Fall 2015

Taxonomy of the Snowden Disclosures

Margaret Hu

Taxonomy of the Snowden Disclosures

Margaret Hu*

Abstract

This brief Essay offers a proposed taxonomy of the Snowden Disclosures. An informed discussion on the legality and constitutionality of the emerging cybersurveillance and mass dataveillance programs revealed by former NSA contractor Edward Snowden necessitates the furtherance of cybersurveillance aptitude. This Essay contends, therefore, that a detailed examination of the Snowden disclosures requires not just a careful inquiry into the legal and constitutional framework that guides the oversight of these programs. A close interrogation also requires a careful inquiry into

---

* Assistant Professor of Law, Washington and Lee School of Law. I would like to extend my deep gratitude to those who graciously offered comments on this draft, or who offered perspectives and expertise on this research on big data cybersurveillance through our thoughtful discussions: Jack Balkin, Kate Bartlett, danah boyd, Guy Charles, Bobby Chesney, Andrew Christensen, Danielle Citron, Geoff Corn, Jennifer Daskal, Nora Demleitner, Charlie Dunlap, Josh Fairfield, Mark Graber, David Gray, Woody Hartzog, Trina Jones, Brett Max Kaufman, Orin Kerr, J.J. Kidder, Sandy Levinson, Rachel Levinson-Waldman, Erik Luna, Tim MacDonnell, Peter Margulies, Russ Miller, Steve Miskinis, Brian Murchison, Richard Myers, Jeff Powell, Jed Purdy, Mark Rush, Hina Shamsi, Dan Tichenor, Patrick Toomey, Chris Slobogin, Steve Vladeck, Russ Weaver, Ben Wittes, and apologies to those whom I may have inadvertently failed to acknowledge. In addition, this research benefited greatly from the discussions generated from the 2015 AALS National Conference, National Security Law Section, Call for Papers, National Security Surveillance Panel; Washington and Lee University School of Law, 2015 Law Review Symposium, "Cybersurveillance in the Post-Snowden Age"; 2015 International Privacy Discussion Forum hosted by Paris-Sorbonne University in Paris, France; University of Freiburg, KORSE Centre for Security and Society, "Privacy and Power: Transatlantic Dialogue in the Shadow of the NSA-Affair" Symposium in Freiburg, Germany; "Transnational Dialogue on Surveillance Methods," hosted by Max Planck Institute in Freiburg, Germany; 2013 "Politics of Surveillance" Symposium, hosted by the Wayne Morse Center for Law and Politics at the University of Oregon School of Law. Much gratitude to the excellent editorial care of the *Washington and Lee Law Review*, including Jennifer Commander, Editor-in-Chief; Claire Leonard, Managing Editor; and Paul Judge, Lead Articles Editor. Many thanks to the research assistance of Lauren Bugg, Russell Caleb Chaplain, Jessica Chi, Katherine Dickinson, Maureen Edobor, Joshua Hock, Andrew House, Cadman Kiker, Kirby Kreider, Bobby Martin, Oscar Molina, Markus Murden, Madeline Morcelle, Kelsey Peregoy, Joe Silver, and Cole Wilson. All errors and omissions are my own.

the big data architecture that guides them. This inquiry includes examining the underlying theories of data science and the rationales of big data-driven policymaking that may drive the expansion of big data cybersurveillance. These technological, theoretical, and policymaking movements are occurring within what has been termed by scholars as the National Surveillance State. Better understanding the manner in which intelligence gathering may be shifting away from small data surveillance methods and toward the adoption of big data cybersurveillance methods—and assessing the efficacy of this shift—can factually ground future debates on how best to constrain comprehensive and ubiquitous surveillance technologies at the dawn of the National Surveillance State.

Table of Contents

I. Introduction

This brief Essay offers a proposed taxonomy of the Snowden disclosures[1] to help situate these programs within the theory of the "National

1. *See generally* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014) (discussing in detail the history of the Snowden disclosures). For more information, see *Documents*, GLENN GREENWALD http://glenngreenwald.net/#BookDocuments (last visited Nov. 4, 2015) (providing further information on the disclosures in *No Place To Hide*) (on file with the Washington and Lee Law Review). *See also* Jon L. Mills, *The Future of Privacy in the Surveillance Age*, *in* AFTER SNOWDEN: PRIVACY, SECRECY, AND SECURITY IN THE INFORMATION AGE 191 (Ronald Goldfarb ed., 2016) (discussing the Snowden disclosures).

Surveillance State."[2] An informed discussion on the legality and constitutionality of the emerging cybersurveillance[3] and mass dataveillance[4] programs revealed by former NSA contractor Edward Snowden necessitates the furtherance of cybersurveillance aptitude. Specifically, a technological grounding of these emerging surveillance methods is needed to assess

---

2. *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 12 (2008) (explaining that the National Surveillance State is a "rich" place for the government to obtain information); Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489, 520–21 (2006) (discussing the importance of the National Surveillance State in "American constitutionalism" and how the National Surveillance State is identified by an increase of resources dedicated to technology and promoting domestic security); s*ee also* EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 5 (2014) [hereinafter PODESTA REPORT], https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf ("[D]ata collection and analysis is being conducted at a velocity that is increasingly approaching real time, which means there is a growing potential for big data analytics to have an immediate effect on a person's surrounding environment or decisions being made about his or her life.") (on file with the Washington and Lee Law Review).

3. *See, e.g.*, LAWRENCE LESSIG, CODE VERSION 2.0 209 (2006) (describing cybersurveillance or "digital surveillance" as "the process by which some form of human activity is analyzed by a computer according to some specified rule. . . . [T]he critical feature in each [case of surveillance] is that a computer is sorting data for some follow-up review by some human"). Several important works have been published in recent years, shedding light on mass surveillance technologies, and the policy and programmatic framework of cybersurveillance and covert intelligence gathering. *See generally, e.g.*, PRIVACY AND POWER: A TRANSATLANTIC DIALOGUE IN THE SHADOW OF THE NSA-AFFAIR (Russell A. Miller ed.) (forthcoming); JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 17–18 (2014); SHANE HARRIS, @WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX (2014); JOHN GILLIOM & TORIN MONAHAN, SUPERVISION: AN INTRODUCTION TO THE SURVEILLANCE SOCIETY (2013); SIMON CHESTERMAN, ONE NATION UNDER SURVEILLANCE: A NEW SOCIAL CONTRACT TO DEFEND FREEDOM WITHOUT SACRIFICING LIBERTY (2011); DANA PRIEST & WILLIAM M. ARKIN, TOP SECRET AMERICA: THE RISE OF THE NEW AMERICAN SECURITY STATE (2011); SHANE HARRIS, THE WATCHERS: THE RISE OF AMERICA'S SURVEILLANCE STATE (2010); ROBERT O'HARROW, JR., NO PLACE TO HIDE (2006); JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE (2004).

4. Roger Clarke is attributed with introducing the term "dataveillance." *See* Roger A. Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498, 499 (1988) (describing dataveillance as the systematic monitoring or investigation of people's actions, activities, or communications through the application of information technology); *see also* DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW 16 (2007) ("Being much cheaper than direct physical or electronic surveillance [dataveillance] enables the watching of more people or populations, because economic constraints to surveillance are reduced. Dataveillance also automates surveillance. Classically, government bureaucracies have been most interested in gathering such data . . . .").

reasonableness in the Fourth Amendment analysis[5] and to assess efficacy and legality under various statutory provisions guiding restrictions on intelligence gathering activities.[6]

---

5. *See* U.S. CONST. amend. IV

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

6. Scholars and experts have focused careful attention on the legal implications of the mass surveillance activities of the NSA and the intelligence community in work both preceding and following the disclosures of former NSA contractor Edward Snowden. *See, generally*, William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633 (2010) (arguing that FISA has become too rigid to adapt to evolving threats and provide speedy surveillance); Anjali S. Dalal, *Shadow Administrative Constitutionalism and the Creation of Surveillance Culture*, 2014 MICH. ST. L. REV. 59 (2014) (arguing that government agencies have added to the growth of the culture of surveillance by shifting the bounds of acceptable behavior); Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* 37 HARV. J.L. & PUB. POL'Y 757 (2014) (providing the basis for Congress passing FISA and arguing that the current bulk collection program violates this Act); Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content,* 38 HARV. J.L. & PUB. POL'Y 117 (2015) (tracing the history of surveillance programs in the United States and exploring the constitutionality of Section 702 of FISA); Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465 (2015) (arguing that the rise of surveillance has certain effects that implicate the theories behind the First Amendment); Orin S. Kerr, *A Rule of Lenity for National Security Surveillance Law*, 100 VA. L. REV. 1513 (2014) (arguing that Congress should adopt a rule of lenity that would favor the citizen over the State in interpreting surveillance statutes); Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden*, 66 HASTINGS L.J. 1 (2014) (arguing that the programs disclosed by Snowden are legal but calling for greater transparency and accountability following Snowden's disclosures); Paul Ohm, *Electronic Surveillance Law and the Intra-Agency Separation of Powers*, 47 U.S.F. L. REV. 269 (2012) (conducting an institutional analysis of electronic surveillance by arguing for the use of an internal separation of powers); Nathan A. Sales, *Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy*, 10 I/S: J.L. & POL'Y INFO. SOC'Y 523 (2014) (exploring the legality of NSA surveillance programs); Margo Schlanger, *Intelligence Realism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L SEC. J. 112 (2015) (arguing that the NSA's mentality in compliance terms is attributable to intelligence legalism); Christopher Slobogin, *Cause to Believe What? The Importance of Defining a Search's Object—Or, How the ABA Would Analyze the NSA Metadata Surveillance Program*, 66 OKLA. L. REV. 725 (2014) (exploring how the demise of a search's object can raise Fourth Amendment implications both generally and in the context with the NSA's information-gathering program); Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721 (2014) (arguing for the possibility of applying administrative law principles to law principles by

Jack Balkin and Sanford Levinson define the National Surveillance State as being "characterized by a significant increase in government investments in technology and government bureaucracies devoted to promoting domestic security and (as its name implies) gathering intelligence and surveillance using all of the devices that the digital revolution allows."[7] The National Surveillance State, like the administrative state, is largely bureaucratized.[8] Thus, through bureaucratized decision making that may bypass traditional constitutional protections,[9] the National Surveillance State harnesses the technologies of big data[10] and the Information Society, and integrates

---

relying on the rise of the surveillance state); Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951 (2006) (arguing that information sharing is critical and exploring the implications of mass information sharing); Omer Tene, *A New Harm Matrix for Cybersecurity Surveillance*, 12 COLO. TECH. L.J. 391 (2014) (proposing parameters for analysis of the privacy impact of communications monitoring programs); Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 SANTA CLARA L. REV. 843 (2014) (arguing that as the rise of the surveillance state continues, notice, an essential restrain on illegal searches, is disappearing); Stephen I. Vladeck, *Big Data Before and After Snowden*, 7 J. NAT'L SEC. L. & POL'Y 333 (2014) (comparing a panel discussion on big data before Snowden's disclosures and hypothesizing how the discussion would unfold after the disclosures); Stephen I. Vladeck, *Standing and Secret Surveillance*, 10 I/S J.L. & POL'Y INFO. SOC'Y 551 (2014) (exploring the Supreme Court's response to secret surveillance programs); John Yoo, *The Legality of the National Security Agency's Bulk Data Surveillance Programs*, 37 HARV. J.L. & PUB. POL'Y 901 (2014) (arguing that the current NSA surveillance programs do not violate the Fourth Amendment).

7. Balkin & Levinson, *supra* note 2, at 520–21.

8. *See* Balkin, *supra* note 2, at 4 ("The National Surveillance State is a permanent feature of governance, and will become as ubiquitous in time as the familiar devices of the regulatory and welfare states.").

9. *See* Balkin & Levinson, *supra* note 2, at 525–26 ("If the information gleaned from the government's national security wing is transferred over to its law enforcement wing . . . law enforcement will be transformed into increasing surveillance of ordinary Americans to prevent not only the most serious threats to national security, but also everyday crimes . . . ."); Joshua A.T. Fairfield & Erik Luna, *Digital Innocence,* 99 CORNELL L. REV. 981, 986 (2014) (explaining the potential for exoneration through the use of mass data collection to prevent and correct wrongful criminal convictions).

10. "Big data" is difficult to define, as it is a newly evolving field, and the technologies that it encompasses are evolving rapidly as well. *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1920–21 (2013) ("'Big Data' is . . . a technology and a process. The technology is a configuration of information-processing hardware capable of sifting, sorting, and interrogating vast quantities of data . . . . The process involves mining the data for patterns, distilling the patterns into predictive analytics, and applying the analytics to new data."). Multiple authors have addressed the characteristics of "big data" and the challenges posed by big data technologies. *See, e.g.*, Neil M. Richards & Jonathan

surveillance into day-to-day governance activities.[11] This governance is often justified by ex ante and pre-crime objectives—for example, the need to prevent perceived criminal and terroristic threats.[12]

Balkin and Levinson have identified the National Surveillance State as an important concern of American constitutionalism that uniquely impacts core democratic principles.[13] Similarly, Glenn Greenwald and Laura Poitras—who enjoy sole possession of the full Snowden archives[14]—explain that the Snowden disclosures profoundly implicate questions of

---

H. King, *Big Data Ethics*, 49 WAKE FOREST L. REV. 393, 394 n.3 (2014) (discussing the relevance of *IT Glossary: Big Data*, GARTNER, http://www.gartner.com/it-glossary/big-data/ (last visited May 11, 2015) (on file with the Washington and Lee Law Review)); *id.* (citing the original "3-V" big data report, Doug Laney, *3D Data Management: Controlling Data Volume, Velocity, and Variety*, GARTNER (Feb. 6, 2001), blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf (last visited Sept. 18, 2015) (arguing that current business conditions are giving rise to more formalized approaches to data management principles) (on file with the Washington and Lee Law Review)). *See generally* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT (Julia Lane et al. eds., 2014) (defining and discussing the "big data" phenomenon); JULES J. BERMAN, PRINCIPLES OF BIG DATA: PREPARING, SHARING, AND ANALYZING COMPLEX INFORMATION (2013) (same); Danah Boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, 15 INFO., COMM. & SOC'Y 662 (2012) (same); ROB KITCHIN, THE DATA REVOLUTION: BIG DATA, OPEN DATA, DATA INFRASTRUCTURES & THEIR CONSEQUENCES (2014) (same); VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013) (same).

11. *See* Balkin & Levinson, *supra* note 2, at 523 (explaining that "information [is] ever more valuable to governments; this causes governments to invest even more heavily in the collection, storage, and collation of data").

12. *See id.* at 526 ("[T]he government will be tempted to move increasingly from investigation and arrest after crimes occur to surveillance, prevention, and interception before crimes occur."); *see also* Jennifer C. Daskal, *Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention*, 99 CORNELL L. REV. 327, 331 (2014) (explaining that precrime "restrictions share common features: they are targeted at particular individuals, entities, or categories of individuals; they impose noncustodial restrictions; and they are preventive in both purpose and effect"); David Cole, *The Difference Prevention Makes: Regulating Preventive Justice*, CRIM. & PHIL. (Mar. 25, 2014), http://link.springer.com/article/10.1007/s11572-013-9289-7/fulltext.html (last visited Dec. 8, 2015) (characterizing "the post-9/11 full-scale adoption of a paradigm of prevention" as "a sea change") (on file with the Washington and Lee Law Review).

13. *See* Balkin & Levinson, *supra* note 2, at 520 ("One of the most important developments in American constitutionalism is the gradual transformation of the United States into a National Surveillance State.").

14. *See* GREENWALD, *supra* note 1, at 7–89 (discussing in detail the history of the Snowden disclosures, including how and why Snowden invited Greenwald and Poitras to possess and disseminate the Snowden files).

democratic governance.[15] It is within this much larger frame of discussion that the importance of the Snowden disclosures can be better understood and appreciated.[16] However, this appreciation is inadequate so long as the Snowden disclosures are referred to in the abstract.[17]

From June 5, 2013, until the present,[18] hundreds of formerly covert programs have been revealed to the public through the disclosures of

---

15. *See id.* at 6 ("[Snowden] has made it clear, with these disclosures, that we stand at a historic crossroads. Will the digital age usher in the individual liberation and political freedoms that the Internet is uniquely capable of unleashing? Or will it bring about a system of omnipresent monitoring and control . . . ?"); CITIZENFOUR (Praxis Films 2014) (featuring interviews with Snowden); Peter Maass, *The Intercept's Laura Poitras Wins Academy Award for 'Citizenfour'*, THE INTERCEPT (Feb. 22, 2015), https://firstlook.org/theintercept/2015/02/22/poitras-wins-oscar-for-citizenfour/ (last visited Dec. 7, 2015) ("'The disclosures that Edward Snowden revealed don't only expose a threat to our privacy but to our democracy itself,' Poitras said in her acceptance speech [at the 87th Academy Awards, immediately after Poitras received the Oscar for Best Documentary Feature for directing Citizenfour].") (on file with the Washington and Lee Law Review); RACHEL LEVINSON-WALDMAN, BRENNAN CTR. FOR JUSTICE, WHAT THE GOVERNMENT DOES WITH AMERICANS' DATA 9 (2013) ("The collection and retention of non-criminal information about Americans for law enforcement and national security purposes poses profound challenges to our democracy and our liberties."); s*ee also* Balkin & Levinson, *supra* note 2, at 520 ("One of the most important developments in American constitutionalism is the gradual transformation of the United States into a National Surveillance State.").

16. *See* GREENWALD, *supra* note 1, at 169 ("[Snowden's revelations] triggered an intense, sustained worldwide debate precisely because the surveillance poses such a grave threat to democratic governance.").

17. *See id.* at 208–09 ("While the government, via surveillance, knows more and more about what its citizens are doing, its citizens know less and less about what their government is doing, shielding as it is by a wall of secrecy.").

18. The Snowden disclosures were launched on June 5, 2013, and June 6, 2013, by Glenn Greenwald and Laura Poitras, respectively, the only two individuals who possess the full Snowden archives. The first Snowden disclosure on the NSA's bulk telephony metadata collection program was revealed by Greenwald in *The Guardian*; the second Snowden disclosure on the NSA's PRISM program was revealed by Barton Gellman and Laura Poitras in *The Washington Post*. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (last visited Sept. 6, 2015) ("The National Security Agency is currently collecting the telephone records of millions of US customers of Verizon, one of America's largest telecoms providers, under a top secret court order issued in April.") (on file with the Washington and Lee Law Review); Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program,* WASH. POST (June 7, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (last visited Sept. 18, 2015) ("The National Security Agency and the FBI are tapping directly into the central servers of nine leading U.S. Internet companies,

National Security Agency (NSA) contractor Edward Snowden.[19] As the disclosures continue to be revealed by various news organizations, the full scope of the revelations is, as of yet, still unknown.[20] To help grapple with the specific contours of the technological, scientific, theoretical, and policy developments that animate the National Surveillance State, this Essay offers an Appendix of several hundred of the programs that now comprise what we refer to collectively and abstractly in the public discourse as "the Snowden disclosures" or "the Snowden revelations."[21]

As part of the Symposium, *Cybersurveillance in the Post-Snowden Age*, this taxonomical effort relies exclusively upon publicly available sources. The public has been granted access to more classified documents relating to covert intelligence activities than ever before by virtue of the Snowden disclosures, media and investigative reports, and national security revelations through other intelligence sources. Nonetheless, this piece and proposed taxonomy might be considered best as a thought experiment, as cybersurveillance research is necessarily constrained in its conclusions and restricted to the information available, which is, of course, incomplete due the covert nature of the programs.

The reader should be careful to note the age of this information. The Appendix does not detail the NSA's current capacities, but, rather, the capacities when Snowden went public. Many of the Snowden documents reference programs and their status as of 2010 to 2012. This Appendix also does not purport to be a comprehensive list of all of the Snowden disclosures. Neither should the categories offered here be viewed as definitive and inflexible classifications. The criteria used for inclusion in one category over another was based upon a certain degree of speculation, depending upon the information available, and in many instances, it appeared that a program could fall within more than one category.

Rather, this work is a good faith attempt to compile the documents that have been made available in the aftermath of the Snowden disclosures from June 2013 until January 2015, and to find a method to classify the hundreds of individualized programs included within these

---

extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets, according to a top-secret document obtained by The Washington Post.") (on file with the Washington and Lee Law Review).

19. *See* Toomey & Kaufman, *supra* note 6, at 844 (describing the amount of NSA disclosures as a "cascade" of information).

20. *See* GREENWALD, *supra* note 1, at 53 (describing Snowden's preference to publish the leaked documents "journalistically" rather than in bulk to allow the public to process the information in a more efficient way).

21. *Infra* App. at 45.

documents. This descriptive effort serves longer-term research aims, including future scholarship on the legality and constitutionality of the Snowden disclosures. For this Essay, however, the ambition is more modest: an attempt to take stock of the current Snowden disclosures through the measure of an initial categorical evaluation and a proposed system of classification, even if such an effort may be incomplete or speculative at this juncture.

