveillance programs specified by any applicable control systems under Sensitive Compartmented Information (SCI) designations and any applicable Exceptionally Controlled Information (ECI) designation. This would help to answer questions like:

      i. What is the technical definition of a single communication transaction (SCT) across all programs?

      ii. What is a multiple communication transaction (MCT) across all programs?

   b. Given how there have been many cases where data was over-collected, inappropriately accessed, and analyzed outside of legal authority, technically speaking, how is the NSA surveillance program designed and operated to ensure compliance with legal requirements on collection, analysis, and retention?

      i. What is a "communication" for each program and how does that map onto authorizations to collect and/or analyze data as the term is used by the FISC?

      ii. When the NSA does upstream collection, what exactly does it obtain? For example, it might obtain raw packet dumps, reassembled network flows, entire assembled files, or something else.

      iii. When it obtains communications via PRISM, what is it that it obtains exactly from various different service providers (e.g., entire emails' contents, entire email inboxes or folders with corresponding emails, entire instant messenger/text message chat histories, raw web server logs)?

      iv. What do the telephone call detail records (CDRs) the NSA collects under Section 215 of the USA PATRIOT Act actually contain, field by field?

      v. To what extent is bulk collection or production of cell site location (and, more granularly, cell sector location) or even more fine-grained geolocation events (GPS, Assisted GPS, WiFi-enabled location services, etc.) occurring? What are the parameters of any collection, retention and analysis of geolocation information, including fidelity/resolution limits, time-domain resolution, retention of these records, scope of the public (both U.S. and non-U.S. persons) affected by such activities?

5. In upstream acquisition, which we believe happens in real-time:

   a. How many identifiers are on the list that is used to conduct to/from/about acquisition? (note: identifiers, not targets) What are the identifiers?

   b. What technical limitations prevent subsequent minimization after upstream acquisition but before transit and storage? (limitations were cited before the FISC in the MCT case as being a substantial and impermeable barrier to adequately minimizing MCTs)

c. In what other contexts in the NSA surveillance programs are there technical barriers, difficulties, and other issues that result in either over-collection (over-acquisition) or inadequate minimization?

6. On foreignness:

   a. What technical parameters are used to determine “foreignness”?

   b. How are these technical parameters used? Are they regularly updated/refined based on information from analyses that indicate false positives and/or false negatives?

   c. Is any effort made to conservatively estimate the location of a potential surveillance target when there are indications that they may be using a proxy service, the Tor network, or a VPN? (e.g., is it easy for a foreigner to simply pick a VPN service that exits out of the United States to avoid surveillance and acquisition of their communications?) Similarly, would a U.S. person who exits out of a foreign country while using, e.g., the Tor anonymity software be targeted without any recognition that Tor users seek to strengthen their privacy online and that any given user may, in fact, be a U.S. person?