palgrave pivot

TECHNOLOGY OF OPPRESSION

Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance

Elliot D. Cohen

Technology of Oppression

DOI: 10.1057/9781137408211.0001

Other Palgrave Pivot titles

Ilan Alon (editor): **Social Franchising**

Richard Michael O'Meara: **Governing Military Technologies in the 21st Century: Ethics and Operations**

Thomas Birtchnell and William Hoyle: **3D Printing for Development in the Global South: The 3D4D Challenge**

David Fitzgerald and David Ryan: **Obama, US Foreign Policy and the Dilemmas of Intervention**

Lars Elleström: **Media Transformation: The Transfer of Media Characteristics Among Media**

Claudio Povolo: **The Novelist and the Archivist: Fiction and History in Alessandro Manzoni's The Betrothed**

Gerbrand Tholen: **The Changing Nature of the Graduate Labour Market: Media, Policy and Political Discourses in the UK**

Aaron Stoller: **Knowing and Learning as Creative Action: A Reexamination of the Epistemological Foundations of Education**

Carl Packman: **Payday Lending: Global Growth of the High-Cost Credit Market**

Lisa Lau and Om Prakash Dwivedi: **Re-Orientalism and Indian Writing in English**

Chapman Rackaway: **Communicating Politics Online**

G. Douglas Atkins: **T.S. Eliot's Christmas Poems: An Essay in Writing-as-Reading and Other "Impossible Unions"**

Marsha Berry and Mark Schleser: **Mobile Media Making in an Age of Smartphones**

Isabel Harbaugh: **Smallholders and the Non-Farm Transition in Latin America**

Daniel A. Wagner (editor): **Learning and Education in Developing Countries: Research and Policy for the Post-2015 UN Development Goals**

Murat Ustaoğlu and Ahmet İncekara: **Islamic Finance Alternatives for Emerging Economies: Empirical Evidence from Turkey**

Laurent Bibard: **Sexuality and Globalization: An Introduction to a Phenomenology of Sexualities**

Thorsten Botz-Bornstein and Noreen Abdullah-Khan: **The Veil in Kuwait: Gender, Fashion, Identity**

Vasilis Kostakis and Michel Bauwens: **Network Society and Future Scenarios for a Collaborative Economy**

Tom Watson (editor): **Eastern European Perspectives on the Development of Public Relations: Other Voices**

Erik Paul: **Australia as US Client State: The Geopolitics of De-Democratization and Insecurity**

Floyd Weatherspoon: **African-American Males and the U.S. Justice System of Marginalization: A National Tragedy**

Mark Axelrod: **No Symbols Where None Intended: Literary Essays from Laclos to Beckett**

DOI: 10.1057/9781137408211.0001

palgrave pivot

Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance

Elliot D. Cohen

palgrave
macmillan

DOI: 10.1057/9781137408211.0001

TECHNOLOGY OF OPPRESSION

Softcover reprint of the hardcover 1st edition 2014 978-1-137-42621-5

First published in 2014 by
PALGRAVE MACMILLAN®
in the United States—a division of St. Martin's Press LLC,
175 Fifth Avenue, New York, NY 10010.

Where this book is distributed in the UK, Europe and the rest of the world, this is by Palgrave Macmillan, a division of Macmillan Publishers Limited, registered in England, company number 785998, of Houndmills, Basingstoke, Hampshire RG21 6XS.

Palgrave Macmillan is the global academic imprint of the above companies and has companies and representatives throughout the world.

Palgrave® and Macmillan® are registered trademarks in the United States, the United Kingdom, Europe and other countries.

ISBN: 978–1–137–40821–1 PDF
ISBN: 978-1-349-49075-2

Library of Congress Cataloging-in-Publication Data is available from the Library of Congress.

A catalogue record of the book is available from the British Library.

First edition: 2014

www.palgrave.com/pivot

DOI: 10.1057/9781137408211

Contents

DOI: 10.1057/9781137408211.0001

Preface

The technological turning point has arrived. We now are at a crossroads where we can, potentially, transform human existence into an automated set of commands that monitor and control thought and action for the sake of national security. Or, we can resist the technological thrust or "imperative" toward this dehumanizing end. This latter option is a monumental challenge; for it requires the resolve and cooperation of people throughout the world to press for substantive changes in law, social consciousness, and technology itself.

This book is largely about the logistics of making these changes. It is intended for a diverse population of readers—including the movers and shakers who can help get the job done. It is intended for those who occupy positions of authority in government and the justice system; for those in the industrial sector, who have the means to make available the "meta-technologies" to curb the overreach of primary surveillance technologies; for those in the media who care passionately about their constitutional charge to keep the people informed about the necessity of such changes; and, finally, for the people, themselves, who are subject to government monitoring and control.