Each part of the Essay briefly describes the system of classification used to categorize the Snowden disclosures that have been included in the Appendix. The proposed system of classification articulated here draws heavily upon Greenwald's description of cybersurveillance architecture as set forth in *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. The specific documents from the Snowden disclosures as revealed by Greenwald, Poitras, and others, have been examined for how best to give form to what was previously formless: the technological and e-programmatic structure of the covert intelligence activities of the National Surveillance State. David Cole, in reviewing Greenwald's book, notes that: "In one remarkable [NSA] slide presented at a 2011 meeting of five nations' intelligence agencies and revealed here for the first time, the NSA described its 'collection posture' as 'Collect it All,' 'Process it All,' 'Exploit it All,' 'Partner it All,' 'Sniff it All' and, ultimately, 'Know it All.'"[22]

This Essay proceeds in five parts. The taxonomy offered below is an attempt to categorize the programs revealed by the Snowden disclosures into one of five categories: Part II briefly describes collection programs ("Collect It All"); Part III briefly describes processing programs ("Process It All"); Part IV briefly describes attack programs ("Exploit It All"); Part V briefly describes isolation programs ("Sniff It All"); and Part VI briefly describes database programs ("Partner It All" and "Know It All"). Each type of program is defined in more detail in the discussion below. In the Appendix, some programs are listed as "Unknown" where there is insufficient information to classify the program.

Through this proposed taxonomy of the Snowden disclosures, the research effort of this Essay strives to illustrate how we are witnessing a historically significant transition from small data surveillance methods to

---

22. David Cole, *'No Place to Hide' by Glenn Greenwald, on the NSA's Sweeping Efforts to 'Know It All'*, WASH. POST (May 12, 2014) https://www.washingtonpost.com/opinions/no-place-to-hide-by-glenn-greenwald-on-the-nsas-sweeping-efforts-to-know-it-all/2014/05/12/dfa45dee-d628-11e3-8a78-8fe50322a72c_story.html (last visited Sept. 18, 2015) (on file with the Washington and Lee Law Review); GREENWALD, *supra* note 1, at 97 (citing an NSA slide from Snowden disclosures titled, "New Collection Posture," quoting NSA data collection procedure as "Collect It All").

big data cybersurveillance methods.[23] The big data revolution is not only technological in nature, but, as several experts have observed, is an epistemological and ontological revolution as well.[24] The manner in which big data impacts philosophies of knowledge acquisition and human perception necessarily impacts government decisionmaking and bureaucratized protocols.[25] As the government increasingly capitalizes on big data tools, the revolution of big data governance has also led to a revolution in contemporary cybersurveillance policies and practices, as can be witnessed by the Snowden disclosures. The Essay concludes that, when evaluating the propriety of the deployment of big data cybersurveillance tools by the Intelligence Community, special attention must be placed on big data. Recognizing the technological significance of big data as a scientific, theoretical, and philosophical axis underlying the

---

23. *See, e.g.*, Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773, 803–05 (2015) (following the Snowden disclosures, at least one expert has asserted that the NSA is attempting to merge big data tools with small data tools); Kate Crawford, *The Anxieties of Big Data*, NEW INQUIRY (May 30, 2014), http://thenewinquiry.com/essays/the-anxieties-of-big-data/ (last visited Sept. 18, 2015)

> [A Squeaky Dolphin PowerPoint slide from the Snowden disclosures] outlines an expansionist program to bring big data together with the more traditional approaches of the social and humanistic sciences: the worlds of small data. . . . [I]t is all about supplementing [big] data analysis with broader sociocultural tools . . . .

(on file with the Washington and Lee Law Review). Scholars and experts have also juxtaposed small data policing and surveillance practices with big data policing and surveillance practices as a way to deepen the legal and constitutional discourse. *See, e.g.*, Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 329 (2015) (discussing what happens if particularized small data suspicion is replaced by big data suspicion in the context of predictive policing practices); Toomey & Kaufman, *supra* note 6, at 847 (describing a "notice paradox" whereby in a small data surveillance world notice was usually given because searches were limited to a "physical world," whereas big data surveillance methods provided the government significant control over when, and to whom, notice is given).

24. *See* Cohen, *supra* note 10, at 1920–21 ("Together, the technology and the process [of big data] comprise a technique for converting data flows into a particular, highly data-intensive type of knowledge."); danah boyd & Kate Crawford, *Critical Questions for Big Data: Provocations for a Cultural, Technological, and Scholarly Phenomenon*, 15 INFO., COMM. & SOC'Y 662, 662–79 (2012) (discussing how big data creates new forms of knowledge and the processes by which we produce knowledge and perception).

25. *See generally, e.g.*, Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1 (2008) [hereinafter Balkin, *National Surveillance State*]; Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489 (2006); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

programs revealed by the Snowden disclosures presents critical foci for future legal and constitutional analysis.[26]

II. "Collect It All": Collection Programs

From the Snowden disclosures, it appears that collection programs are used to gather information from a wide range of sources, including the content of communications (traditional wiretapping), non-content of communications (metadata of phone records, such as the time and duration of a call, but not the conversation of the call), and the non-content of non-communications, but, digital data generated through social media (data points of a digital photograph taken from the internet for potential facial recognition technology use).[27] These programs can incorporate big data collection, small data collection, or both.[28] Some programs exhibit a physical element, such as hardwiring into a fiber

---

26. *See, e.g.*, Hu, *supra* note 23, at 803–05 (following the Snowden disclosures, at least one expert has asserted that the NSA is attempting to merge big data tools with small data tools). *See generally* Crawford, *supra* note 23. Scholars and experts have also juxtaposed small data policing and surveillance practices with big data policing and surveillance practices as a way to deepen the legal and constitutional discourse. *See, e.g.*, Ferguson, *supra* note 23, at 329 (discussing what happens if particularized small data suspicion is replaced by big data suspicion in the context of predictive policing practices); Toomey & Kaufman, *supra* note 6, at 847 (describing a "notice paradox" whereby in a small data surveillance world notice was usually given because searches were limited to a "physical world," whereas big data surveillance methods provided the government significant control over when, and to whom, notice is given).

27. *See, e.g.*, Charlie Savage, *Government Declassifies 2007 Surveillance Court Rulings*, N.Y. TIMES, (Jan. 26, 2015), http://www.nytimes.com/interactive/2015/01/27/us/27-fisc-foia-documents.html (last visited Nov. 23, 2015) (citing Memorandum of Law in Support of Application for Authority to Conduct Electronic Surveillance, U.S. Foreign Intelligence Surveillance Court (Dec. 12, 2005), https://assets.documentcloud.org/documents/1509488/nyt-savage-foia-fisc-may-august-2007-orders.pdf) (on file with the Washington and Lee Law Review)); Charlie Savage, *Documents Show N.S.A.'s Wiretap Moves Without Congress's Approval*, N.Y. TIMES, (Jan. 27, 2015), http://www.nytimes.com/2015/01/28/us/documents-show-nsas-wiretap-moves-before-congresss-approval.html?_r=0 (last visited Nov. 23, 2015) (on file with the Washington and Lee Law Review); Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (last visited Nov. 23, 2015) (on file with the Washington and Lee Law Review); James Risen & Laura Poitras, *N.S.A. Collecting Millions of Faces From Web Images*, N.Y. TIMES (May 31, 2014), http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html (last visited Nov. 23, 2015) (on file with the Washington and Lee Law Review).

28. Following the Snowden disclosures, at least one expert has asserted that the NSA is attempting to merge big data tools with small data tools. Crawford, *supra* note 23.

connection at a major hub.[29] Others gather data from telecommunication or software companies.[30]

The "Collect-It-All" theory of covert cybersurveillance appears to be driven by a historical dimension as well as a modern technological dimension. On one hand, a "collect-it-all" approach in a small data world was a deeply-rooted, historical precept of intelligence gathering. As David Pozen explains, "[A] basic precept of intelligence gathering . . . [is that] [d]isparate items of information, though individually of limited or no utility to their possessor, can take on added significance when combined with other items of information."[31] At the same time, the theory and science of big data requires a "collect-it-all" approach in a big data world.[32] The algorithmic intelligence of big data tools drives incentives for comprehensive and ubiquitous data collection for big data accuracy purposes.[33] As one intelligence official explained, "[e]verybody's a target; everybody with [digital] communication is a target."[34] From the Snowden disclosures, it appears that a big data "target" is not a small data "target." Under traditional surveillance methods that tracked and intercepted traditional communications, a small data "target" was akin to a suspect or a known or suspected terrorist, for example. In contrast, from the Snowden disclosures, it appears that a big data "target" is a digital data target. Under big data cybersurveillance architecture, big data tools appear to track and isolate suspicious data and not suspicious persons. Thus, "everybody's a target; everybody with [digital] communications is a

29. Craig Timberg, *NSA Slide Shows Surveillance of Undersea Cables*, WASH. POST (July 10, 2013), https://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html (last visited Nov. 23, 2015) ("A classified NSA slide obtained by The Washington Post . . . shows a separate category [of data collection] labeled 'Upstream,' described as accessing 'communications on fiber cables and infrastructure as data flows past . . . .'") (on file with the Washington and Lee Law Review).

30. T.C. Sottek & Joshua Kopstein, *Everything You Need to Know About PRISM*, THE VERGE (July 17, 2013, 1:36 PM), http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet (last visited Nov. 23, 2015) ("PRISM is considered a highly classified program that allows the National Security Agency and Federal Bureau of Investigation to retrieve data directly from Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple.") (on file with the Washington and Lee Law Review).

31. David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act,* 115 YALE L.J. 628, 630 (2005).

32. GREENWALD, *supra* note 1, at 95.

33. Sottek & Kopstein, *supra* note 30.

34. *See generally* BAMFORD, THE PUZZLE PALACE: INSIDE THE NATIONAL SECURITY AGENCY, AMERICA'S MOST SECRET INTELLIGENCE ORGANIZATION (1982).

target" of the Intelligence Community by historical, theoretical, and technological default.

In other words, "collect-it-all" big data cybersurveillance and mass dataveillance tools are in the process of transforming into a "connect-the-dots" theory of intelligence gathering. Rachel Levinson-Waldman explains the "connect-the-dots" theory of big data cybersurveillance and mass dataveillance this way: "One chief argument in favor of retaining all information gathered, regardless of its apparent law enforcement value, is that seemingly innocuous information may prove meaningful today or in the future when connected with other 'dots' of information."[35] Multiple leaders in the intelligence community, including Gus Hunt, Chief Technology Officer of the CIA, have used this theory:

> The value of any piece of information is only known when you can connect it with something else that arrives at a future point in time[.] Since you can't connect dots you don't have, it drives us into a mode of, we fundamentally try to collect everything and hang on to it forever.[36]

Former NSA Director, General Keith Alexander, similarly used the "connect-the-dots" theory to justify NSA cybersurveillance programs after the Snowden disclosures.[37] The process of combining these dots into a pattern that suggests terrorist activity is generally called data mining, or "pattern prediction": analyzing a store of data to tease out patterns connected to certain behaviors, and then looking for matching patterns in other datasets in order to predict other instances in which those behaviors are likely to occur.[38]

Consequently, both the historical precepts of small data intelligence gathering and big data cybersurveillance systems appear to be dependent upon a "collect-it-all" approach or a "connect-the-dots" theory of mass surveillance.[39] This new approach to intelligence gathering is highly

---

35. LEVINSON-WALDMAN, *supra* note 15, at 17 (citing Pozen, *supra* note 31, at 630–31).

36. Matt Sledge, *CIA's Gus Hunt on Big Data: We 'Try to Collect Everything and Hang onto It Forever*,*'* HUFFINGTON POST (Mar. 20, 2013), http://www.huffington post.com/2013/03/20/ cia-gus-hunt-big-data_n_2917842.html (last visited Sept. 6, 2015) (on file with the Washington and Lee Law Review).

37. *See Collect It All: America's Surveillance State*, ALJAZEERA (Nov. 7, 2013), http://www.aljazeera.com/programmes/faultlines/2013/11/collect-it-all-america-surveillance-state-20131158358543439.html (last visited Sept. 6, 2015) (showing video of General Alexander justifying the NSA cybersurveillance programs) (on file with the Washington and Lee Law Review).

38. LEVINSON-WALDMAN, *supra* note 15, at 17.

39. *See, e.g.*, GREENWALD, *supra* note 1, at 97 (displaying a top secret presentation slide which explains that the NSA embraces a "collect it all" approach to gathering data).

controversial;[40] as Levinson-Waldman explains, it is a put-the-"haystack-before-the-needle approach to information gathering."[41] Stephen Vladeck further notes that there is a presumption that there is, in fact, a needle in the haystack.[42] In short, big data cybersurveillance tools allow for the presumption that there is a needle in the haystack, and such a presumption may appear to justify a "collect-it-all" approach.

Also worthy of caution is the fact that this presumption presents the potential for multiple challenges,[43] including integrating biases into data-driven systems (confirmation bias, implicit bias, cognitive bias); path dependency (building systems to guarantee a correlative "hit" or "miss" that is intended to indicate data is suspicious; and assuming statistical certainty that suspicious data proves guilt of terroristic or criminal threat); overreliance on automation and risk of undertrained analysts; and exacerbation of perverse incentives (metrics of success designed to track the number of suspects identified rather than assess whether intelligence can independently verify suspect classification). In other words, presuming that there is a digitally constructed needle—a suspect, terrorist target, or a pre-crime or pre-terrorist threat that can be digitally identified through big data tools—in the government's digitally constructed haystack[44] (e.g., government's attempt to store and analyze all digitally produced data in order to, purportedly, preempt crime and terrorism)[45] can create incentives to construct imaginary needles.

---

40. *See, e.g.*, Banks, *supra* note 6, at 1636 (explaining the issues that surveillance causes for law enforcement in regards to the consistency in procedures being followed).

41. Vladeck, *Big Data Before and After Snowden, supra* note 6 (citing Rachel Levinson-Waldman, *The Double Danger of the NSA's "Collect It All" Policy on Surveillance*, THE GUARDIAN (Oct. 10, 2013), http://www.theguardian.com/commentisfree/2013/oct/10/double-danger-nsa-surveillance (last visited Sept. 6, 2015) (on file with the Washington and Lee Law Review)).

42. *Id.* at 334 n.11.

43. *Id.*

44. *See id.* ("One of the government's principal descriptive justifications for the metadata program is the need to collect the haystack in order to find the needle.").

45. *See* Ira Hunt, *Even the CIA Is Struggling to Deal with the Volume of Real-Time Social Data*, GIGAOM (Mar. 20, 2013), https://gigaom.com/2013/03/20/even-the-cia-is-struggling-to-deal-with-the-volume-of-real-time-social-data/2/ (last visited Aug. 26, 2015) (discussing the government's interest in obtaining and analyzing real-time social data) (on file with the Washington and Lee Law Review).

Table 1 provides examples of collection programs revealed by the Snowden disclosures that can be described as "Collect It All" programs.

Table 1. Examples of Collection Programs

NSA's Bulk Telephony Metadata Collection Program (NSA)	"The National Security Agency is currently collecting the telephone records of millions of U.S. customers of Verizon, one of America's largest telecoms providers, under a top secret court order issued in April."[46] "Under the terms of the blanket order, the numbers of both parties on a call are handed over, as is location data, call duration, unique identifiers, and the time and duration of all calls."[47] "[T]he communication records of millions of US citizens are being collected indiscriminately and in bulk—regardless of whether they are suspected of any wrongdoing."[48]

46. GREENWALD, *supra* note 1.

47. *Id.*

48. *Id.*

PRISM[49] (NSA)	"PRISM is a tool used by the [NSA] to collect private electronic data belonging to URLs [(uniform resource locator)] of major internet services like Gmail, Facebook, Outlook, and others."[50] "Material collected through Prism is routinely shared with the FBI and CIA, with one NSA document describing the program as a 'team sport.'"[51] The NSA's Special Source Operations (SSO) division is responsible for all programs directed at U.S. communications systems through corporate partnerships like PRISM.[52] The sharing between the NSA, the FBI and the CIA has automated aspects that "enable[s] [them] to see which selectors [search terms] the National Security Agency has tasked to Prism."[53]
UPSTREAM Fiber-Optic Cybersurveillance Programs[54] (STROMBREW, FAIRVIEW, BLARNEY, OAKSTAR) (NSA)	NSA's collection of both metadata and the content of communications traveling through fiber-optic cables.[55] The identities of the four U.S. telecom providers that cooperate with the NSA are tightly guarded.[56] Reportedly, some 11,000 pieces of information come from Blarney every year. It is one of the "top sources" for the President's daily brief, a top-secret document briefing the president every morning on security matters.[57]

49. *Everything You Need to Know About PRISM*, THE VERGE (July 17, 2013), http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet (last visited Sept. 6, 2015) (on file with the Washington and Lee Law Review).

50. *Id.*

51. Glenn Greenwald, Ewen MacAskill, Laura Poitras, Spencer Ackerman & Dominic Rushe, *Microsoft Handed the NSA Access to Encrypted Messages*, THE GUARDIAN (July 12, 2013), http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (last visited Sept. 6, 2015) (on file with the Washington and Lee Law Review).

52. *Id.*

53. *Id.*

54. James Ball, *Edward Snowden NSA Files: Secret Surveillance and Our Revelations so Far,* THE GUARDIAN (Aug. 21, 2013), http://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations (last visited Sept. 8, 2015) (on file with the Washington and Lee Law Review).

55. *Id.*

56. *Id.*

57. Laura Poitras, Marcel Rosenbach & Holger Stark, *Codename 'Apalachee': How America Spies on Europe and the UN*, SPIEGEL ONLINE INT'L (Aug. 26, 2013), http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html (last visited Sept. 8, 2015) (on file with the Washington and Lee Law Review).

III. "Process It All": Processing Programs

Processing programs appear to be used to organize and quantify the vast amount of information gathered by collection programs.[58] Processing programs appear to be built to make sense of a "tsunami of intercept,"[59] or "unthinkably large"[60] volumes of information now generated by big data collection tools. Processing programs appear to drop the identified data into the proper database, or to flag a piece of data based on "selectors."[61] These selectors are instrumental in ascribing a threat level to a particular person, group, IP address,[62] digital user of certain key words,[63] consumer

---

58. *See, e.g.*, Peter Maass, *Inside NSA, Officials Privately Criticize "Collect It All" Surveillance*, THE INTERCEPT (May 28, 2015), https://theintercept.com/2015/05/28/nsa-officials-privately-criticize-collect-it-all-surveillance/ (last visited Dec. 7, 2015) (citing to NSA documents that "outlined a series of programs to prepare for a near future in which the speed and volume of signals intelligence would explode 'almost beyond imagination'") (on file with the Washington and Lee Law Review); Cole, *supra* note 22

> In a one-month period last year, for example, a single unit of the NSA, the Global Access Operations unit, collected data on more than 97 billion e-mails and 124 billion phone calls from around the world; more than 3 billion of those calls and e-mails were collected as they passed through the United States. As of 2012, the agency was processing more than 20 billion telecommunications per day. In a single month in 2011, the NSA collected 71 million calls and e-mails from Poland alone—not a major hub of terrorist activity, the last time I checked. The NSA has admitted that it collects far more content than is routinely useful to analysts.

59. Maass, *supra* note 58 (citing *Dealing with a Tsunami of Intercept*, THE INTERCEPT (May 5, 2015), https://theintercept.com/document/2015/05/05/dealing-tsunami-intercept/ (last visited Nov. 11, 2015) (on file with the Washington and Lee Law Review)).

60. *See, e.g.*, VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 157 (2013) ("When the collection expands to information like financial transactions, health records, and Facebook status updates, the quantity being gleaned is unthinkably large.").

61. *See, e.g.*, Gellman & Poitras, *supra* note 18 ("Analysts who use the system [PRISM] from a Web portal at Fort Meade, Md., key in 'selectors,' or search terms, that are designed to produce at least 51 percent confidence in a target's 'foreignness.'").

62. *See, e.g.*, Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet,'* THE GUARDIAN (July 31, 2013), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (last visited Nov. 24, 2015) ("Analysts can also search by name, telephone number, IP address, keywords, the language in which the internet activity was conducted or the type of browser used.") (on file with the Washington and Lee Law Review).

63. *Id.*

of software intended to secure browsing privacy,[64] etc.[65]

Table 2 provides examples of processing programs that help to illuminate the "Process It All" posture of the intelligence community.

Table 2. Examples of Processing Programs

SHELL TRUMPET[66] (NSA)	SHELLTRUMPET "began as a near-real-time metadata analyzer . . . for a classic collection system."[67] "In its five year history, numerous other systems from across the Agency have come to use SHELLTRUMPET's processing capabilities for performance monitoring and other tasks, such as direct email tip alerting."[68] "On December 31, 2012, an SSO official wrote that SHELLTRUMPET had just processed its One Trillionth metadata record."[69]

64. *See, e.g.*, Spiegel Staff, *Prying Eyes: Inside the NSA's War on Internet Security*, SPIEGEL ONLINE INT'L (Dec. 28, 2014), www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html (last visited Nov. 24, 2015) ("For the NSA, encrypted communication—or what all other Internet users would call secure communication—is 'a threat.'") (on file with the Washington and Lee Law Review).

65. *See* Ryan Gallagher, *How the NSA Is Trying to Sabotage a U.S. Government-Funded Countersurveillance Tool*, SLATE (Sept. 8, 2014), http://www.slate.com/blogs/future_tense/2013/10/04/tor_foxacid_flying_pig_nsa_attempts_to_sabotage_countersurveillance_tool.html (last visited Sept. 9, 2015) (explaining that the TOR browser, created by the U.S. government to help secure military communications, is a more secure way of browsing the Internet; the NSA, however, considers the use of TOR as an "extremist" activity and is constantly developing ways to bypass its security or render it unusable) (on file with the Washington and Lee Law Review).

66. Glenn Greenwald & Spencer Ackerman, *How the NSA Is Still Harvesting Your Online Data*, THE GUARDIAN (June 27, 2013), http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection (last visited Sept. 9, 2015) (on file with the Washington and Lee Law Review).

67. *Id.*

68. *Id.*

69. *Id.*

SNACKS[70] (NSA)	NSA's "Social Network Analysis Collaboration Knowledge Services" (SNACKS) "figures out the personnel hierarchies of organizations from texts."[71]
TEMPORA[72] (UK's GCHQ)	GCHQ's (UK) TEMPORA program has been described as an "internet buffer that lets analysts search vast databases of metadata on internet traffic crossing the UK, for up to 30 days after data is sent." "GCHQ's internet monitoring allows it to tap up to a quarter of internet traffic flowing through the UK at any one time, then use the NSA-developed XKEYSCORE system to search for individuals' communications, search terms, browsing habits, and more. GCHQ and NSA analysts have direct access to the data collected."[73]
XKEYSCORE[74] (NSA)	XKEYSCORE is the system "used to collect, process and search these vast troves of data."[75] "One presentation, published . . . in the Guardian, claimed the system allowed NSA analysts to query 'nearly everything a typical user does on the internet,' including the content of emails, websites visited and searches, as well as their metadata. The system works almost in real-time, documents claimed."[76]

IV. "Exploit It All": Attack Programs

Attack programs go beyond passive surveillance and actively impact an isolated entity's electronic communication or technological device in some way.[77] These programs vary in application and encompass what has

---

70. Scott Shane, *No Morsel Too Miniscule for All-Consuming N.S.A.*, N.Y. TIMES, Nov. 3, 2013, at A1.

71. *Id.*

72. James Ball, *Privacy International to Challenge Telecom Firms over GCHQ Cooperation*, THE GUARDIAN (Aug. 8, 2013), http://www.theguardian.com/uk-news/2013/aug/08/privacy-international-challenges-bt-vodafone-gchq (last visited Sept. 8, 2015) (on file with the Washington and Lee Law Review).

73. *Id.*

74. Ball, *supra* note 54.

75. *Id.*

76. *Id.*

77. *See, e.g.*, Bruce Schneier, *Blog Entries Tagged "Exploit of the Day*," SCHNEIER ON SECURITY (Mar. 12, 2014), https://www.schneier.com/cgi-bin/mt/mt-search.cgi?search=exploit%20of%20the%20day&__mode=tag&IncludeBlogs=2&limit=10&page=1 (last visited Nov. 24, 2015)

> It's important that we know the details of these attack tools. Not because we want to evade the NSA—although some of us do—but because the NSA doesn't have a monopoly on either technology or cleverness. The NSA might have a larger budget than every other intelligence agency in the world combined, but these tools are the sorts of things that any well-funded nation-state adversary would use. And as technology advances, they are the sorts of tools we're going to see cybercriminals use. So think of this less as what the NSA does, and more of

been described as hacking.[78]

Table 3 provides examples of attack, malware, and hacking programs.

Table 3. Examples of Attack Programs

QUANTUMHAND (Disguised Social Media Site Malware) (NSA)	Through QUANTUMHAND, "the agency disguises itself as a fake Facebook server. . . . By concealing its malware within what looks like an ordinary Facebook page, the NSA is able to hack into the targeted computer and covertly siphon out data from its hard drive."[79]
QUANTUMSKY and QUANTUMCOPPER (Disruption Malware) (NSA)	"Sometimes, the agency's aim is disruption rather than surveillance."[80] QUANTUMSKY "is used to block targets from accessing certain websites."[81] QUANTUMCOPPER "corrupts a target file's downloads."[82]
SECONDDATE and FOXACID (Web-Browser Redirection Malware) (NSA)	SECONDDATE can "'influence real-time communications between client and server'" and "'quietly redirect web-browsers' to NSA malware servers called FOXACID."[83]

> a head start as to what everyone will be using. Which means we need to figure out how to defend against them.

(on file with the Washington and Lee Law Review).

78. Joanna Walters, *NSA 'Hacking Unit' Infiltrates Computers Around the World—Report*, THE GUARDIAN (Dec. 29, 2013), http://www.theguardian.com/world/2013/dec/29/der-spiegel-nsa-hacking-unit-tao (last visited Nov. 24, 2015) (citing to Speigel Staff, *Inside TAO: Documents Reveal Top NSA Hacking Unit*, SPIEGEL ONLINE INT'L (Dec. 29, 2013), http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a- 940969.html (last visited Nov. 24, 2015) (on file with Washington and Lee Law Review)) (on file with the Washington and Lee Law Review).

79. Ryan Gallagher & Glenn Greenwald, *How the NSA Plans to Infect 'Millions' of Computers with Malware*, THE INTERCEPT (Mar. 12, 2014), https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ (last visited Sept. 8, 2015) (on file with the Washington and Lee Law Review).

80. *Id.*

81. *Id.*

82. *Id.*

83. *See id.* (citing a "top-secret NSA presentation from 2012").

TURBINE (NSA)	"[G]roundbreaking surveillance technology [NSA] has developed to infect potentially millions of computers worldwide with malware 'implants.'"[84] The automated hacking cybersurveillance technology "enables the NSA to break into targeted computers and to siphon data from foreign Internet and phone networks."[85]

V. "Sniff It All": Isolation Programs

Isolation programs single out a person, group, Internet location, or other entity or device for specialized surveillance.[86] Important, albeit nuanced, differences exist between isolation programs, attack programs, and targeting. While isolation programs may still involve passive surveillance, even though it is more focused, an attack program appears actively impact the isolated entity's computer via malware or spyware.

Table 4 provides examples of isolation programs that appear to flag persons, entities, and devices for heightened suspicion and to isolate them for more concentrated surveillance activities.

---

84. *Id.*

> In 2004, according to secret internal records, the agency was managing a small network of only 100 to 150 implants. But over the next six to eight years, as an elite unit called Tailored Access Operations (TAO) recruited new hackers and developed new malware tools, the number of implants soared to tens of thousands. . . . [TURBINE] is described in the leaked documents as an "intelligent command and control capability" that enables "industrial-scale exploitation."

85. *See id.* ("The automated system—codenamed TURBINE—is designed to 'allow the current implant network to scale to large size (millions of implants) by creating a system that does automated control implants by groups instead of individually.'").

86. *See, e.g.*, Bruce Schneier, *Surveillance by Algorithm*, SCHNEIER ON SECURITY (Mar. 5, 2014), https://www.schneier.com/blog/archives/2014/03/surveillance_by.html (last visited Nov. 24, 2015)

> Increasingly, we are watched not by people but by algorithms. . . . If the agency uses computers to search those emails for keywords, or correlates that location information for relationships between people, it doesn't count as collection, either. Only when those computers spit out a particular person has the data—in NSA terms—actually been collected.

(on file with the Washington and Lee Law Review).

Table 4. Examples of Isolation Programs

SPINALTAP[87] (NSA)	Program under the "Tailored Access Operations" branch of the NSA. It is used to identify unique Internet Protocol addresses used by groups, which makes it possible to snatch messages from a flood of global communications sifted by the agency.[88]
RAMPART-T (NSA)	NSA program that has been running since 1991.[89] This program involves "penetration of hard targets at or near the leadership level"—in other words: heads of state and their closest aides."[90] RAMPART-T is directed against some 20 countries, including China and Russia, but also Eastern European states.[91]

VI. "Partner It All" and "Know It All": Database Programs

Database programs appear to store sorted and categorized information for later access and analysis,[92] and to facilitate intelligence partnering.[93] These immense repositories of information allow for the picture of the digital self[94] to be better realized, but they also facilitate the sharing of data

87. Shane, *supra* note 70, at A1.

88. *Id.*

89. Poitras, Rosenbach & Stark, *supra* note 57.

90. *Id.*

91. *Id.*

92. *See* Greenwald, *supra* note 62 ("A top secret National Security Agency program allows analysts to search with no prior authorization through vast databases containing emails, online chats and the browsing histories of millions of individuals.").

93. *See, e.g.*, Ryan Gallagher, *How Secret Partners Expand NSA's Surveillance Dragnet,* THE INTERCEPT (June 18, 2014), https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/ (last visited Nov. 24, 2015)

> The NSA documents state that under RAMPART-A, foreign partners 'provide access to cables and host U.S. equipment.' This allows the agency to covertly tap into 'congestion points around the world' where it says it can intercept the content of phone calls, faxes, e-mails, internet chats, data from virtual private networks, and calls made using Voice over IP software like Skype.

(on file with the Washington and Lee Law Review).

94. The concept of "digital personhood" describes how "digital dossiers" can be created by others to construct our "data-double," "data image," "digital persona," and "digital self." *See, e.g.*, Roger Clarke, *The Digital Persona and Its Application to Data Surveillance*, 10 THE INFO. SOC. 2, 77–92 (1994); Robert Gordon, *The Electronic Personality and Digital Self*, 56 DISP. RESOL. J. 8 (2001); Kevin D. Haggerty & Richard V. Ericson, *The Surveillant Assemblage*, 51 BRIT. J. SOC. 605 (2000); DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW 87 (2007) (citing DAVID LYON, THE ELECTRONIC EYE: THE RISE OF SURVEILLANCE SOCIETY 19 (1994)); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1149–51 (2002).

between intelligence organizations internally,[95] and between intelligence organizations externally.[96]

Table 5 provides examples of database programs.

95. *See, e.g.*, Ryan Gallagher, *The Surveillance Engine: How the NSA Built Its Own Secret Google*, THE INTERCEPT (Aug. 25, 2014), https://theintercept.com/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/ (last visited Nov. 24, 2015) ("The National Security Agency is secretly providing data to nearly two dozen U.S. government agencies with a 'Google-like' search engine built to share more than 850 billion records about phone calls, emails, cellphone locations, and internet chats, according to classified documents obtained by *The Intercept*.") (on file with the Washington and Lee Law Review).

96. *See, e.g.*, Owen Bowcott, *UK–US Surveillance Regime was Unlawful 'for Seven Years,'* THE GUARDIAN (Feb. 6, 2015), http://www.theguardian.com/uk-news/2015/feb/06/gchq-mass-internet-surveillance-unlawful-court-nsa (last visited Nov. 24, 2015) ("The Investigatory Powers Tribunal (IPT) declared on Friday that regulations covering access by Britain's GCHQ to emails and phone records intercepted by the US National Security Agency (NSA) breached human rights law." (citing Liberty v. Secretary of State for Foreign and Commonwealth Affairs, Investigatory Power Tribunal (June 2, 2015), http://www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf)) (on file with the Washington and Lee Law Review); James Ball, *US and UK Struck Secret Deal to Allow NSA to 'Unmask' Britons' Personal Data*, THE GUARDIAN (Nov. 20, 2013), http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data (last visited Nov. 24, 2015) (on file with the Washington and Lee Law Review).

Table 5. Examples of Database Programs

DISHFIRE[97] (NSA)	NSA database that stores years of text messages from around the world. "The [NSA] has collected almost 200 million text messages a day from across the globe, using them to extract data including location, contact networks and credit card details."[98] According to GCHQ documents, DISHFIRE collects "pretty much everything it can."[99]
MAINWAY[100] (NSA)	MAINWAY is an NSA phone metadata repository that is "one of the main tools used for chaining phone numbers and e-mail addresses . . . ."[101] The system compiles metadata for hundreds of billions of telephone calls made through AT&T and Verizon. Beginning in 2011, MAINWAY was collecting 700 million phone records per day,[102] and "[i]n August 2011, it began receiving an additional 1.1 billion cellphone records daily from an unnamed American service provider under Section 702 of the 2008 FISA Amendments Act, which allows for the collection of the data of Americans if at least one end of the communication is believed to be foreign."[103]
MARINA[104] (NSA)	Database of metadata stored on millions of internet users for up to a year. "The . . . metadata application tracks a user's browser experience, gathers contact information/content and develops summaries of target." "This tool offers the ability to export the data in a variety of formats, as well as create various charts to assist in pattern-of-life development."[105]
TRACFIN[106] (NSA)	NSA database that stores credit card purchase histories.[107]

97. James Ball, *NSA Collects Millions of Text Messages Daily in 'Untargeted' Global Sweep*, THE GUARDIAN (Jan. 15, 2014), http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep (last visited Sept. 8, 2015) (on file with the Washington and Lee Law Review).

98. *Id.*

99. *Id.*

100. *See* James Risen & Laura Poitras, *NSA Gathers Data on Social Connections of U.S. Citizens*, N.Y. TIMES (Sept. 28, 2013), http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?_r=0 (last visited Nov. 6, 2015) (explaining that MAINWAY is "a repository into which vast amounts of data flow daily from the agency's fiber-optic cables, corporate partners and foreign computer networks that have been hacked") (on file with the Washington and Lee Law Review).

101. *Id.*

102. *Id.*

103. *Id.*

104. James Ball, *NSA Stores Metadata of Millions of Web Users for Up to a Year, Secret Files Show*, THE GUARDIAN (Sept. 30, 2013), http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents (last visited Sept. 8, 2015) (on file with the Washington and Lee Law Review).

105. *Id.*

106. Shane, *supra* note 70.

107. *Id.*

VII. Conclusion

Distinctions between small data surveillance and big data cybersurveillance are difficult to grasp in light of the opacity of the intelligence gathering programs and the technical complexity of the technologies now deployed. Small data intelligence gathering[108] methods in a small data world have relied upon human intelligence, including human sensory perception analysis, and other communication gathering and analytic methods that have depended upon human judgment and human decision making; traditional evidence based upon analog data and paper-based files; traditional intelligence collection methods, such as traditional signals intelligence and other traditional communications interception; and other data analytic tools that have centered upon traditional research approaches, such as hypothesis-driven methods.[109]

Yet several scholars have begun to use the term "big data surveillance" to describe how surveillance methods are evolving in light of the emerging pervasiveness of big data technologies.[110] Following the Snowden disclosures, at least one expert has asserted that the NSA is attempting to merge big data tools with small data tools.[111] At the dawn of the big data revolution, scholars are now actively interrogating the implications of government-led big data uses by the government and law

---

108. "'Small data,' like 'big data,' has no set definition." Ferguson, *supra* note 23, at 329 n.6. "Small data" has been described in the following way: "Generally, small data is thought of as solving discrete questions with limited and structured data, and the data are generally controlled by one institution." *Id.* (citing JULES J. BERMAN, PRINCIPLES OF BIG DATA: PREPARING, SHARING, AND ANALYZING COMPLEX INFORMATION 1–2 (2013)).

109. *See, e.g.*, ROBERT M. CLARK, INTELLIGENCE COLLECTION 45–83 (2014) (describing small data collection methods through human intelligence (HUMINT)). *See generally* ROBERT WALLACE & H. KEITH MELTON, WITH HENRY R. SCHLESINGER, SPYCRAFT: THE SECRET HISTORY OF THE CIA'S SPYTECHS FROM COMMUNISM TO AL-QAEDA (2008) (listing the various ways that the CIA has acquired intelligence throughout its existence).

110. *See, e.g.*, Mark Andrejevic, *Surveillance in the Big Data Era*, *in* EMERGING PERVASIVE INFORMATION AND COMMUNICATION TECHNOLOGIES (PICT): ETHICAL CHALLENGES, OPPORTUNITIES, AND SAFEGUARDS 56 (Kenneth D. Pimple ed., 2014) ("[I]n the era of 'big data' surveillance, the imperative is to monitor the population as a whole: otherwise it is harder to consistently and reliably discern useful patterns."); David Lyon, *Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique*, BIG DATA & SOC'Y (July 9, 2014), http://bds.sagepub.com/content/1/2/2053951714541861.full.pdf+html (last visited Sept. 8, 2015) ("The Big Data/surveillance link was recognized by US President Obama on 17 January 2014, when he called for a 'comprehensive review of Big Data and privacy' following the Snowden leaks." (citation omitted)) (on file with the Washington and Lee Law Review).

111. Crawford, *supra* note 23.

enforcement.[112] Several scholars have noted how transformative technological shifts have also transformed methods of governance and surveillance as a tool of governance, including the transformation of the administrative state into a National Surveillance State.[113]

This Essay attempts to contribute to this important discourse through expository research that is largely empirical in its method, with the recognition that a true empirical approach is challenged given the covert nature of the subject matter. Various scholars have juxtaposed small data policing and surveillance practices with big data policing and surveillance practices as a way to deepen the legal and constitutional discourse.[114] Many experts have documented how the NSA, CIA and other intelligence organizations capitalized on technological innovation in the evolution and expansion of intelligence-gathering tools and methods.[115]

---

112. *See generally*, Fairfield & Luna, *supra* note 9 (illustrating how data mining has applications in exonerating innocent parties, despite the privacy concerns); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013) (explaining the negative effects that surveillance has on personal development); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013) (stating that data mining and surveillance increases the power disparity between individual and government, and can harm free exercise of civil liberties).

113. *See, e.g.*, Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2297 (2014) ("The digital era is different. Governments can target for control or surveillance many different aspects of the digital infrastructure that people use to communicate: telecommunications and broadband companies, web hosting services, domain name registrars, search engines, social media platforms, payment systems, and advertisers."); Balkin, *supra* note 2 ("The question is not whether we will have a surveillance state in the years to come, but what sort of surveillance state we will have."). *See generally* Balkin & Levinson, *supra* note 2 (illustrating how partisan philosophies from decades ago indicated that this could happen); David Lyon, *Biometrics, Identification and Surveillance*, 22 BIOETHICS 499 (2008) (pointing out that biometric data grants the government a non-invasive method to identify individuals); Erin Murphy, *Paradigms of Restraint*, 57 DUKE L.J. 1321 (2008) (saying that, while useful, these government programs are excessively controlling without any scrutiny); Lior Jacob Strahilevitz, *Signaling Exhaustion and Perfect Exclusion*, 10 J. ON TELECOMM. & HIGH TECH L. 321 (2012) (stating that we are in an entirely new era of technology that is cementing inequality by homogenizing contacts).

114. *See, e.g.*, Ferguson, *supra* note 23, at 329 (discussing in the context of predictive policing practices: "[W]hat happens if this small data suspicion [suspicion that is 'individualized to a particular person at a particular place'] is replaced by 'big data' suspicion?"); Toomey & Kaufman, *supra* note 6, at 847 (describing a "notice paradox" whereby, in a small data surveillance world, notice was usually given because searches were limited to a "physical world," whereas big data surveillance methods provided the government significant control over when and to whom notice is given).

115. *See generally, e.g.*, JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA (2008) (detailing how the NSA's

Some have focused particularly on the algorithmic-driven decision-making consequences of emerging big data technologies.[116] Other experts have focused on the data mining and predictive analytic capacities of big data tools.[117]

This Essay concludes that a detailed examination of the Snowden disclosures requires not only a careful inquiry into the legal and constitutional framework that guides the oversight of these programs. A close interrogation also requires a careful inquiry into the big data technological architecture, as well as the theories of data science and the rationales of big data-driven policymaking that informs them. These technological, theoretical, and policymaking movements are occurring within what has been termed by scholars as the National Surveillance State. Better understanding the manner in which intelligence gathering may be shifting away from small data surveillance methods and toward the adoption of big data cybersurveillance methods—and assessing the efficacy of this shift[118]—can serve as a foundation for

---

technology has been evolving to maintain an ability to unscramble cryptic communications); BAMFORD, *supra* note 34 (explaining the Armed Forces Security Agency's methods for cracking cleartext and cryptanalyzed ciphertext); Banks, *supra* note 6; Swire, *supra* note 6 (observing that espionage agencies are now able to use data-mining to identify terrorists); GREENWALD, *supra* note 1, at 97 (citing NSA slide from Snowden disclosures titled, "New Collection Posture," quoting NSA data collection procedure as "Collect it All"); *see also* Cole, *supra* note 22 ("In one remarkable [NSA] slide presented at a 2011 meeting of five nations' intelligence agencies and revealed here for the first time, the NSA described its "collection posture" as 'Collect It All,' 'Process It All,' 'Exploit It All,' 'Partner It All,' 'Sniff It All' and, ultimately, 'Know It All.'").

116. *See, e.g.*, FRANK PASQUALE, THE BLACK BOX SOCIETY (2015) (comparing the existing intelligence systems to error-prone commercial credit scoring systems); Danielle Keats Citron & Frank A. Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 20–22 (2014) (stating the need for oversight on existing automated scoring systems used by intelligence agencies to analyze possible threats).

117. *See, e.g.*, STEVEN FINLAY, PREDICTIVE ANALYTICS, DATA MINING AND BIG DATA: MYTHS, MISCONCEPTIONS, AND METHODS (2014) (stating that big data has become a price to organizations large enough to use it for professional purposes); ERIC SIEGEL, PREDICTIVE ANALYTICS: THE POWER TO PREDICT WHO WILL CLICK, BUY, LIE, OR DIE 3 (2013) (saying that data mining increases by "an estimated 2.5 quintillion bytes per day"); NATE SILVER, THE SIGNAL AND THE NOISE: WHY SO MANY PREDICTIONS FAIL—BUT SOME DON'T (2012) (pointing out ways in which predictive analysis is becoming increasingly accurate). *See generally* Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435 (2008) (documenting the need for regulations now that data mining has become ubiquitous); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317 (2008) (listing legal concerns over governmental and third party data mining); Daniel J. Solove, *Data Mining and the Security–Liberty Debate*, 75 U. CHI. L. REV. 343 (2008) (advocating that "courts fail to give adequate scrutiny to security interests").

118. Several recent reports, conducted by both the public and nonprofit sectors, have

debates[119] on how best to constrain comprehensive and ubiquitous surveillance technologies under the rule of law at the dawn of the National Surveillance State.

---

investigated the efficacy of several of the programs revealed by the Snowden disclosures. *See, e.g.*, PETER BERGEN, DAVID STERMAN, EMILY SCHNEIDER & BAILEY CAHALL, NEW AMERICA FOUNDATION, DO NSA'S BULK SURVEILLANCE PROGRAMS STOP TERRORISTS? (2014), https://static.newamerica.org/ attachments/1311-do-nsas-bulk-surveillance-programs-stop-terrorists/IS_NSA_surveillance.pdf (arguing that "traditional" investigative tools like the use of informants have been the primary method used by the NSA in counterterrorism operations in the past); RICHARD A. CLARKE, MICHAEL J. MORRELL, GEOFFREY R. STONE, CASS R. SUNSTEIN & PETER SWIRE, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES (2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (describing how the effectiveness of big data surveillance relies on the enemy's ignorance); LEVINSON-WALDMAN, *supra* note 15; PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014), https://www.pclob.gov/library/215-Report_on_the_ Telephone_Records_Program.pdf (stating that the NSA's phone records program fails to meet effectiveness requirements); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014), https://www.pclob.gov /library/702-Report.pdf (observing difficulties in assessing the efficacy of surveillance programs).

119. *See, e.g.*, Jennifer Stisa Granick & Christopher Jon Sprigman, Opinion, *The Criminal N.S.A.*, N.Y. TIMES (June 27, 2013), http://www.nytimes.com/2013/06/28/opinion/the-criminal-nsa.html (last visited Sept. 8, 2015) ("If all data is 'relevant,' it makes a mockery of the already shaky concept of relevance.") (on file with the Washington and Lee Law Review); Bruce Schneier, *NSA Surveillance: A Guide to Staying Secure*, THE GUARDIAN (Sept. 6, 2013), http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance (last visited Sept. 8, 2015) ("The NSA has turned the fabric of the internet into a vast surveillance platform, but they are not magical.") (on file with the Washington and Lee Law Review); Glyn Moody, *The Repeated Failure of the US and UK Governments' 'Add More Hay' Approach to Surveillance*, TECHDIRT (Dec. 3, 2014), https://www.techdirt.com/articles/20141201/09320729286/repeated-failure-us-uk-governments-add-more-hay-approach-to-surveillance.shtml (last visited Sept. 9, 2015) (pointing out that mistakes are still made despite this data influx) (on file with the Washington and Lee Law Review).

Appendix: The Snowden Disclosures [from June 2013 to January 2015]

Program Name	Type	Description
A-PLUS[120]	Collection	NSA program listed under "Collect it All" that states it will: "Increase volume of signals: ASPHALT/A-PLUS"[121]
ACRIDMINI[122]	Collection	NSA program that is listed as being under BOUNDLESSINFORMANT,[123] a GCHQ [Government Communications Headquarters], Britain's intelligence, and security program.[124]
AGILEVIEW[125]	Collection	NSA "DNI [digital network intelligence] tool."[126]
AGILITY[127]	Database	NSA "DNI [digital network intelligence] tool."[128]
AIGHANDLER[129]	Processing	NSA program used for "geolocation analysis."[130]

120. GREENWALD, *supra* note 1, at 97.

121. *Id.*

122. *The NSA in Germany: Snowden's Documents Available for Download*, SPIEGEL ONLINE INT'L (June 18, 2014, 4:21 PM), http://www.spiegel.de/international/the-germany-file-of-edward-snowden-documents-available-for-download-a-975917.html (last visited Nov. 17, 2015) (on file with the Washington and Lee Law Review).

123. *Id.*

124. Glenn Greenwald, *Snowden's Documents Reveal Covert Surveillance and Pressure Tactics Aimed at Wikileaks and Its Supporters*, THE INTERCEPT (Feb. 18, 2014), https://firstlook.org/theintercept/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/ (last visited Sept. 9, 2015) (on file with the Washington and Lee Law Review).

125. William Arkin, *NSA Code Names Revealed*, WILLIAM M. ARKIN ONLINE (Mar. 13, 2012), http://williamaarkin.wordpress.com/2012/03/13/nsa-code-names-revealed/ (last visited Sept. 9, 2015) (on file with the Washington and Lee Law Review).

126. *Id.*

127. *Id.*

128. *Id.*

129. *Id.*

130. *Id.*

AIRBAG[131]	Collection	GCHQ program that provides "JTRIG Laptop capability for field operations."[132] Status is listed as "operational."[133]
AIRGAP[134]	Processing	NSA tool that, according to Marc Ambinder, serves as a "[p]riority missions tool used to determine SIGINT gaps."[135]
AIRWOLF[136]	Collection	GCHQ program that collects YouTube information and falls under the JTRIG program.
ALLIUM ARCH[137]	Processing	GCHQ program that uses "JTRIG UIA via the Tor network."[138] Status is listed as "operational."[139]
ANGRY PIRATE[140]	Attack	GCHQ program that "is a tool that will permanently disable a target's account on their computer."[141] Status is listed as "[r]eady to fire (but see target restrictions)."[142]

131. *JTRIG Tools and Techniques*, THE INTERCEPT (July 14, 2014), https://firstlook.org/theintercept/document/2014/07/14/jtrig-tools-techniques (last visited Sept. 8, 2015) (on file with the Washington and Lee Law Review).

132. *Id.*

133. *Id.*

134. Marc Ambinder, *An Educated Guess About How the NSA Is Structured*, THE ATLANTIC (Aug. 14, 2014), http://www.theatlantic.com/technology/archive/2013/08/an-educated-guess-about-how-the-nsa-is-structured/278697/%20 (last visited Sept. 9, 2015) (on file with the Washington and Lee Law Review); David Somerville, *The National Security Agency*, MINDMEISTER, http://www.mindmeister.com/308518551/the-national-security-agency-operates-more-than-500-separate-signals-intelligence-platforms-employs-roughly-30-000-civilians-and-military-budget-10-billion (last visited Sept. 9, 2015) (on file with the Washington and Lee Law Review).

135. Ambinder, *supra* note 134.

136. *JTRIG Tools and Techniques*, *supra* note 131.

137. *Id.*

138. *Id.*

139. *Id.*

140. *Id.*

141. *Id.*

142. *Id.*

ANCESTRY[143]	Collection	GCHQ "tool for discovering the creation date of yahoo selectors."[144] Listed as "fully operational."[145]
ANCHORY[146]	Database	NSA program that, according to Marc Ambinder, is the "[m]ain repository of finished NSA SIGINT reports going back three years."[147]
ANTICRISIS GIRL[148]	Collection	GCHQ program used to collect user information on visitors to WikiLeaks and other activist sites.
ANTO LP PROSS GUI[149]	Collection	NSA remote operations center (RDC) that is part of the IRONCHEF attack program.
APERTURE SCIENCE[150]	Collection	NSA collection program that is a parent of BOUNDLESSINFORMANT.
AQUADOR[151]	Processing	NSA program that, according to Marc Ambinder, is a "[m]erchant ship tracking tool."[152]
ARSON SAM[153]	Collection	GCHQ program that "is a tool to test the effect of certain types of PDU SMS messages on phones/network. It also includes PDU SMS Dumb Fuzz Testing."[154] Status is listed as "[r]eady to fire," (not against live targets—this is an R&D Tool).[155]

143. *Id.*

144. *Id.*

145. *Id.*

146. Ambinder, *supra* note 134; Somerville, *supra* note 134.

147. *Id.*

148. Greenwald, *supra* note 124.

149. *NSA Catalogue*, AM. C.L. UNION, https://www.aclu.org/sites/default/files/assets/nsas_spy_catalogue _0.pdf.

150. *The NSA in Germany: Snowden's Documents Available for Download*, *supra* note 122.

151. Ambinder, *supra* note 134.

152. *Id.*; Somerville, *supra* note 134.

153. *JTRIG Tools and Techniques*, *supra* note 131.

154. *Id.*

155. *Id.*

ARTEMIS[156]	Processing	NSA program that performs geospatial analysis for an undetermined purpose.
ARTIFICE[157]	Collection	NSA program that is part of the STORMBREW—appears to be a codename for an unknown corporate partner.
ASPHAULT[158]	Collection	NSA program that is described as "'Collect it All' proof-of-concept system."[159]
ASSOCIATION[160]	Database	NSA program that, according to Marc Ambinder, is a "[t]actical SIGINT social network database."[161]
ASTRAL PROJECTION[162]	Processing	JTRIG "[r]emote GSM secure covert internet proxy using TOR hidden services."[163] Status listed as "operational."[164]
AUTOSOURCE[165]	Collection	
AXLE GREASE[166]	Collection	GCHQ's "covert banking link for CPG."[167] Listed as "operational."[168]
BABYLON[169]	Collection	GCHQ "tool that bulk queries web mail addresses and verifies whether they can be signed up for. A green tick indicates that the address is currently in use. Verification can currently be done for Hotmail and Yahoo."[170]

156. Arkin, *supra* note 125.

157. Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST (Dec. 4, 2013), http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html (last visited Sept. 9, 2015) (on file with the Washington and Lee Law Review).

158. GREENWALD, *supra* note 1.

159. *Id.*

160. Ambinder, *supra* note 134.

161. *Id.*; Somerville, *supra* note 134.

162. *JTRIG Tools and Techniques*, *supra* note 131.

163. *Id.*

164. *Id.*

165. Arkin, *supra* note 125.

166. *JTRIG Tools and Techniques*, *supra* note 131.

167. *Id.*

168. *Id.*

169. *Id.*

170. *Id.*

BADGER[171]	Collection	GCHQ program that provides "mass delivery of email messaging to support an information Operations campaign."[172] Status is listed as "[r]eady to fire."[173]
BALLOONKNOT[174]	Collection	Listed in "United Kingdom—Collection Information" with Validator ID of "610210370."[175]
BANYAN176	Database	Marc Ambinder describes this as an "NSA tactical geospatial correlation database."[177]
BEARSCRAPE[178]	Isolation	GCHQ program that "can extract WiFi connection history (MAC and timing) when supplied with a copy of the registry structure or run on the box."[179]
BEARTRAP[180]	Collection	GCHQ program that allows "[b]ulk retrieval of public BEBO profiles from member or group ID."[181] Status listed as "[f]ully operational."[182]
BERRY TWISTER[183]	Collection	GCHQ program that is a "sub-system of FRUIT BOWL."[184] Listed as a "[p]ilot."[185]

171. *Id.*
172. *Id.*
173. *Id.*
174. *United Kingdom—Collection Information*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/files/2014/06/23/ boundless_informant_statistics_on_the_uk.pdf.
175. *Id.*
176. Ambinder, *supra* note 134
177. *Id.*; Somerville, *supra* note 134.
178. *JTRIG Tools and Techniques*, *supra* note 131.
179. *Id.*
180. *Id.*
181. *Id.*
182. *Id.*
183. *Id.*
184. *Id.*
185. *Id.*

BERRYTWISTER PLUS[186]	Collection	GCHQ program that is a "sub-system of FRUIT BOWL."[187] Listed as a "[p]ilot."[188]
BIRDSONG[189]	Collection	GCHQ program that provides "[a]utomatic posting of Twitter updates."[190] Status listed as "[r]eplaced by SYLVESTER."[191]
BIRDSTRIKE[192]	Collection	GCHQ program for "Twitter monitoring and profile collection."[193] Status listed as "[f]ully operational."[194]
BLACKHEART[195]	Collection	NSA exploit tool that facilitates "[c]ollection from an FBI implant."[196]
BLACKPEARL[197]	Collection	Intelligence Analysis Intern used BLACKPEARL and "successfully located, identified, and submitted several new targets . . . ."[198]
BLARNEY[199]	Collection	NSA program that "among others, filter[s] and gather[s] information at major telecommunications companies."[200]

186. *Id.*

187. *Id.*

188. *Id.*

189. *Id.*

190. *Id.*

191. *Id.*

192. *Id.*

193. *Id.*

194. *Id.*

195. Bruce Schneier, *Code Names for NSA Exploit Tools*, SCHNEIER ON SECURITY (Oct. 23, 2013), https://www.schneier.com/blog/archives/2013/10/code_names_for.html (last visited Nov. 5, 2015) (on file with the Washington and Lee Law Review).

196. *Id.*

197. Arkin, *supra* note 125.

198. *The NSA in Germany: Snowden's Documents Available for Download*, *supra* note 122.

199. Siobhan Gorman & Jennifer Valentino-Devries, *New Details Show Broader NSA Surveillance Reach*, WALL ST. J. (Aug. 20, 2013), http://www.wsj.com/articles/SB10001424127887324108204579022874091732470 (last visited Sept. 1, 2015) (on file with the Washington and Lee Law Review).

200. *Id.*

BLUEANCHOR[201]	Collection	A part of an NSA system with "the capacity to reach roughly 75% of all U.S. Internet traffic in the hunt for foreign intelligence, including a wide array of communications by foreigners and Americans."[202]
BOMBAYROLL[203]	Collection	GCHQ program providing "JTRIG's legacy UIA standalone capability."[204] Listed as "[o]perational."[205]
BOTANICREALTY[206]	Collection	TEC program "installed at LADYLOVE in hopes of locating, identifying, and collecting clear and encrypted video signals."[207]
BOUNDLESS INFORMANT[208]	Processing	"The focus of [this] internal NSA tool is on counting and categorizing the records of communications, known as metadata, rather than the content of an email or instant message."[209]
BRANDYSNAP[210]	Collection	GCHQ program that is a "JTRIG UIA contingency at Scarborough."[211] Listed as "implementation."[212]
BUFFALOGREEN[213]	Collection	The codename for information shared with Poland under the ORANGECRUSH system.[214]

201. *NSA Government Over Reach vs. Privacy Rights*, OLIVE BIO DIESEL, http://www.olivebiodiesel.com/NSAOverReach.htm (last visited Nov. 5, 2015) (on file with the Washington and Lee Law Review).

202. *Id.*

203. *JTRIG Tools and Techniques*, *supra* note 131.

204. *Id.*

205. *Id.*

206. *TEC Successfully Installs BOTANICREALTY at LADYLOVE (USJ-799),* ELECTRONIC FRONTIER FOUND., https://www.eff.org/files/2014/06/23/report_on_the_nsa-bnd_cooperation_known_as_joint _sigint_activity_jsa.pdf.

207. *Id.*

208. GREENWALD, *supra* note 1, at 92–93.

209. *Id.*; Glenn Greenwald & Ewen MacAskill, *Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data*, THE GUARDIAN (June 11, 2013), http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining (last visited Nov. 5, 2015) (on file with the Washington and Lee Law Review).

210. *JTRIG Tools and Techniques*, *supra* note 131.

211. *Id.*

212. *Id.*

213. GREENWALD, *supra* note 1, at 106.

214. *Id.*; Wayne Madsen, *Washington Spies on NATO; Other Allies*, STRATEGIC

BUGSY[215]	Collection	GCHQ program for "Google+ monitoring (circles, profiles, etc.)."[216]
BULLRUN[217]	Processing	"The agency defines capability as 'the NSA/CSS ability to exploit a specific technology,' according to a 2010 document outlining the Bullrun program. Here, the agency is claiming that it can gain access to the text and audio of an Internet chat service. It is unclear from the documents that The New York Times and ProPublica have access to which service this document refers to."[218]
BUMBLEBEEDANCE[219]	Collection	GCHQ's "JTRIG Operational VM/TOR architecture."[220] Listed as "[o]perational."[221]
BUMPERCAR+[222]	Attack	GCHQ program that "is an automated system by JTRIG CITD to support BUMPERCAR operations. BUMPERCAR operations are used to disrupt and deny Internet-based terror videos or other material. The technique employs the services provided by upload providers to report offensive materials."[223] Status listed as "[r]eady to fire."[224]

CULTURE FOUND. (May 18, 2014), http://www.strategic-culture.org/pview/2014/05/18/washington-spies-on-nato-other-allies.html (last visited Nov. 5, 2015) (on file with the Washington and Lee Law Review).

215. *JTRIG Tools and Techniques*, *supra* note 131.

216. *Id.*

217. *Secrets Documents Reveal N.S.A. Campaign Against Encryption*, N.Y. TIMES (Sept. 5, 2013), http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?_r=1& (last visited Nov. 5, 2015) (on file with the Washington and Lee Law Review).

218. *Id.*

219. *JTRIG Tools and Techniques*, *supra* note 131.

220. *Id.*

221. *Id.*

222. *Id.*

223. *Id.*

224. *Id.*

BURLESQUE[225]	Attack	GCHQ program that provides the "capability to send spoofed SMS text messages."[226] Status is listed as "[r]eady to fire."[227]
BYSTANDER[228]	Database	GCHQ "categorisation database accessed via web service."[229]
CANDYGRAM[230]	Collection	NSA program that "[t]ypical use scenarios are asset validation, target tracking and identification as well as identifying hostile surveillance units with GSM handsets."[231]
CANNONBALL[232]	Attack	GCHQ program that provides the "capability to send repeated text messages to a single target."[233] Status listed as "[r]eady to fire."[234]
CAPTIVATEDAUDIENC[235]	Collection	An NSA implant plug-in that "is used to take over a targeted computer's microphone and record conversations taking place near the device."[236]

225. *Id.*

226. *Id.*

227. *Id.*

228. *Id.*

229. *Id.*

230. *CANDYGRAM GSM Telephone Tripwire*, SECURITY LEDGER (Jan. 8, 2007), https://securityledger.com/wp-content/uploads/2013/12/nsa-ant-candygram.jpg (last visited Nov. 5, 2015) (on file with the Washington and Lee Law Review).

231. *Id.*

232. *JTRIG Tools and Techniques*, *supra* note 131.

233. *Id.*

234. *Id.*

235. Ryan Gallager & Glenn Greenwald, *How the NSA Plans to Infect Millions of Computers with Malware*, THE INTERCEPT (Mar. 12, 2014), https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/ (last visited Nov. 5, 2015) (on file with the Washington and Lee Law Review).

236. *Id.*

CARBOY[237]	Collection	A collection station in Bude, England that "intercept[s] high-priority communications traffic moving through communications satellites parked over the Atlantic."[238]
CASPORT[239]	Processing	NSA program that grants "access to NSA Establishment FISA data."[240]
CASTANET[241]	Collection	An "NSA document shows what appears to be an SCS antenna system with the code name 'Einstein' and its corresponding control device 'Castanet.'"[242]
CCDP[243]	Collection	"[C]alled the Communications Capabilities Development Programme." "Under the scheme the security services would be granted 'real time' access to phone and internet records of people they want to put under surveillance, as well as the ability to reconstruct their movements through the information stored in the databases."[244]

237. *NSA Sugar Grove Listening Post*, LEAKSOURCE (Jan. 4, 2014) http://leaksource.info/2014/01/06/nsa-sugar-grove-listening-post/ (last visited Sept. 8, 2015) (on file with the Washington and Lee Law Review).

238. *Id.*; Rick Steelhammer, *In W.Va., Mountains of NSA Secrecy*, SATURDAY GAZETTE MAIL (Jan. 4, 2014), http://www.wvgazette.com/News/201401040095 (last visited Sept. 1, 2015) (on file with the Washington and Lee Law Review).

239. Memorandum from SID Oversight and Compliance, to SIGINT Director (May 3, 2012), http://nsarchive.gwu.edu/NSAEBB/NSAEBB436/docs/EBB-044.pdf.

240. *Id.*

241. *NSA/CIA "Special Collection Service" Agents Posing as Diplomats in Embassies/Consulates, 80 Locations Worldwide*, LEAKS SOURCE (Oct. 27, 2013) http://leaksource.info/2013/10/27/nsa-cia-special-collection-service-agents-posing-as-diplomats-in-embassies-consulates-80-locations-worldwide/ (last visited Nov. 4, 2015) (on file with the Washington and Lee Law Review).

242. *Id.*

243. David Barnett, *Phone and Email Records to be Stored in New Spy Plan*, TELEGRAPH (Feb. 18, 2012), http://www.telegraph.co.uk/technology/internet/9090617/Phone-and-email-records-to-be-stored-in-new-spy-plan.html (last visited Nov. 5, 2015) (on file with the Washington and Lee Law Review).

244. *Id.*

CERBERUS[245]	Collection	GCHQ program that is "JTRIG's legacy UIA desktop, soon to be replaced by FOREST WARRIOR."[246] Listed as "[o]perational."[247]
CERBERUS STATISTICS COLLECTION[248]	Collection	GCHQ program that "[c]ollects on-going usage information about how many users utilize JTRIG's UIA capability, what sites are the most frequently visited etc. This is in order to provide JTRIG infrastructure and ITServices management information statistics."[249] Status is listed as "operational."[250]
CHANGELING[251]	Isolation	GCHQ program that provides the "[a]bility to spoof any email address and send email under that identity."[252]
CHINESEFIRECRACKER[253]	Attack	GCHQ program that provides "[o]vert brute login attempts against online forums."[254] Status is listed as "[r]eady to fire."[255]
CHIPPEWA[256]	Processing	A repository for written reports when "the identity of a U.S. person is found in the raw SIGINT."[257]

245. *JTRIG Tools and Techniques*, *supra* note 131.

246. *Id.*

247. *Id.*

248. *Id.*

249. *Id.*

250. *Id.*

251. *Id.*

252. *Id.*

253. *Id.*

254. *Id.*

255. *Id.*

256. *NSA and Israeli Intelligence: Memorandum of Understanding*, THE GUARDIAN (Sept. 11, 2013), http://www.theguardian.com/world/interactive/2013/sep/11/nsa-israel-intelligence-memorandum-understanding-document (last visited Nov. 4, 2015) (on file with the Washington and Lee Law Review).

257. *Id.*

CIMBRI[258]	Processing	NSA program with which "the agency filters the communications that needed more attention."[259]
CLEANSWEEP[260]	Attack	GCHQ program that allows "[m]asquerade Facebook Wall Posts for individuals or entire countries."[261] Status listed as "[r]eady to fire (SIGINT sources required)."[262]
CLUMSYBEEKEEPER[263]	None	GCHQ program that is simply described as "[s]ome work in progress to investigate IRC effects."[264] Status is listed as "NOT READY TO FIRE."[265]
CONCRETEDONKEY[266]	Attack	GCHQ program that has "the capability to scatter an audio message to a large number of telephones, or repeatedly bomb a target number with the same message."[267] Status is listed as "[i]n development."[268]
CONDUIT[269]	Database	GCHQ "database of C2C identifiers for Intelligence Community assets acting online, either under alias or in real name."[270]

258. Shobhan Saxena, *NSA Picked Content from Brazilian President's Phone, Emails, and Texts*, HINDU (Sept. 3, 2013), http://www.thehindu.com/news/national/nsa-picked-content-from-brazilian-presidents-phones-emails-texts/article5086977.ece (last visited Sept. 1, 2015) (on file with the Washington and Lee Law Review).

259. *Id.*

260. *JTRIG Tools and Techniques*, *supra* note 131.

261. *Id.*

262. *Id.*

263. *Id.*

264. *Id.*

265. *Id.*

266. *Id.*

267. *Id.*

268. *Id.*

269. *Id.*

270. *Id.*

OCTAVE/ CONTRAOACTAVE[271]	Collection	NSA program that Marc Ambinder describes as a "[c]ollection mission tasking tool."[272]
CONVEYANCE[273]	Processing	One of two NSA programs that "appear to be a final layer of filtering to reduce the intake of information about Americans."[274]
CORALREEF[275]	Database	NSA database involved with "Cryptovariable Management."[276]
CO TRAVELER[277]	Collection	"[The NSA] collects locations in bulk because its most powerful analytic tools—known collectively as CO-TRAVELER—allow it to look for unknown associates of known intelligence targets by tracking people whose movements intersect."[278] "CO-TRAVELER and related tools require the methodical collection and storage of location data on what amounts to a planetary scale."[279]
COUNTRYFILE[280]	Collection	GCHQ "sub-system of JAZZ FUSION."[281] Listed as "operational."[282]

271. Ambinder, *supra* note 134.

272. *Id*.

273. *NSA Slides Explain the PRISM Data-Collection Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (last visited Sept. 2, 2015) (on file with the Washington and Lee Law Review).

274. *Id*.

275. *NSA Hammerchant and Hammerstein*, INTERNET ARCHIVE (Jan. 1, 2014), https://archive.org/stream/pdfy-90YSg4WAqCQCF8I4/0955_peter_gutmann_djvu.txt (last visited Sept. 2, 2015) (on file with the Washington and Lee Law Review).

276. *Id*.

277. Gellman & Soltani, *supra* note 157.

278. *Id*.

279. *Id*.

280. *JTRIG Tools and Techniques*, *supra* note 131.

281. *Id.*

282. *Id.*

CRISSCROSS[283]	Database	An "older top-secret data sharing system named CRISSCROSS/PROTON, which was launched in the 1990s and managed by the CIA."[284]
CROSSEYEDSLOTH[285]	Collection	Listed in "United Kingdom—Collection Information" with Validator IDs of "610209553" and "610209558."[286]
CRYOSTAT[287]	Isolation	GCHQ program that "is a JTRIG tool that runs against data held in NEWPIN. It then displays this data in a chart to show links between targets."[288]
CUSTOMS[289]	Unknown	NSA exploit tool described only as "[c]ustoms opportunities (not LIFESAVER)."[290]
CYBERCOMMANCCONSOLE[291]	Processing	GCHQ "centralised suite of tools, statistics and viewers for tracking current operations across the Cyber community."[292]
DANCINGBEAR[293]	Collection	GCHQ program that "obtains the locations of WiFi access points."[294] Status is listed as "fully operational."[295]
DANCINGOASIS[296]	Unknown	Listed in NSA documents as "DGOT (metadata TOGD)-US-3171 (DACINGOASIS 13 MAR 2012" and "DGOD (metadata DOGD)-US-3717 (DANCINGOASIS) 13 Mar 2012."[297]

283. Gallagher, *supra* note 95.
284. *Id.*
285. *United Kingdom—Collection Information*, *supra* note 174.
286. *Id.*
287. *JTRIG Tools and Techniques*, *supra* note 131.
288. *Id.*
289. Schneier, *supra* note 195.
290. *Id.*
291. *JTRIG Tools and Techniques*, *supra* note 131.
292. *Id.*
293. *Id.*
294. *Id.*
295. *Id.*
296. GREENWALD, *supra* note 1, at 100.
297. *Id.*

DAREDEVIL[298]	Attack	Listed in NSA documents as an "Implant/Shooter," along with STRAIGHTBIZARRE.[299]
DARKFIRE[300]	Collection	Listed in "United Kingdom—Collection Information," with Validator ID of "610208689."[301]
DARKQUEST[302]	Processing	Listed in NSA documents under "know it all" bubble of "New Collection Posture."[303]
DARKTHUNDER[304]	Attack	According to NSA documents, this is "[a] SIGAD used for TAO, and thus QUANTUM, FOXACID, and the like."[305]
DEADPOOL[306]	Isolation	GCHQ Program that serves as a "URL shortening service."[307]
DEER STALKER[308]	Isolation	GCHQ program that provides the "[a]bility to aid geolocation of Sat Phones/GSM Phones via a silent calling to the phone."[309] Status listed as "[r]eady to fire."[310]
DEVILS HANDSHAKE[311]	Collection	GCHQ program that is described as an "ECI Data Technique."[312] Status is listed as "fully operational."[313]

298. *The NSA and GCHQ's QUANTUMTHEORY Hacking Tactics*, THE INTERCEPT (Mar. 12, 2014), https://firstlook.org/theintercept/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/ (last visited Sept. 2, 2015) (on file with the Washington and Lee Law Review).

299. *Id*.

300. *United Kingdom—Collection Information*, *supra* note 174.

301. *Id*.

302 GREENWALD, *supra* note 1, at 97.

303. *Id.*; *New Collection Posture Slide*, AM. C.L. UNION, https://www.aclu.org/files/natsec/nsa/20140722/New%20Data%20Collection%20Posture.pdf.

304. *NSA Codenames*, CRYPTOME (Jan. 1, 2014), https://cryptome.org/2014/01/nsa-codenames.htm (last visited Sept. 5, 2015) (on file with the Washington and Lee Law Review).

305. *Id*.

306. *JTRIG Tools and Techniques*, *supra* note 131.

307. *Id*.

308. *Id*.

309. *Id*.

310. *Id*.

311. *Id*.

312. *Id*.

313. *Id*.

DEWSWEEPER[314]	Isolation	NSA exploit tool that is described as "USB (Universal Serial Bus) hardware host tap that provides COVERT link over US link into a target network. Operates w/RF relay subsystem to provide wireless Bridge into target network."[315]
DIALD[316]	Collection	GCHQ program that is an "external Internet Redial and Monitor Daemon."[317] Listed as "operational."[318]
DIKTER[319]	N/A	The "SIGINT Exchange designator" for Norway.[320]
DIRTYDEVIL[321]	Collection	GCHQ program that is "JTRIG's research network."[322] Listed as "design."[323]
DISCOROUTE[324]	Collection	NSA "tool specifically designed to suck up and database router configuration files seen in passively collected telnet sessions."[325]
DISHFIRE[326]	Database	"SMS data is flowing into DISHFIRE."[327]

314. Schneier, *supra* note 195.

315. *Id.*

316. *JTRIG Tools and Techniques*, *supra* note 131.

317. *Id.*

318. *Id.*

319. Wayne Madsen, *Senate Delivers Fatal End-of-Term Blow to Constitution*, INTREPID (Jan. 9, 2013), http://www.intrepidreport.com/archives/8588 (last visited Sept. 2, 2015) (on file with the Washington and Lee Law Review).

320. *Id.*

321. *JTRIG Tools and Techniques*, *supra* note 131.

322. *Id.*

323. *Id.*

324. *I Hunt Sys Admins*, THE INTERCEPT (Mar. 20, 2014), https://firstlook.org/theintercept/document/2014/03/20/hunt-sys-admins/ (last visited Aug. 25, 2015) (on file with the Washington and Lee Law Review).

325. *Id.*

326. *Id.*; Ball, *supra* note 97.

327. *The NSA in Germany: Snowden's Documents Available for Download*, *supra* note 122.

DISTANTFOCUS[328]	Collection	NSA program described as a pod that "is [a] new system for tactical SIGINT and precision geolocation . . . first deployed in December (S)."[329]
DISTILLERY[330]	Processing	Tactical Collection System . . . . "Stream-based platform for executing hacking identification applications."[331]
DOGHANDLER[332]	Collection	GCHQ program that is "JTRIG's development network."[333] Listed as "design."[334]
DRAGGABLEKITTEN[335]	Processing	NSA program that is described as "an XKEYSCORE Map/Reduce analytic that leverages the packets collected and made accessible to analytics by XKEYSCORE DEEPDIVE systems. DRAGGABBLEKITTEN identifies the QUANTUMTHEORY keywords in a packet capture and generates statistics for each service (currently Hotmail and Yahoo) to determine how often all of the keywords occur within a single packet."[336]

328. FVEYDOCS.ORG, https://fveydocs.org/search/definitions?q=NSA&page=3 (last visited Sept. 2, 2015) (on file with the Washington and Lee Law Review).

329. *Id*.

330. *NSA Nicknames and Codewords*, TOP LEVEL COMMS., http://electrospaces.blogspot.com/p/nicknames-and-codewords.html (last updated Oct. 24, 2015) (last visited Nov. 24, 2015) (on file with the Washington and Lee Law Review).

331. *Id*.

332. *JTRIG Tools and Techniques*, *supra* note 131.

333. *Id.*

334. *Id.*

335. *Menwith Hill Station Leverages XKeyscore for Quantum Against Yahoo and Hotmail*, THE INTERCEPT (Mar. 12, 2014), https://firstlook.org/theintercept/document/2014/03/12/menwith-hill-station-leverages-xkeyscore-quantum-yahoo-hotmail/ (last visited Aug. 25, 2015) (on file with the Washington and Lee Law Review).

336. *Id*.

DROPMIRE[337]	Collection	NSA exploit tool that is described as both "[p]assive collection of emanations using antenna" and "[l]aser printer collection, purely proximal access (***NOT*** implanted)."[338]
DRUID[339]	Processing	NSA designator that indicates information should be "shared with third parties, countries with NATO or defense treaty relationships with the United States."[340]
DYNAMO[341]	N/A	The "SIGINT Exchange designator" for Denmark.[342]
EINSTEIN[343]	Collection	A publicized DHS and NSA collaborative program that "called for telecommunications companies to route the Internet traffic of civilian agencies through a monitoring box that would search for and block computer codes designed to penetrate or otherwise compromise networks."[344]
ELATE[345]	Collection	A GCHQ "suite of tools for monitoring target use of the UK auction site eBay (www.ebay.co.uk). These tools are hosted on an Internet server, and the results are retrieved by encrypted email."[346]

337. Ewen MacAskill & Julian Borger, *New NSA Leaks Show How US Is Bugging Its European Allies*, THE GUARDIAN (June 30, 2013), http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies (last visited Sept. 2, 2015) (on file with the Washington and Lee Law Review).

338. *How Classified NSA Exploit Tools RADON and DEWSWEEPER Work*, INFOSEC INST. (Nov. 11, 2013), http://resources.infosecinstitute.com/classified-nsa-exploit-tools-radon-dewsweeper-work/ (last visited Sept. 6, 2015) (on file with the Washington and Lee Law Review).

339. Madsen, *supra* note 319.

340. *Id*.

341. *Id.*

342. *Id*.

343. Ellen Nakashima, *DHS Cybersecurity Plan Will Involve NSA, Telecoms*, WASH. POST (July 3, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/07/02/AR2009070202771.html (last visited Sept. 6, 2015) (on file with the Washington and Lee Law Review).

344. *Id.*

345. *JTRIG Tools and Techniques*, *supra* note 131.

346. *Id.*

ELEGANTCHAOS[347]	Processing	NSA program for "[a]nalysis of data at scale."[348]
ENDUE[349]	Database	NSA database where "some decrypts are placed . . . due to the sensitivity or fragility of the exploitation capability."[350]
EVENINGEASEL[351]	Collection	"The NSA conducts its surveillance of telephone conversations and text messages transmitted through Mexico's cell phone network under [this] internal code name."[352] This program was claimed to have been used to directly spy on the Mexican president.
EVILOLIVE[353]	Collection	NSA program that "capture[s] sensitive internet metadata—such as email logs, web browsing histories, and IP addresses, which can reveal location information—but not the content of email communications."[354]
EXCALIBUR[355]	Collection	GCHQ program that facilitates "Paltalk group chat collection."[356] Status listed as "beta release."[357]

347. GREENWALD, *supra* note 1, at 97.

348. *Id*.

349. *TOP SECRET STRAP 1 COMINT*, AM. C.L. UNION, https://www.aclu.org/sites/default/files/field_document/GCHQ%20Briefing%20on%20the%20BULLRUN%20Program.pdf.

350. *Id*.

351. Jens Glüsing, Laura Poitras, Marcel Rosenbach & Holger Stark, *Fresh Leak on US Spying: NSA Accessed Mexican President's Email*, SPIEGEL ONLINE INT'L (Oct. 20, 2013), http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html (last visited Aug. 27, 2015) (on file with the Washington and Lee Law Review).

352. *Id*.

353. Joshua Kopstein, *NSA Expanded Bulk Collection of Internet Data Under Newly Uncovered Surveillance Programs*, THE VERGE (June 27, 2013), http://www.theverge.com/2013 /6/27/4470442/nsa-surveillance-programs-bulk-collection-of-internet-metadata (last visited Aug. 25, 2015) (on file with the Washington and Lee Law Review).

354. *Id*.

355. *JTRIG Tools and Techniques*, *supra* note 131.

356. *Id.*

357. *Id.*

EXPOW[358]	Processing	"GCHQ's UIA capability provided by JTRIG."[359] Listed as "operational."[360]
FAIRVIEW[361]	Collection	NSA program that, "among others, filter[s] and gather[s] information at major telecommunications companies."[362]
FALLOUT[363]	Processing	One of two NSA programs that "appear to be a final layer of filtering to reduce the intake of information about Americans."[364]
FASCIA[365]	Database	"The SMS data is flowing into DISHFIRE and the corresponding call event data into FASCIA."[366]
FASHIONCLEFT[367]	Unknown	Found on an NSA slide with the explanation "Wrapped Exfil."[368]
FAST SCOPE[369]	Database	Listed on an NSA slide—"If the S2 QFD Review Panel elects to ask for HOMING PIGEON to be made persistent, its natural home would be incorporation into FAST SCOPE."[370]

358. *Id*.

359. *Id.*

360. *Id.*

361 GREENWALD, *supra* note 1, at 104.

362. *Id*.; Gorman & Valentino-Devries, *supra* note 199.

363. *NSA Slides Explain the PRISM Data-Collection Program*, *supra* note 273.

364. *Id*.

365. Gellman & Soltani, *supra* note 157; *NSA Documents Related to U.S. Spying in Germany*, INTERNET ARCHIVE, https://archive.org/stream/NSA-Surveillance-Germany-Snowden/ media-34084_djvu.txt (last visited Nov. 4, 2015) (on file with the Washington and Lee Law Review).

366. Gellman & Soltani, *supra* note 157.

367. *APEX VPN Phases Slide*, AM. C.L. UNION, https://www.aclu.org/sites/default/files/assets/vpn-and-voip-exploitation-with-hammerchant-and.pdf.

368. *Id*.

369. Danny Schechter, *REVIEW: Oh George Orwell, We Need You More Than Ever, Ever*, HUFFINGTON POST (May 23, 2014), http://www.huffingtonpost.com/danny-schechter/review-oh-george-orwell-w_b_5376870.html (last updated July 22, 2014) (last visited Sept. 6, 2015) (on file with the Washington and Lee Law Review)

370. *Id*.

FATYAK[371]	Collection	GCHQ program that is used for "public data collection from Linkedin [sic]."[372] Status listed as "in development."[373]
FOGGYBOTTOM[374]	Collection	This NSA program "records logs of Internet browsing histories and collects login details and passwords used to access websites and email accounts."[375]
FORESTWARRIOR[376]	Processing	GCHQ program that will be part of "JTRIG's new infrastructure"[377] serving as a "[d]esktop replacement for CERBERUS."[378] Status listed as "design."[379]
FOXACID[380]	Attack	"SECONDDATE can 'influence real-time communications between client and server' and to 'quietly redirect web-browsers' to NSA malware servers called FOXACID."[381]
FRONTO[382]	N/A	Listed as one of "[o]ther SIGINT Exchange Designators with Third and Fourth Parties."[383]

371. *JTRIG Tools and Techniques*, *supra* note 131.

372. *Id.*

373. *Id.*

374. Gallagher & Greenwald, *supra* note 235.

375. *Id.*

376. *JTRIG Tools and Techniques*, *supra* note 131.

377. *Id.*

378. *Id.*

379. *Id.*

380. *NSA Quantum Tasking Techniques for the R&T Analyst*, AM. C.L. UNION, https://www.aclu.org/files/natsec/nsa/20140130/%28TS%29%20NSA%20Quantum%20Tasking%20Techniques%20for%20the%20R&T%20Analyst.pdf.

381. Gallagher & Greenwald, *supra* note 235.

382. Madsen, *supra* note 319.

383. *Id.*

FRUIT BOWL[384]	Processing	GCHQ program that is a "CEREBERUS UIA Replacement and new tools infrastructure—Primary Domain for Generic User/Tools Access and TOR split into 3 sub-systems."[385] Listed as in "design."[386]
FUSEWIRE[387]	Collection	GCHQ program that "provides 24/7 monitoring of Vbulliten forums for target postings/online activity. Also allows staggered postings to be made."[388] Status not indicated.[389]
GAMBIT[390]	Collection	GCHQ "[d]eployable pocket-sized proxy server."[391] Status listed as "[i]n-development."[392]
GARLICK[393]	Collection	System with "which the NSA monitored satellite communication out of the Bavarian town of Bad Aibling for years."[394]
GATEWAY[395]	Attack	GCHQ program that provides the "[a]bility to artificially increase traffic to a website."[396] Status listed as "[r]eady to fire."[397]

384. *JTRIG Tools and Techniques*, *supra* note 131.

385. *Id.*

386. *Id.*

387. *Id.*

388. *Id.*

389. *Id.*

390. *Id.*

391. *Id.*

392. *Id.*

393. Laura Poitras et al., *How the NSA Targets Germany and Euro*pe, SPIEGEL ONLINE INT'L (July 1, 2013), http://www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609-2.html (last visited on Aug. 25, 2015) (on file with the Washington and Lee Law Review).

394. *Id.*

395. *JTRIG Tools and Techniques*, *supra* note 131.

396. *Id.*

397. *Id.*

GENIE[398]	Collection	NSA exploit tool that is a "multi-stage operation: jumping the airgap etc."[399]
GESTATOR[400]	Isolation	GCHQ program that provides "amplification of a given message, normally video, on popular multimedia websites (youtube)."[401] Status is not listed.[402]
GHOSTMACHINE[403]	Collection	"NSA's Special Source Operations cloud analytics platform."[404]
GILGAMESH[405]	Collection	Described in NSA documents as the "NSA geolocation system used by JSOC [Joint Special Operations Command]."[406]
GLASSBACK[407]	Attack	GCHQ program that uses "technique of getting a target's IP address by pretending to be a spammer and ringing them. Target does not need to answer."[408] Status listed as "fully operational."[409]

398. Schneier, *supra* note 195.

399. *Id*.

400. *JTRIG Tools and Techniques*, *supra* note 131.

401. *Id.*

402. *Id.*

403. *Raw List of NSA Nicknames and Codewords*, DECRYPTED MATRIX (May 19, 2014), https://decryptedmatrix.com/raw-list-of-nsa-nicknames-and-codewords/ (last visited Sept. 5, 2015) (on file with the Washington and Lee Law Review).

404. *Id*.

405. Jeremy Scahill & Glenn Greenwald, *The NSA's Secret Role in the U.S. Assassination Program*, THE INTERCEPT (Feb. 10, 2014, 12:03 AM), https://theintercept.com/2014/02/10/the-nsas-secret-role/ (last visited Dec. 7, 2015) (on file with the Washington and Lee Law Review).

406. *Id*.

407. *JTRIG Tools and Techniques*, *supra* note 131.

408. *Id.*

409. *Id.*

GLITTERBALL[410]	Isolation	GCHQ program that provides "Online Gaming Capabilities for Sensitive Operations. Currently Second Life."[411] Status is listed as "[i]n development."[412]
GODFATHER[413]	Collection	GCHQ program that facilitates "[p]ublic data collection from Facebook."[414] Status listed as "[f]ully operational."[415]
GOODFELLA[416]	Collection	GCHQ program that is a "[g]eneric framework for public data collection from Online Social Networks."[417] Status listed as "[i]n development."[418]
GRANDMASTER[419]	Processing	DNI processing system, which has evolved "from GRANDMASTER to WEALTHYCLUSTER, and in the future, TURMOIL."[420]
GROK[421]	Collection	NSA program "used to log keystrokes."[422]
GUMFISH[423]	Collection	NSA program that "can covertly take over a computer's webcam and snap photographs."[424]
GURKHAS SWORD[425]	Isolation	GCHQ program that consists of "[b]eaconed Microsoft Office Documents to elicit a targets [sic] IP address."[426]

410. *Id.*
411. *Id.*
412. *Id.*
413. *Id.*
414. *Id.*
415. *Id.*
416. *Id.*
417. *Id.*
418. *Id.*
419. Marc Ambinder, *The NSA's Big Problem, Explained by the NSA*, THE WEEK, http://theweek.com/articles/446002/nsas-big-problem-explained-by-nsa (last visited Sept. 7, 2015) (on file with the Washington and Lee Law Review).
420. *Id.*
421. Gallagher & Greenwald, *supra* note 235.
422. *Id.*
423. *Id.*
424. *Id.*
425. *JTRIG Tools and Techniques*, *supra* note 131.
426. *Id.*

HACIENDA[427]	Processing	GCHQ program that "is a port scanning tool designed to scan an entire country or city. It uses GEOFUSION to identify IP locations."[428]
HAPPYFOOT[429]	Processing	NSA program that "helps the NSA to map Internet addresses to physical locations more precisely than is possible with traditional Internet geolocation services."[430]
HAVOK[431]	Isolation	GCHQ program that provides a "[r]eal-time website cloning technique allowing on-the-fly alterations."[432]
HEADMOVIES[433]	Collection	Listed as "United Kingdom—Collection Information" with Validator ID of "6210000230."[434]
HIGHCASTLE[435]	Processing	"[F]or voice processing and analysis and reporting."[436]
HIGHLANDS[437]	Collection	NSA exploit tool that, according to Bruce Schneier, involves "[c]ollection from Implants."[438]
HOMEBASE[439]	Isolation	NSA program that, according to Marc Ambinder, is a "[t]actical tasking tool for digital network identification."[440]

427. *Id.*

428. *Id.*

429. Ashkan Soltani, Andrea Petersen & Barton Gellman, *NSA Uses Google Cookies to Pinpoint Targets for Hacking*, WASH. POST (Dec. 10, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking/ (last visited Sept. 6, 2015) (on file with the Washington and Lee Law Review).

430. *Id.*

431. *JTRIG Tools and Techniques*, *supra* note 131.

432. *Id.*

433. *United Kingdom—Collection Information*, *supra* note 174.

434. *Id.*

435. *Id.*

436. *European Security Center to Begin Operations*, SPIEGEL ONLINE INT'L, http://www.spiegel.de/ media/media-34070.pdf.

437. Schneier, *supra* note 195.

438. *Id.*

439. Ambinder, *supra* note 134.

440. *Id.*

HOME PORTAL[441]	Unknown	GCHQ "central hub for all JTRIG Cerberus tools."[442]
HOMING PIGEON[443]	Unknown	Listed in NSA documents as follows: "If the S2 QFD Review Panel elects to ask for HOMING PIGEON to be made persistent, its natural home would be incorporation into FASTSCOPE."[444]
HUSK[445]	Isolation	GCHQ program that provides a "[s]ecure one-to-one web based dead-drop messaging platform."[446]
ICE[447]	Collection	GCHQ program that "is an advance IP harvesting technique."[448] Status is not listed.[449]
ICREACH[450]	Processing	NSA program described as follows: "ICREACH contains information on the private communications of foreigners and, it appears, millions of records on American citizens who have not been accused of any wrongdoing."[451] Often referred to as "Google-like."[452]
IMPERIALBARGE[453]	Attack	GCHQ program "[f]or connecting two target phone[s] together in a call."[454] Status is listed as "[t]ested."[455]
INDRA[456]	Unknown	Listed in NSA documents under "FORNSAT 1."[457]

441. *JTRIG Tools and Techniques*, *supra* note 131.
442. *Id.*
443. GREENWALD, *supra* note 1, at 166.
444. *Id.*
445. *JTRIG Tools and Techniques*, *supra* note 131.
446. *Id.*
447. *Id.*
448. *Id.*
449. *Id.*
450. Gallagher, *supra* note 95.
451. *Id.*
452. *Id.*
453. *JTRIG Tools and Techniques*, *supra* note 131.
454. *Id.*
455. *Id.*
456. GREENWALD, *supra* note 1, at 117.
457. *Id.*

INSPECTOR[458]	Collection	GCHQ "tool for monitoring domain information and site availability."[459] Status listed as "fully operational."[460]
INTERQUAKE[461]	Collection	"Terrestrial Environmental Knowledge Base. Available to all NSA analysts and partners."[462]
IRONSAND[463]	Unknown	Listed in NSA documents under "FORNSAT 1."[464]
ISHTAR[465]	N/A	The "SIGINT Exchange designator" for Japan.[466]
JACKKNIFE[467]	Unknown	Listed in NSA documents under "FORNSAT 1."[468]
JAZZ FUSION[469]	Database	GCHQ program that is a "BOMBAYROLL Replacement which will also incorporate new collectors—Primary Domain for Dedicated Connections split into 3 sub-systems."[470] Listed as "implementation."[471]

458. *JTRIG Tools and Techniques*, *supra* note 131.

459. *Id.*

460. *Id.*

461. *The NSA in Germany: Snowden's Documents Available for Download*, *supra* note 122.

462. *Id.*

463. GREENWALD, *supra* note 1, at 117.

464. *Id.*

465. Madsen, *supra* note 319.

466. *Id.*

467. GREENWALD, *supra* note 1, at 117.

468. *Id.*

469. *JTRIG Tools and Techniques*, *supra* note 131.

470. *Id.*

471. *Id.*

JEDI[472]	Unknown	This is a GCHQ program or object. The description provided states: "JTRIG will shortly be rolling out a JEDI pod to every desk of every member of an intelligence Production Team. The challenge is to scale up to over 1,200 users whilst remaining agile, efficent [sic] and responsive to customer needs."[473]
JTRIG[474]	N/A	This is a GCHQ collection of "[t]ools and techniques . . . developed by various teams."[475] One of the largest collections of tools of all types.
JTRIG RADIANT SPLENDOUR[476]	Collection	GCHQ "'Data Diode'" connecting the CERBERUS network with GCNET."[477] Status listed as "operational."[478]
JUGGERNAUT[479]	Collection	"NSA has been forwarding SMS data from it's [sic] JUGGERNAUT GSM collection platform since 2007."[480]

472. *Id*.

473. *Id*.

474. *Id*.

475. *Id*.

476. *Id*.

477. *Id*.

478. *Id*.

479. *GHOSTMACHINE: The NSA's Cloud Analytics Platform*, WASH. POST, http://apps.washingtonpost.com/g/page/world/ghostmachine-the-nsas-cloud-analytics-platform/644/#document/p2/a135401 (last visited Sept. 6, 2015) (on file with the Washington and Lee Law Review).

480. *SIGDEV Conference*, SPECIAL COLLECTION SERV. (March 2011), http://nsarchive.gwu.edu/NSAEBB/NSAEBB506/docs/ciasignals_41.pdf.

KOALAPUNCH[481]	Collection	Listed in "United Kingdom—Collection Information" with Validator ID of "610210091."[482]
LADYLOVE[483]	Processing	"Automatically processes . . . signals of interest" from BOTANICREALTY.[484]
LANDINGPARTY[485]	Processing	GCHQ "tool for auditing dissemination of VIKING PILLAGE data."[486] Status listed as "fully operational."[487]
LIFESAVER[488]	Collection	NSA exploit tool that provides "[i]maging of the [h]ard [d]rive."[489]
LITHIUM[490]	Collection	NSA program that "among others, filter[s] and gather[s] information at major telecommunications companies."[491]
LOCKSTOCK[492]	Collection	NSA program described as "[a]n eight-year, $51 million contract to process 'all MYSTIC data and data for other NSA accesses' at a facility in Annapolis Junction, Maryland, down the road from NSA's headquarters."[493]

481. *United Kingdom—Collection Information*, *supra* note 174.

482. *Id*.

483. GREENWALD, *supra* note 1, at 117.

484. *The NSA in Germany: Snowden's Documents Available for Download*, *supra* note 122.

485. *JTRIG Tools and Techniques*, *supra* note 131.

486. *Id.*

487. *Id.*

488. Schneier, *supra* note 195.

489. *Id*.

490. Gorman & Valentino-Devries, *supra* note 199.

491. *Id*.

492. Ryan Devereaux, Glenn Greenwald & Laura Poitras, *Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas*, THE INTERCEPT (May 19, 2014), https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ (last visited Nov. 11, 2015) (on file with the Washington and Lee Law Review).

493. *Id*.

LONGRUN[494]	Collection	Joint GCHQ/NSA program described as a "[d]ata reconnaissance tool developed by the CITD team in JTRIG[,] Port Scans entire countries[,] [u]ses nmap as port scanning tool[,] [u]ses GEOGUSION for IP Geolocation[,] [r]andomly scans every IP identified for that country."[495]
LONGSHOT[496]	Collection	GCHQ "[f]ile-upload and sharing website."[497]
LOPERS[498]	Unknown	Described only as "40.940, 994, 147 Records."[499]
LUMP[500]	Isolation	GCHQ "system that finds the avatar name from a SecondLife AgentID."[501]
LUTEUSICARUS[502]	Collection	Listed as "United Kingdom—Collection Information" with a validator ID of "100033767."[503]
MAGNETIC[504]	Collection	According to Bruce Schneier, this NSA exploit tool involves the "Sensor Collection of Magnetic Emanations."[505]
MAGNUMOPUS[506]	Collection	Listed in "United Kingdom—Collection Information" with Validator ID of "100032919" and "611000994."[507]

494. Julian Kirsch et al., *The HACIENDA Program for Internet Colonization*, HEISE ONLINE (Aug. 15, 2014), http://www.heise.de/ct/artikel/NSA-GCHQ-The-HACIENDA-Program-for-Internet-Colonization-2292681.html?hg=1&hgi=18 (last visited Sept. 6, 2015) (on file with the Washington and Lee Law Review).

495. *Id.*

496. *JTRIG Tools and Techniques*, *supra* note 131.

497. *Id.*

498. GREENWALD, *supra* note 1, at 139.

499. *Id.*

500. *JTRIG Tools and Techniques*, *supra* note 131.

501. *Id.*

502. *United Kingdom—Collection Information*, *supra* note 174.

503. *Id.*

504. Schneier, *supra* note 195.

505. *Id.*

506. *United Kingdom—Collection Information*, *supra* note 174.

507. *Id.*

MAIN CORE[508]	Database	NSA database that "reportedly collects and stores vast amounts of personal and financial data about millions of Americans."[509]
MAINWAY[510]	Database	According to Marc Ambinder, this is an NSA "[t]elephony metadata collection database."[511] The SCISSORS program "sort[s] data types for analysis in NUCLEON (voice), PINWALE (video), MAINWAY (call records), and MARINA (Internet records)."[512]
MARINA[513]	Database	Marc Ambinder describes this as an "Internet metadata collection database."[514] The SCISSORS program "sort[s] data types for analysis in NUCLEON (voice), PINWALE (video), MAINWAY (call records), and MARINA (Internet records)."[515]
MESSIAH/WHAMI[516]	Database	According to Marc Ambinder, this NSA program is an "[e]lectronic intelligence processing and analytical database."[517]
METROTUBE[518]	Processing	Described on an NSA slide simply as "[a]nalytic."[519]

508. Tim Shorrock, *Main Core: New Evidence Reveals Top Secret Government Database Used in Bush Spy Program*, DEMOCRACY NOW! (July 25, 2008), http://www.democracynow.org/2008/7/25/main_core_new_evidence_reveals_top (last visited Sept. 8, 2015) (on file with the Washington and Lee Law Review).

509. *Id.*

510. Schneier, *supra* note 195.

511. Ambinder, *supra* note 134.

512. *NSA Slides Explain the PRISM Data-Collection Program*, *supra* note 273.

513. GREENWALD, *supra* note 1, at 160.

514. Ambinder, *supra* note 134.

515. *NSA Slides Explain the PRISM Data-Collection Program*, *supra* note 273.

516. Ambinder, *supra* note 134.

517. *Id.*

518. *Turmoil VPN Processing*, SNOWDEN DOC SEARCH, https://search.edwardsnowden.com/docs/TurmoilVPNProcessing20141228 (last visited Sept. 8, 2015) (on file with the Washington and Lee Law Review).

519. *Id.*

MIDDLEMAN[520]	Processing	GCHQ "distributed real-time event aggregation, tip-off and tasking platform utilized by JTRIG as a middleware layer."[521]
MINERALIZE[522]	Collection	NSA exploit tool that provides "[c]ollection from LAN implant."[523]
MINIATURE HERO[524]	Collection	GCHQ program the provides "[a]ctive [S]kype capability. Provision of real time call records (SkypeOut and SkypetoSkype) and bidirectional instant messaging. Also contact lists."[525] Status is listed as "fully operational, but note usage restrictions."[526]
MIRAGE[527]	Unknown	Unknown.
MOBILEHOOVER[528]	Isolation	GCHQ "tool to extract data from field forensics' reports created by Celidek, Cellegrite, XRY, Snoopy and USIM detective. These reports are transposed into a Newpin XML format to upload to Newpin."[529]
MOLTEN-MAGMA[530]	Collection	GCHQ program that is a "CGI HTTP Proxy with ability to log all traffic and perform HTTPS Man in the Middle."[531]

520. *JTRIG Tools and Techniques*, *supra* note 131.
521. *Id.*
522. Schneier, *supra* note 195.
523. *Id.*
524. *JTRIG Tools and Techniques*, *supra* note 131.
525. *Id.*
526. *Id.*
527. *Id.*
528. *Id.*
529. *Id.*
530. *Id.*
531. *Id.*

MONSTERMIND[532]	Attack	NSA program that is described as "an automatic strike-back system for cyberattacks. The program, disclosed here for the first time, would automate the process of hunting for the beginnings of a foreign cyberattack. Software would constantly be on the lookout for traffic patterns indicating known or suspected attacks. When it detected an attack, MonsterMind would automatically block it from entering the country—a 'kill' in cyber terminology. Programs like this had existed for decades, but MonsterMind software would add a unique new capability: Instead of simply detecting and killing the malware at the point of entry, MonsterMind would automatically fire back, with no human involvement."[533]
MOONLIGHTPATH[534]	Collection	Part of a "joint surveillance collection operation with an unnamed partner agency yielded a new program 'to query metadata' that was 'turned on in the Fall 2012.' Two others, called MoonLightPath and Spinneret, 'are planned to be added by September 2013.'"[535]
MOONPENNY[536]	Unknown	Listed under "FORNSTAT 1."[537]

532. Bruce Schneier, *New Snowden Interview in Wired*, SCHNEIER ON SECURITY (Aug. 14, 2014), https://www.schneier.com/blog/archives/2014/08/new_snowden_int.html (last visited Sept. 8, 2015) (on file with the Washington and Lee Law Review).

533. *Id.*

534. James Bamford, *The Most Wanted Man in the World*, WIRED (Aug. 22, 2014), http://www.wired.com/2014/08/edward-snowden#ch-1 (last visited Sept. 4, 2015) (on file with the Washington and Lee Law Review).

535. *Id.*

536. GREENWALD, *supra* note 1.

537. *Id.*

MOUTH[538]	Collection	GCHQ program that serves as a "[t]ool for collection for downloading a user's files from archive.org."[539] Status is listed as "[f]ully operational."[540]
MTI[541]	Collection	A joint NSA/GCHQ program that stands for "Mastering the Internet—[was created] to collect a significant amount of the world's communications."[542]
MUGSHOT[543]	Processing	"[W]ith MUGSHOT the GCHQ integrates results from active scans (HACIENDA) as well as passive monitoring (Figure 26), to 'understand everything important about all machines on the Internet.'"[544]

538. *JTRIG Tools and Techniques*, *supra* note 131.

539. *Id.*

540. *Id.*

541. Henry Porter, *GCHQ Revelations: Mastery of the Internet Will Mean Mastery of Everyone*, THE GUARDIAN (June 21, 2013), http://www.theguardian.com/commentisfree/2013/jun/21/gchq-mastery-internet-mastery-everyone (last visited Sept. 6, 2015) (on file with the Washington and Lee Law Review).

542. *Id.*

543. Kirsch et al., *supra* note 494.

544. *Id.*

MUSCULAR[545]	Collection	A "GCHQ special source access."[546] This is part of the NSA's WINDSTOP project, and "is used to break in to the internal 'cloud' networks of Google and Yahoo which goes by the alphanumeric designator DS-200B."[547]
MUSKETEER[548]	Collection	NSA program that feeds SHELLTRUMPET and is listed as a "Second Party system[]."[549]
MUSTANG[550]	Collection	GCHQ program that "provides covert access to the locations of GSM cell towers."[551] Status is listed as "[f]ully operational."[552]
MYSTIC[553]	Collection	An NSA SSO "SHELLTRUMPET is currently processing Two Billion call events/day from select SSO (Ram-M, OAKSTAR, MYSTIC and NCSC enabled systems)."[554]

545. Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html (last visited Sept. 6, 2015) (on file with the Washington and Lee Law Review).

546. *The NSA in Germany: Snowden's Documents Available for Download*, *supra* note 122.

547. *One Month, Hundreds of Millions of Records Collected*, WASH. POST, http://apps.washingtonpost.com/g/page/world/one-month-hundreds-of-millions-of-records-collected/554/ (last visited Aug. 28, 2015) (on file with the Washington and Lee Law Review).

548. GREENWALD, *supra* note 1, at 100.

549. *Id.*

550. *JTRIG Tools and Techniques*, *supra* note 131.

551. *Id.*

552. *Id.*

553. GREENWALD, *supra* note 1, at 100.

554. *Id.*

NAMEJACKER[555]	Isolation	GCHQ program that is a "web service and admin console for the translation of usernames between networks. For use with gateways and other such technologies."[556]
NCSC[557]	Collection	An NSA SSO "SHELLTRUMPET is currently processing Two Billion call events/day from select SSO (Ram-M, OAKSTAR, MYSTIC and NCSC enabled systems)."[558]
NEVIS[559]	Isolation	GCHQ "tool developed by NTAC to search disk images for signs of possible Encryption products. CMA have further developed this tool to look for signs of Steganography."[560]
NEWPIN[561]	Database	A GCHQ "database of C2C identifiers obtained from a variety of unique sources, and a suite of tools for exploring this data."[562]
NIAGARAFILES[563]	Processing	Listed in "'Real Time' Analytics" and is "filed based" and "starting to gain experience."[564]
NIGHTCRAWLER[565]	Collection	GCHQ program that is a "[p]ublic online group against dodgy websites."[566]

555. *JTRIG Tools and Techniques*, *supra* note 131.

556. *Id.*

557. GREENWALD, *supra* note 1, at 100.

558. *Id.*

559. *JTRIG Tools and Techniques*, *supra* note 131.

560. *Id.*

561. *Id.*

562. *Id.*

563. *The NSA in Germany: Snowden's Documents Available for Download*, *supra* note 122.

564. *Id.*

565. *JTRIG Tools and Techniques*, *supra* note 131.

566. *Id.*

NKB[567]	Collection	Intelligence Analysis Intern used BLACKPEARL and "successfully located, identified, and submitted several new targets."[568]
NUCLEON[569]	Database	NSA database that, according to Marc Ambinder, is a "[g]lobal telephone content database."[570] The SCISSORS program "sort[s] data types for analysis in NUCLEON (voice), PINWALE (video), MAINWAY (call records), and MARINA (Internet records)."[571]
NUTALLERGY[572]	Collection	GCHQ program that serves as a "JTRIG Tor web browser—Sandbox IE replacement and FRUITBOWL sub-system."[573] Listed as a "pilot."[574]
NYMROD[575]	Processing	NYMROD is a "name matching system" that "can accept queries consisting of personal names."[576]
OAKSTAR[577]	Collection	An NSA SSO "SHELLTRUMPET is currently processing Two Billion call events/day from select SSO (Ram-M, OAKSTAR, MYSTIC and NCSC enabled systems)."[578]

567. *The NSA in Germany: Snowden's Documents Available for Download*, *supra* note 122.

568. *Id.*

569. Barton Gellman, *U.S. Surveillance Architecture Includes Collection of Revealing Internet, Phone Metadata*, WASH. POST (June 15, 2013) https://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html (last visited Dec. 14, 2015) (on file with the Washington and Lee Law Review).

570. *Id.*; Ambinder, *supra* note 134; Somerville, *supra* note 134.

571. *NSA Slides Explain the PRISM Data-Collection Program*, *supra* note 273.

572. *JTRIG Tools and Techniques*, *supra* note 131.

573. *Id.*

574. *Id.*

575. *Content Extraction Analytics,* CTR. FOR CONTENT EXTRACTION (2009), http://www.spiegel.de/media/media-34089.pdf.

576. *Id.*

577. GREENWALD, *supra* note 1, at 100.

578. *Id.*

OCEAN[579]	Collection	NSA exploit tool that provides "[o]ptical [c]ollection [s]ystem for Raster-Based [c]omputer [s]creens."[580]
OCTAVE[581]	Collection	NSA program described as a "[c]ollection mission tasking tool."[582]
OILSTOCK[583]	Collection	Marc Ambinder claims that this is an "Air Force/Navy tool to track ships in real time."[584]
OLYMPIA[585]	Processing	NSA program described as "CSEC's Network Knowledge Engine," "[v]arious data sources," "[c]hained enrichments," and "[a]utomated analysis."[586]
ONEROOF[587]	Database	NSA database that, according to Marc Ambinder, is the "[m]ain tactical SIGINT database (Afghanistan), consisting of raw and unfiltered intercepts."[588]
OPTICNERVE[589]	Collection	A GCHQ program that "collected still images of Yahoo webcam chats in bulk and saved them to agency databases, regardless of whether individual users were an intelligence target or not."[590]
ORANGEBLOSSOM[591]	Unknown	Listed in NSA slides as having "DNR capability."[592]

579. Schneier, *supra* note 195.

580. *Id.*

581. Ambinder, *supra* note 134.

582. *Id.*

583. *Id.*

584. *Id.*

585. GREENWALD, *supra* note 1, at 94.

586. *Id.*

587. Ambinder, *supra* note 134.

588. *Id.*; Somerville, *supra* note 134.

589. Spencer Ackerman & James Ball, *Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ*, THE GUARDIAN (Feb. 27, 2014), http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo (last visited Dec. 14, 2015) (on file with the Washington and Lee Law Review).

590. *Id.*

591. GREENWALD, *supra* note 1, at 106.

592. *Id.*

ORANGECRUSH[593]	Collection	NSA program that, as "part of the OAKSTAR program under SSO's corporate portfolio, began forwarding metadata from a third party partner site (Poland) to NSA repositories as of 3 March and content as of 25 March. This program is a collaborative effort between SSO, NCSC, ETC, FAD, an NSA Corporate Partner and a division of the Polish Government. ORANGECRUSH is only known to the Poles as BUFFALOGREEN. This multi-group partnership began in May 2009 and will incorporate the OAKSTAR project of ORANGEBLOSSOM and its DNR capability. The new access will provide SIGINT from commercial links managed by the NSA Corporate Partner and is anticipated to include Afghan National Army, Middle East, limited African continent, and European communications. A notification has been posted to SPRINGRAY and this collection is available to Second Parties via TICKETWINDOW."[594]
OSN[595]	Collection	NSA social media collection and life mapping tool. Slides indicate reasons to use this as "Targets increasing usage of Facebook, BEBO, MySpace etc. . . . A very rich source of information on targets: . . . Personal details . . . 'Pattern of Life' . . . Connections to associates . . . Media."[596]
OUTWARD[597]	Processing	GCHQ "collection of DNS lookup, WHOIS Lookup and other network tools."[598]

593. *Id.*
594. *Id.*
595. *Id.* at 161.
596. *Id.*
597. *JTRIG Tools and Techniques*, *supra* note 131.
598. *Id.*

PACKAGEDGOODS[599]	Processing	NSA program that "tracks the 'traceroutes' through which data flows around the Internet. Through Packaged Goods, the N.S.A. has gained access to '13 covered servers in unwitting data centers around the globe,' according to the PowerPoint. The document identifies a list of countries where the data centers are located, including Germany, Poland, Denmark, South Africa and Taiwan as well as Russia, China and Singapore."[600]
PANOPLY[601]	Processing	"[P]opulates IQ with emitter information and reports including: signal externals, radio and payload information, LACs and cell ID's, protocol stacks."[602]
PARCHDUSK[603]	Collection	From an NSA slide in collaboration with the Texas Cryptologic Center, listed as a Production Operation. Der Spiegel describes this program as follows: "Operations using the OLYMPUS spyware during the 2007 and 2008 fiscal years, FOXACID spam operations, and operations with the spying programs SHARPFOCUS and PARCHDUSK."[604]
PBX[605]	Unknown	NSA program described as "Public Branch Exchange Switch."[606]

599. James Risen & Laura Poitras, *NSA Report Outlined Goals for More Power*, N.Y. TIMES (Nov. 22, 2013), http://www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html?pagewanted=all (last visited Sept. 8, 2015) (on file with the Washington and Lee Law Review).

600. *Id.*

601. *Pacific SIGDEV Conference Slides*, SPIEGEL ONLINE INT'L, http://www.spiegel.de/media/media-34100.pdf.

602. *Id.*

603. *Photo Gallery: NSA's TAO Unit Introduces Itself*, SPIEGEL ONLINE INT'L (Dec. 30, 2013), http://www.spiegel.de/fotostrecke/photo-gallery-nsa-s-tao-unit-introduces-itself-fotostrecke-105372.html (last visited Sept. 8, 2015) (on file with the Washington and Lee Law Review).

604. *Id.*

605. GREENWALD, *supra* note 1, at 147.

606. *Id.*

PHOTONTORPEDO[607]	Attack	GCHQ program that is "[a] technique to actively grab the IP address of an MSN messenger user."[608] Status is listed as "[o]perational, but usage restrictions."[609]
PICASSO[610]	Isolation	NSA device that is a "Modified GSM (target) handset that collects user data, location information and room audio. Command and data exfil is done from a laptop and regular phone via SMS (Short Messaging Service), without alerting the target."[611]
PINWALE[612]	Database	NSA program that is described as an "Internet data content database."[613] "[P]ersona session collection (where the data is collected and forwarded to NSA's PINWALE . . .)."[614] The SCISSORS program "sort[s] data types for analysis in NUCLEON (voice), PINWALE (video), MAINWAY (call records), and MARINA (Internet records)."[615]
PISTRIX[616]	Collection	GCHQ program that is an "image hosting and sharing website."[617]
PODRACE[618]	Collection	GCHQ program that is "JTRIG's MS update farm."[619] Status is listed as "design."[620]

607. *JTRIG Tools and Techniques*, *supra* note 131.

608. *Id.*

609. *Id.*

610. Bruce Schneier, *PICASSO: NSA Exploit of the Day*, SCHNEIER ON SECURITY (Feb. 17, 2014), https://www.schneier.com/blog/archives/2014/02/picasso_nsa_exp.html (last visited Sept. 8, 2015) (on file with the Washington and Lee Law Review).

611. *Id.*

612. GREENWALD, *supra* note 1, at 160.

613. Ambinder, *supra* note 134; Somerville, *supra* note 134.

614. *The NSA in Germany: Snowden's Documents Available for Download*, *supra* note 122.

615. *NSA Slides Explain the PRISM Data-Collection Program*, *supra* note 273.

616. *JTRIG Tools and Techniques*, *supra* note 131.

617. *Id.*

618. *Id.*

619. *Id.*

620. *Id.*

PREDATORSFACE[621]	Attack	GCHQ program that provides "Targeted Denial Of Service against Web Servers."[622] Status is not listed.[623]
PREFER[624]	Collection	This NSA "program uses automated text messages such as missed call alerts or texts sent with international roaming charges to extract information, which the agency describes as 'content-derived metadata,' and explains that 'such gems are not in current metadata stores and would enhance current analytics.' On average, each day the NSA was able to extract: • More than 5 million missed-call alerts, for use in contact-chaining analysis (working out someone's social network from who they contact and when) • Details of 1.6 million border crossings a day, from network roaming alerts • More than 110,000 names, from electronic business cards, which also included the ability to extract and save images. • Over 800,000 financial transactions, either through text-to-text payments or linking credit cards to phone users."[625]
PRESSUREWAVE[626]	Database	Described on a NSA slide as being fed "IKE Full take metadata (files)" and "Selected Decrypted Content" from "TURMOIL."[627]
PRIMATE[628]	Processing	GCHQ "JTRIG tool that aims to provides [sic] the capability to identify trends in seized computer media data and metadata."[629]

621. *Id.*
622. *Id.*
623. *Id.*
624. Ball, *supra* note 97.
625. *Id.*
626. Gallagher & Greenwald, *supra* note 235.
627. *Id.*
628. *JTRIG Tools and Techniques*, *supra* note 131.
629. *Id.*

PRINTAURA[630]	Collection	NSA program that is part of PRISM, this "automates the traffic flow."[631]
PRISM[632]	Collection	"PRISM is the most cited collection source in NSA 1st Party end-product reporting. More NSA product reports were based on PRISM than on any other single SIGAD for all of NSA's 1st Party reporting during FY12: cited in 15.1% of all reports (up from 14% in FYll). PRISM was cited in 13.4% of all 1st, 2nd, and 3rd Party NSA reporting (up from 11.9% in FYll), and is also the top cited SIGAD overall."[633] "PRISM is a tool used by the [NSA] to collect private electronic data belonging to URLs [uniform resource locator] of major internet services like Gmail, Facebook, Outlook, and others."[634] "Material collected through Prism is routinely shared with the FBI and CIA, with one NSA document describing the program as a 'team sport.'"[635] The NSA's Special Source Operations (SSO) division is responsible for all programs directed at U.S. communications systems through corporate partnerships like PRISM.[636] The sharing between the NSA, the FBI and the CIA has automated aspects that "enable[] [them] to see which selectors [search terms] the National Security Agency has tasked to Prism."[637]

630. GREENWALD, *supra* note 1, at 116.

631. *Id.*; *NSA Slides Explain the PRISM Data-Collection Program*, *supra* note 273.

632. GREENWALD, *supra* note 1, at 111.

633. *Id.*

634. T.C. Sottek & Joshua Kopstein, *Everything You Need to Know About PRISM*, THE VERGE (July 17, 2013), http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet (last visited Sept. 4, 2015) (on file with the Washington and Lee Law Review).

635. *Id.*

636. *Id.*

637. *Id.*

PROTON[638]	Database	NSA database that is described by Marc Ambinder as "SIGINT database for time-sensitive targets/counterintelligence."[639]
QUANTUMBISCUIT[640]	Attack	Listed as a joint NSA/GCHQ tool for "[r]edirection based on keywork" and "Mostly HTML Cookie Values."[641]
QUANTUMBOT[642]	Attack	Listed as a joint NSA/GCHQ tool for "IRC botnet hijacking."[643]
QUANTUMCOPPER[644]	Attack	Listed as a joint NSA/GCHQ tool for "[f]ile download disruption."[645]
QUANTUMDNS[646]	Attack	Listed as a joint NSA/GCHQ tool for "DNS Hijacking" and "Caching Nameservers."[647]
QUANTUMSQUIRREL[648]	Isolation	Listed as a joint NSA/GCHQ tool for "[t]ruly covert infrastructure, be any IP in the world."[649]
QUINCY[650]	Processing	GCHQ program that "is an enterprise level suite of tools for the exploitation of seized media."[651]
RADON[652]	Attack	NSA exploit tool that provides "[b]i-directional host tap that can inject Ethernet packets onto the same targets. Allows bi-directional exploitation of denied networks using standard on-net tools."[653]

638. GREENWALD, *supra* note 1, at 152.
639. Ambinder, *supra* note 134; Somerville, *supra* note 134.
640. *The NSA and GCHQ's QUANTUMTHEORY Hacking Tactics*, *supra* note 298.
641. *Id.*
642. *Id.*
643. *Id.*
644. *Id.*
645. *Id.*
646. *Id.*
647. *Id.*
648. *Id.*
649. *Id.*
650. *JTRIG Tools and Techniques*, *supra* note 131.
651. *Id.*
652. Schneier, *supra* note 195.
653. *Id.*

RAM-M[654]	Unknown	Described in NSA documents in the following sentence: "SHELLTRUMPET is currently processing Two Billion call events/day from select SSO (Ram-M, OAKSTAR, MYSTIC and NCSC enabled systems)."[655]
RAMPART-T[656]	Collection	NSA program that "has to do with penetration of hard targets at or near the leadership level, in other words: heads of state and their closest aides."[657]
RANA[658]	Unknown	GCHQ "system developed by ICTR-CISA providing CAPTCHA-solving via a web service on CERBERUS. This is intended for use by BUMPERCAR+ and possibly in future by SHORTFALL but anyone is welcome to use it."[659]
RC-10[660]	Collection	NSA program "that increased the agency's capacity to suck up and process all-source communications intelligence by a factor of 10."[661]
REAPER[662]	Collection	GCHQ's "Cerberus-> GCNET Import Gateway Interface System."[663] Listed as "operational."[664]

654. *JTRIG Tools and Techniques*, *supra* note 131.

655. *Id.*

656. Laura Poitras, Marcel Rosenbach & Holger Stark, *Codename 'Apachee': How America Spies on Europe and the UN*, SPIEGEL ONLINE INT'L (Aug. 26, 2013), http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html (last visited Aug. 26, 2015) (on file with the Washington and Lee Law Review).

657. *Id.*

658. *JTRIG Tools and Techniques*, *supra* note 131.

659. *Id.*

660. Marc Ambinder, *The Quick Read: Obama's Wars, by Bob Woodward*, THE ATLANTIC (Sept. 27, 2010), http://www.theatlantic.com/politics/archive/2010/09/the-quick-read-obamas-wars-by-bob-woodward/63586/ (last visited Aug. 26, 2015) (on file with the Washington and Lee Law Review).

661. *Id.*

662. *JTRIG Tools and Techniques*, *supra* note 131.

663. *Id.*

664. *Id.*

RESERVOIR[665]	Collection	GCHQ's "Facebook application allowing collection of various information."[666] Status is listed as "[f]ully operational, but note operational restrictions."[667]
RETRO[668]	Collection	NSA program under the "voice interception program, called MYSTIC, [which] began in 2009. Its RETRO tool, short for 'retrospective retrieval,' and related projects reached full capacity against the first target nation in 2011." "The call buffer opens a door 'into the past,' the summary says, enabling users to 'retrieve audio of interest that was not tasked at the time of the original call.' Analysts listen to only a fraction of 1 percent of the calls, but the absolute numbers are high. Each month, they send millions of voice clippings, or 'cuts,' for processing and long-term storage."[669]
ROADBED[670]	Collection	Intelligence Analysis Intern used BLACKPEARL and "successfully located, identified, and submitted several new targets."[671]
ROLLINGTHUNDER[672]	Attack	GCHQ program that provides "[d]istributed denial of service using P2P. Built by ICTR, deployed by JTRIG."[673] Status is not listed.[674]

665. *Id.*

666. *Id.*

667. *Id.*

668. Barton Gellman & Ashkan Soltani, *NSA Surveillance Program Reaches 'Into the Past' to Retrieve, Replay Phone Calls*, WASH. POST (Mar. 18, 2014), http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html (last visited Sept. 4, 2015) (on file with the Washington and Lee Law Review).

669. *Id.*

670. *Starting Up a New Mission at the European Security Operations Center: End-to-End SIGINT*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/files/2014/06/23/esoc_report_on_the_experiences_of_one_nsa_worker.pdf.

671. *Id.*

672. *JTRIG Tools and Techniques*, *supra* note 131.

673. *Id.*

674. *Id.*

SALVAGERABBIT[675]	Collection	NSA program that "exfiltrates data from removable flash drives that connect to an infected computer."[676]
SARATOGA[677]	Unknown	NSA/GCHQ joint program listed as "coming soon."[678]
SCARLETEMPEROR[679]	Attack	GCHQ program that provides "[t]argeted denial of service against targets' phones via call bombing."[680] Status listed as "[r]eady to fire."[681]
SCISSORS[682]	Processing	This NSA program "sort[s] data types for analysis in NUCLEON (voice), PINWALE (video), MAINWAY (call records), and MARINA (Internet records)."[683]
SCRAPHEAPCHALLENGE[684]	Attack	GCHQ program that provides "[p]erfect spoofing of emails from Blackberry targets."[685] Status listed as "[r]eady to fire, but see constraints."[686]
SCREAMINGEAGLE[687]	Processing	GCHQ "tool that processes kismet data into geolocation information."[688]
SEBACIUM[689]	Isolation	GCHQ's "ICTR developed system to identify P2P file sharing activity of intelligence value."[690] The status of this program is not listed.[691]

675. Gallagher & Greenwald, *supra* note 235.
676. *Id.*
677. *The NSA and GCHQ's QUANTUMTHEORY Hacking Tactics*, *supra* note 298.
678. *Id.*
679. *JTRIG Tools and Techniques*, *supra* note 131.
680. *Id.*
681. *Id.*
682. *NSA Slides Explain the PRISM Data-Collection Program*, *supra* note 273.
683. *Id.*
684. *JTRIG Tools and Techniques*, *supra* note 131.
685. *Id.*
686. *Id.*
687. *Id.*
688. *Id.*
689. *Id.*
690. *Id.*
691. *Id.*

SECONDDATE[692]	Attack	NSA program designed to “”influence real-time communications between client and server” and to “quietly redirect web-browsers” to NSA malware servers called FOXACID.”[693]
SEMESTER[694]	Isolation	NSA program described as “SIGINT targeting and reporting system[].”[695]
SERPENTSTONGUE[696]	Isolation	GCHQ program “for fax message broadcasting to multiple numbers.”[697] Status is listed as “[i]n redevelopment.”[698]
SFL[699]	Isolation	“The Sigint Forensics Laboratory was developed within NSA. It has been adapted by JTRIG as its email extraction and first-pass analysis of seized media solution.”[700]
SHADOWCAT[701]	Collection	GCHQ program that allows for “[e]nd to [e]nd encrypted access to a VPS over SSH using the TOR network.”[702]
SHAREDIVISION[703]	Unknown	Listed in NSA documents under “MHS has a growing FORNSAT mission.”[704]
SHARKFIN[705]	Collection	NSA program that is a “high-capacity/high-speed vacuum cleaner once called SHARKFIN and renamed RC-10, sweeps up all-source communications intelligence (COMINT) from a variety of communication methods and systems.”[706]

692. Gallagher & Greenwald, *supra* note 235.
693. *Id*.
694. Madsen, *supra* note 319.
695. *Id*.
696. *JTRIG Tools and Techniques*, *supra* note 131.
697. *Id*.
698. *Id*.
699. *Id*.
700. *Id*.
701. *Id*.
702. *Id*.
703. *Id*.
704. *Id*.
705. GREENWALD, supra note 1, at 97.
706. *Id*.

SHELLTRUMPET[707]	Processing	NSA program that, on December 31, 2012, "processed its One Trillionth metadata record."[708] SHELLTRUMPET "began as a near-real-time metadata analyzer . . . for a classic collection system."[709] "In its five year history, numerous other systems from across the Agency have come to use SHELLTRUMPET's processing capabilities for performance monitoring and other tasks, such as "direct email tip alerting."[710]
SHENANIGANS[711]	Collection	NSA program, used by the CIA, that "utilizes a pod on aircraft that vacuums up massive amounts of data from any wireless routers, computers, smart phones or other electronic devices that are within range."[712]
SILENTMOVIE[713]	Attack	GCHQ program that is used for the "[t]argeted denial of service against SSH services."[714] Status is listed as "[r]eady to fire."[715]
SILVERBLADE[716]	Collection	GCHQ program that provides "[r]eporting of extremist material on DAILYMOTION."[717] Status is listed as "[r]eady to fire."[718]

707. GREENWALD, supra note 1, at 100.

708. *Id.*

709. *Id.*

710. *Id.*

711. Glenn Greenwald, *The NSA's in the U.S. Assassination Program*, THE INTERCEPT (Feb. 10, 2014), https://theintercept.com/2014/02/10/the-nsas-secret-role/ (last visited Nov. 11, 2015) (on file with the Washington and Lee Law Review).

712. *Id.*

713. *JTRIG Tools and Techniques*, *supra* note 131.

714. *Id.*

715. *Id.*

716. *Id.*

717. *Id.*

718. *Id.*

SILVERFOX[719]	Isolation	GCHQ program that consists of a "[l]ist provided to industry of live extremist material files hosted on FFUs 720."[721] Status is listed as "[r]eady to fire."[722]
SILVERLORD[723]	Attack	GCHQ program that provides "[d]isruption of video-based websites hosting extremist content through concerted target discovery and content removal."[724]
SILVERSPECTER[725]	Isolation	GCHQ program that "[a]llows batch Nmap[726] scanning over TOR."[727] This program's status is listed as "[i]n development."[728]
SILVERZEPHYR[729]	Collection	NSA program that provides "customers with authorized, transit DNR collection. SSO is working with the partner to gain access to an additional 80Gbs of DNI data on their peering network, bundled in 10 Gbs increments."[730]

719. *Id.*

720. *See Files for Upload*, WIKIPEDIA, http://en.wikipedia.org/wiki/Wikipedia:Files_for_upload (last visited Nov. 24, 2015) (showing that FFU stands for "Files For Upload" and is a part of WikiProject Articles for creation, allowing "unregistered users to add new files to Wikipedia with the assistance of experienced Wikipedians") (on file with the Washington and Lee Law Review).

721. *JTRIG Tools and Techniques*, *supra* note 131.

722. *Id.*

723. *Id.*

724. *Id.*

725. *Id.*

726. *See Nmap Reference Guide*, NMAP.ORG, http://nmap.org/book/man.html#man-description (last visited Nov. 24, 2015) ("Nmap ('Network Mapper') is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts.") (on file with the Washington and Lee Law Review).

727. *JTRIG Tools and Techniques*, *supra* note 131.

728. *Id.*

729. GREENWALD, *supra* note 1, at 106.

730. *Id.*

SKYSCRAPER[731]	Isolation	GCHQ program that provides for the "[p]roduction and dissemination of multimedia via the web in the course of information operations."[732]
SKYWRITER[733]	Isolation	NSA "SIGINT targeting and reporting system."[734]
SLAMMER[735]	Processing	GCHQ program that "is a data index and repository that provides analysts with the ability to query data collected from the Internet from various JTRIG sources, such as EARTHLING, HACIENDA, web pages saved by analysis etc."[736]
SLIPSTREAM[737]	Attack	GCHQ program that provides the "[a]bility to inflate page views on websites."[738]
SMOKEYSINK[739]	Unknown	NSA/GCHQ joint program listed as "coming soon."[740]
SNICK[741]	Unknown	NSA program listed under "FORNSAT 1."[742]
SNOOPY[743]	Isolation	GCHQ "tool to extract mobile phone data from a copy of the phone's memory (usually supplied as an image file extracted through FTK)."[744]
SNORT[745]	Attack	According to Marc Ambinder, this is a NSA "[r]epository of computer network attack techniques/coding."[746]

731. *Id.*
732. *Id.*
733. *JTRIG Tools and Techniques*, *supra* note 131.
734. *Id.*
735. *Id.*
736. *Id.*
737. *Id.*
738. *Id.*
739. *The NSA and GCHQ's QUANTUMTHEORY Hacking Tactics*, *supra* note 298.
740. *Id.*
741. Greenwald, *supra* note 1.
742. *Id.*
743. *JTRIG Tools and Techniques*, *supra* note 131.
744. *Id.*
745. Ambinder, *supra* note 134; Somerville, *supra* note 134.
746. *Id.*

SODAWATER[747]	Collection	GCHQ program that is "[a] tool for regularly downloading gmail messages and forwarding them onto CERBERUS mailboxes."[748] Status listed as "[f]ully [o]perational."[749]
SOMALGET[750]	Collection	NSA program that "used access legally obtained in cooperation with the U.S. Drug Enforcement Administration to open a backdoor to the country's cellular telephone network, enabling it to covertly record and store the 'full-take audio' of every mobile call made to, from and within the Bahamas—and to replay those calls for up to a month."[751]
SOUNDER[752]	Unknown	NSA program listed under "FORNSAT 1."[753]
SOUTHWINDS[754]	Unknown	NSA program found in a slide that states: "Global coverage via SOUTHWINDS is planned in the next year."[755]
SPACEROCKET[756]	Attack	GCHQ "programme [sic] covering insertion of media into target networks. CRINKLE CUT is a tool developed by ICTR-CISA to enable JTRIG track images as part of SPACE ROCKET."[757]
SPICEISLAND[758]	Collection	GCHQ program that will be "JTRIG's new infrastructure. FOREST WARRIOR, FRUITBOWL, JAZZFUSION and other JTRIG systems will form part of the SPICEISLAND infrastructure."[759] Status listed as "DEV [development]."[760]

747. *JTRIG Tools and Techniques*, *supra* note 131.
748. *Id.*
749. *Id.*
750. Devereaux, Greenwald & Poitras, *supra* note 492.
751. *Id.*
752. GREENWALD, *supra* note 1.
753. *Id.*
754. *Id.* at 165.
755. *Id.*
756. *JTRIG Tools and Techniques*, *supra* note 131.
757. *Id.*
758. *Id.*
759. *Id.*
760. *Id.*

SPINNERET[761]	Collection	"[D]esigned to allow users to view the metadata record counts by organizational structure all the way down to the cover term."[762]
SPRINGBISHOP[763]	Isolation	GCHQ program that can "[f]ind private photographs of targets on Facebook."[764] The status of this program is not listed.[765]
SPRINGRAY[766]	Unknown	"A notification has been posted to SPRINGRAY and this collection is available to Second Parties via TICKETWINDOW."[767]
SQUEAKYDOLPHIN[768]	Collection	GCHQ tool that collects and analyzes data from social media networks.[769]
STEALTHMOOSE[770]	Attack	GCHQ "tool that will Disrupt target's Windows machine. Logs of how long and when the effect is active."[771]
STELLAR[772]	Unknown	NSA program that is listed under "FORNSAT 1."[773]
STORMBREW[774]	Collection	NSA program that "among others, filter[s] and gather[s] information at major telecommunications companies."[775]

761. GREENWALD, *supra* note 1, at 43; *BOUNDLESSINFORMANT—Frequently Asked Questions* (Sept. 6, 2012), https://www.eff.org/files/2014/04/09/20131122-dagbladet-boundless_informant_faq.pdf (last visited Nov. 4, 2015) (on file with the Washington and Lee Law Review).

762. *BOUNDLESSINFORMANT—Frequently Asked Questions*, *supra* note 761.

763. GREENWALD, *supra* note 1, at 43.

764. *JTRIG Tools and Techniques*, *supra* note 131.

765. *Id.*

766. *Id.*; GREENWALD, *supra* note 1, at 106.

767. *Id.*

768. Richard Esposito et al., *Snowden Docs Reveal British Spies Snooped on Youtube and Facebook*, NBC NEWS (Jan. 27, 2014), http://investigations.nbcnews.com/_news/2014/01/27/22469304-snowden-docs-reveal-british-spies-snooped-on-youtube-and-facebook (last visited Aug. 28, 2015) (on file with the Washington and Lee Law Review).

769. *Id.*

770. *JTRIG Tools and Techniques*, *supra* note 131.

771. *Id.*

772. GREENWALD, *supra* note 1.

773. *Id.*

774. Gorman & Valentino-Devries, *supra* note 199; GREENWALD, *supra* note 1, at 103.

775. Gorman & Valentino-Devries, *supra* note 199; GREENWALD, *supra* note 1, at 103.

SUNBLOCK[776]	Attack	GCHQ program that provides the "[a]bility to deny functionality to send/receive email or view material online."[777]
SURREY[778]	Database	Marc Ambinder describes this as the "[m]ain NSA requirements database, where targets and selectors are 'validated' by NSA managers."[779]
SYLVESTER[780]	Collection	GCHQ program that is a "[f]ramework for automated interaction/alias management on social networks."[781]
SWAMPDONKEY[782]	Attack	A GCHQ "tool that will silently locate all predefined types of file and encrypt them on a targets [sic] machine."[783]
TANGLEFOOT[784]	Processing	GCHQ "bulk search tool which queries a set of online resources. This allows analysts to quickly check the online presence of a target."[785]
TANNER[786]	Isolation	GCHQ "technical program allowing operators to log on to a JTRIG website to grab IP addresses of Internet Café's [sic]."[787] Status listed as "[r]eplaced by HAVOK."[788]
TARMAC[789]	Unknown	NSA program listed in slides under "Why TARMAC? . . . MHS has a growing FORNSAT mission . . . SHAREDIVISION mission . . . SigDev ('Difficult Signals collection')."[790]

776. *JTRIG Tools and Techniques*, *supra* note 131.
777. *Id.*
778. Ambinder, *supra* note 134.
779. *Id.*; Somerville, *supra* note 134.
780. *JTRIG Tools and Techniques*, *supra* note 131.
781. *Id.*
782. *Id.*
783. *Id.*
784. *Id.*
785. *Id.*
786. *Id.*
787. *Id.*
788. *Id.*
789. GREENWALD, *supra* note 1, at 43.
790. *Id.*

TECHNOVIKING[791]	Collection	GCHQ "sub-system of JAZZFUSION."[792] Listed as "design."[793]
TEMPORA[794]	Collection	GCHQ program that "aims to eventually allow the agency (and its partner) to survey over 90 percent of the cables that route through the United Kingdom, pulling data from 400 at once."[795] This data can also source from the US and is allegedly shared with the NSA.[796]
THIEVINGMAGPIE[797]	Isolation	NSA program "using on-board GSM/GPRS services to track targets."[798]
TICKETWINDOW[799]	Unknown	Found on NSA slide: "collection is available to Second Parties via TICKETWINDOW."[800]
TOPHAT[801]	Isolation	GCHQ program that is "[a] version of the MUSTANG and DANCING BEAR techniques that allows us [GCHQ] to pull back Cell Tower and WiFi locations targeted against particular areas."[802] Status is listed as "in development."[803]
TORNADOALLEY[804]	Attack	GCHQ "delivery method (Excel Spreadsheet) that can silently extract and run an executable on a target's machine."[805]

791. *JTRIG Tools and Techniques*, *supra* note 131.

792. *Id.*

793. *Id.*

794. *The NSA in Germany: Snowden's Documents Available for Download*, *supra* note 122.

795. *Id.*; Philip Bump, *The UK Tempora Program Captures Vast Amounts of Data—and Shares with the NSA,* WIRE (June 21, 2013), http://www.thewire.com/national/2013/06/uk-tempora-program/66490/ (last visited Nov. 24, 2015) (on file with the Washington and Lee Law Review).

796. Bump, *supra* note 795.

797. GREENWALD, *supra* note 1, at 106.

798. *Id.*

799. *Id.*

800. *Id.*

801. *JTRIG Tools and Techniques*, *supra* note 131.

802. *Id.*

803. *Id.*

804. *Id.*

805. *Id.*

TOYGRIPPE[806]	Database	NSA program that is described on a slide as a "[f]ull take metadata repository."[807]
TRACERFIRE[808]	Attack	GCHQ program that is "[a]n Office Document that grabs the target's Machine info, files, logs, etc and posts it back to GCHQ."[809] Status listed as "[i]n [d]evelopment."[810]
TRAFFICTHIEF[811]	Processing	NSA program that Marc Ambinder describes as a "[r]aw SIGINT viewer for data analysis."[812]
TRAILBLAZER[813]	Collection	A failed NSA collection program, described as an "abandoned . . . $1.2-billion flop."[814]
TREASUREMAP[815]	Processing	NSA program that provides "a near real-time, interactive map of the global Internet" and is a "massive Internet mapping, analysis and exploration engine."[816]
TROJANCLASSICXXI[817]	Collection/ Processing	"[C]ollection, procession, analysis and reporting system."[818]

806. *Bad Guys Are Everywhere,* SPIEGEL ONLINE INT'L (Sept. 14, 2014), http://www.spiegel.de/media/media-34757.pdf.

807. *Id.*

808. *JTRIG Tools and Techniques*, *supra* note 131.

809. *Id.*

810. *Id.*

811. Ambinder, *supra* note 134; Somerville, *supra* note 134.

812. Ambinder, *supra* note 134.

813. Jane Mayer, *The Secret Sharer*, THE NEW YORKER (May 23, 2011), http://www.newyorker.com/magazine/2011/05/23/the-secret-sharer (last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

814. *Id.*

815. James Risen & Laura Poitras, *NSA Report Outlined Goals for More Power*, N. Y. TIMES (Nov. 22, 2013), http://www.nytimes.com/2013/11/23/us/politics/nsa-report-outlined-goals-for-more-power.html?_r=0 (last visited Oct. 2, 2015) (on file with the Washington and Lee Law Review).

816. *Id.*

817. *The NSA in Germany: Snowden's Documents Available for Download*, *supra* note 122.

818. *European Security Center to Begin Operations*, AM. C.L. UNION, https://www.aclu.org/files/natsec/nsa/20140722/European%20Security%20Center%20to%20Begin%20Operations.pdf.

TROPICPUMA[819]	Processing	A program with "fax processing capabilities" that provided "unique and valuable intelligence to ESOC and BND."[820]
TURBULENCE[821]	Collection	NSA program that "includes nine core programs, with intriguing names such as Turmoil, Tutelage and Traffic Thief. Among their goals: mapping social networks based on intercepted communications, embedding technology on networks to collect data, and searching for patterns across hundreds of NSA databases."[822]
TURMOIL[823]	Processing	DNI processing system, which has evolved "from GRANDMASTER to WEALTHYCLUSTER and, in the future, TURMOIL"[824]
TWILIGHTARROW[825]	Processing	GCHQ program that is a "[r]emote GSM secure covert internet proxy using VPN services."[826] Status listed as "operational."[827]
UNDERPASS[828]	Attack	GCHQ program that allows users to "[c]hange outcome[s] of online polls (previously known as NUBILO)."[829]

819. *The NSA in Germany: Snowden's Documents Available for Download*, *supra* note 122.

820. *Id.*

821. Siobhan Gorman, *Costly NSA Initiative Has a Shaky Takeoff*, BALT. SUN (Feb. 11, 2007), http://articles.baltimoresun.com/2007-02-11/news/0702110034_1_turbulence-cyberspace-nsa/2 (last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

822. *Id.*

823. Somerville, *supra* note 134, at 44.

824. *German, NSA SIGINTers Share DNI Processing Knowledge*, SPIEGEL ONLINE INT'L, http://www.spiegel.de/media/media-34087.pdf.

825. *JTRIG Tools and Techniques*, *supra* note 131.

826. *Id.*

827. *Id.*

828. *Id.*

829. *Id.*

UPSTREAM[830]	Collection	NSA program that provides "Collection of communications on fiber cables and infrastructure as data flows past."[831] This includes STROMBREW, FAIRVIEW, BLARNEY, and OAKSTAR.[832] The identities of the four U.S. telecom providers that cooperate with the NSA are tightly guarded.[833] Reportedly, some 11,000 pieces of information come from Blarney every year. It is one of the "top sources" for the President's daily brief, a top-secret document briefing the president every morning on security matters.[834]
VAGRANT[835]	Unknown	Bruce Schneier describes this as a "[c]ollection of [c]omputer screens."[836]
VIEWER[837]	Isolation	GCHQ "programme that (hopefully) provides advance tip off of the kidnappers IP address for HMG personnel." Status listed as "operational, but awaiting field trial."[838]
VIKINGPILLAGE[839]	Collection	GCHQ "[d]istributed network for the automatic collection of encrypted/compressed data from remotely hosted JTRIG projects."[840] Status listed as "[o]perational."[841]

830. GREENWALD, *supra* note 1, at 108.
831. *Id.*
832. Ball, *supra* note 54.
833. *Id.*
834. Poitras, Rosenbach & Stark, *supra* note 656.
835. Schneier, *supra* note 195.
836. *Id.*
837. *JTRIG Tools and Techniques*, *supra* note 131.
838. *Id.*
839. *Id.*
840. *Id.*
841. *Id.*

VIPERSTONGUE[842]	Attack	GCHQ "tool that will silently Denial of Service calls on a Satellite Phone or a GSM Phone."[843]
WARPATH[844]	Attack	GCHQ tool that provides for the "[m]ass delivery of SMS messages to support an Information Operations campaign."[845]
WATCHTOWER[846]	Collection	GCHQ's "GCNET->CERBERUS Export Gateway Interface System."[847] Listed as "operational."[848]
WAXTITAN[849]	Collection	Listed in "United Kingdom—Collection Information" with Validator ID of "610102256."[850]
WEALTHYCLUSTER[851]	Processing	DNI processing system, which has evolved "from GRANDMASTER to WEALTHYCLUSTER and, in the future, TURMOIL."[852]
WEBCANDID[853]	Unknown	NSA codename found "on LinkedIn profiles."[854]
WILDCOUGAR[855]	Collection	Listed in "United Kingdom—Collection Information" with Validator ID of "611001840."[856]

842. *Id.*

843. *Id.*

844. *Id.*

845. *Id.*

846. *Id.*

847. *Id.*

848. *Id.*

849. *United Kingdom—Collection Information*, *supra* note 174.

850. *Id.*

851. Gorman, *supra* note 821.

852. *The NSA in Germany: Snowden's Documents Available for Download*, *supra* note 122.

853. Bruce Schneier, *More NSA Code Names,* SCHNEIER ON SECURITY (July 11, 2013), https://www.schneier.com/blog/archives/2013/07/more_nsa_codena.html (last visited Aug. 28, 2015) (on file with the Washington and Lee Law Review).

854. *Id.*

855. *United Kingdom—Collection Information*, *supra* note 174.

856. *Id.*

WINDSTOP[857]	Collection	NSA program described as the "name for at least four collection systems that depend on trusted '2nd Party' partners from Britain, Canada, Australia or New Zealand. One WINDSTOP project, with the cover name MUSCULAR, is used to break into the internal 'cloud' networks of Google and Yahoo which goes by the alphanumeric designator DS-200B."[858]
WIRESHARK[859]	Attack	According to Marc Ambinder, this is a NSA "[r]epository of malicious network signatures."[860]
WORDGOPHER [861]	Collection	NSA program listed as "bringing our enterprise one step closer to 'collecting it all.'"[862] Listed in the following sentence on a NSA slide: "In the future, MSOC hopes to expand the number of WORDGOPHER platforms to enable demodulation of thousands of additional low-rate carriers."[863]
WRANGLER[864]	Database	NSA program that is described by Marc Ambinder as an "[e]lectronic intelligence intercept raw database."[865]
WURLITZER[866]	Attack	GCHQ program used to "[d]istribute a file to multiple file hosting websites."[867]

857. *WINDSTOP System Highlights*, AM. C.L. UNION, https://www.aclu.org/files/assets/2013.10.30%20NSA%20Special%20Operations%20Weekly%20Excerpt.pdf; *One Month, Hundreds of Millions of Records Collected*, *supra* note 547.

858. *One Month, Hundreds of Millions of Records Collected*, *supra* note 547.

859. Ambinder, *supra* note 134; Somerville, *supra* note 134.

860. Ambinder, *supra* note 134.

861. *Id.*; *One Month, Hundreds of Millions of Records Collected*, *supra* note 547; GREENWALD, *supra* note 1, at 98.

862. *Id.*

863. *Id.*

864. Ambinder, *supra* note 134.

865. *Id.*; Somerville, *supra* note 134.

866. *JTRIG Tools and Techniques*, *supra* note 131.

867. *Id.*

XKEYSCORE[868]	Collection	NSA program that, according to Marc Ambinder, is a "[c]ollection tool for international metadata."[869] "XKEYSCORE is a computer-network exploitation system that combines high-speed filtering with SIGDEV."[870] "[F]ocused on understanding, creating, and implementing discovery capabilities."[871] "Through the provision of XKEYSCORE, NSA will enable Germany to provide unique contribution in the form of collection, data summaries, and/or finished intelligence to the high-priority NSA CT mission."[872] "XKEYSCORE software from DIRNSA to further enable the BfV to achieve its mission goal of countering terrorist activities in Germany."[873] This program has also been used by the GCHQ to "access . . . private emails hosted by the SIM card and mobile companies' servers, as well as those of major tech corporations, including Yahoo and Google."[874]
YACHTSHOP[875]	Collection	NSA collection tool for "worldwide Internet metadata."[876]

868. GREENWALD, *supra* note 1, at 165.

869. Ambinder, *supra* note 134.

870. *The NSA in Germany: Snowden's Documents Available for Download*, *supra* note 122.

871. *Id.*

872. *Id.*

873. *Id.*

874. Jeremy Scahill & Josh Begley, *The Great SIM Heist*, THE INTERCEPT (Feb. 19, 2015), https://theintercept.com/2015/02/19/great-sim-heist/ (last visited Aug. 28, 2015) (on file with the Washington and Lee Law Review).

875. Emily Heil, *What's the Deal with NSA's Operation Names?*, WASH. POST (Oct. 22, 2013), http://www.washingtonpost.com/blogs/in-the-loop/wp/2013/10/22/whats-the-deal-with-nsas-operation-names/ (last visited Sept. 20, 2015) (on file with the Washington and Lee Law Review).

876. *Id.*