For two decades, I have studied information capture and analysis technologies, including their propensity for generating false positives. I have also invented and held U.S. patents in content filtering for electronic message systems.[1] Thus, my interest in mass surveillance technologies is not a passing interest. In 2010, I published the Palgrave Macmillan book titled, *Mass Surveillance and State*

DOI: 10.1057/9781137408211.0002

Control: The Total Information Awareness Project, in which I described a significant amount of what Edward Snowden later confirmed through his leaked documents, although in less detail. This book is a follow-up and update to the previous book in light of these new revelations. The previous book aimed largely at exposing the nature and magnitude of the "Total Information Awareness Project" for purposes of issuing a sobering warning about the steady advance toward a "culture of control." In contrast, the present book tackles, in greater detail, the practical question of how to make constructive changes in order to safeguard the basic values that make human life human.

I wrote this book because I felt the urgency. Now is the time for revamping the manner in which government—that of the United States and its allies—conducts foreign intelligence investigations. This is by sweeping up masses of personal and private electronic information in global proportions, virtually all of which is irrelevant for foreign intelligence gathering purposes. Exposing the true terrorist plot does not require such mass violation of rights. In the aftermath of the Snowden leaks, more people are, at last, asking questions about this program. While the world community is expressing serious concern, it is the best time to get down to particulars about what changes are needed. I hope the specific recommendations for change advanced in this book are useful toward this end.

Note

1 For example, US 5796948, as discussed in the Introduction to this book.

DOI: 10.1057/9781137408211.0002

palgrave pivot

www.palgrave.com/pivot

Introduction: Why Privacy Matters

Abstract: *The Introduction to this book carefully defines the moral and legal significance of privacy, freedom, and dignity. It then discusses the mounting threat posed to these core human values by the technological expansion of mass, warrantless surveillance technologies. Accordingly, it sets the stage for an examination of this technological expansion.*

Cohen, Elliot D. *Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.* New York: Palgrave Macmillan, 2014.
DOI: 10.1057/9781137408211.0003.

The rate of development of new tracking and surveillance technologies is progressing at an incredible rate. This progression is moving toward increasingly intrusive devices for gathering information. As this progression continues, unopposed by means to curtail the invasiveness of these technologies, the prospects for the survival of human freedom and dignity in the not-so-distant future are bleak. This is true because these humanizing values are possible only if there remains intact a zone of privacy, which is offline and surveillance-free. Without such a private zone, the most personal decisions become fodder for politico-media-industrial manipulation and control. As more intrusive means of technology advance, and as human beings, with each successive generation, become increasingly accustomed to conducting their personal lives online, this sphere of privacy continues to be eroded. The inevitable result of this forward thrust toward the demise of privacy is the demise of human freedom and dignity, which are dependent on its survival.

Privacy, freedom, and dignity

"Privacy," as understood in the informational context, refers to the state of not having one's personal information shared with others without one's informed consent. Personal information includes the most intimate facts about oneself. It includes information about one's (physical and mental) health, bank records, social security number, and credit history. It includes facts about oneself such as one's age, weight, and one's mental and physical abilities. It also includes personal beliefs, desires, attitudes, and preferences such as one's social and political views, religious convictions (or the lack thereof), sexual orientation, sexual preferences or fantasies; and it includes one's indiscretions, secret rendezvous, lies, legal infractions, and many and sundry other personal things.

There can also be, and often is, a significant difference between one's public persona and one's private self. What one chooses to disclose in public may not truly capture who one truly is. For example, in public, one may be outgoing while privately one may be shy and reserved. Some of us may publicly project an image of caring greatly for others, while, in private, be rather self-centered. Regardless of the moral quality of one's inner, private self, people generally have a right not to share personal information about themselves with others. This right to privacy is both a moral and legal right.

DOI: 10.1057/9781137408211.0003

To say that one has a moral right to privacy means that one has a morally justified claim or interest that others not gain access to one's personal information without one's informed consent; and this right can be said to be violated or abridged when others manage to gain such access. Further, the moral right to privacy derives from a more general right of self-determination, that is, the liberty or freedom to choose for oneself in matters concerning what is one's own, such as one's personal possessions or property, or one's own life—provided, of course, one is a competent adult. Thus, one has such a right to dispose of personal information in any way one sees fit inasmuch as such information is one's own.

This general moral right of self-determination also has legal standing pursuant to the US Constitution. It is enshrined in the Fourteenth Amendment, which holds that no state shall "deprive any person of life, liberty, or property, without due process of law," and the same language is repeated in the Fifth Amendment. The First Amendment holds that "Congress shall make no law…abridging the freedom of speech, or of the press…" But, clearly, without a sphere of privacy in which to speak freely without the government listening, or of the press to gather news without the government eavesdropping on its sources, there can be no protected legal right to free speech, or a free press. Again, the Fourth Amendment recognizes "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures…" Here is where the Constitution makes clear that the government will, in no case, violate one's personal space without a warrant based on probable cause. In *Olmstead v. U.S.* (1928), Justice Brandeis famously expressed,

> The makers of our Constitution understood the need to secure conditions favorable to the pursuit of happiness, and the protections guaranteed by this are much broader in scope, and include the right to life and an inviolate personality—the right to be left alone—the most comprehensive of rights and the right most valued by civilized men. The principle underlying the Fourth and Fifth Amendments is protection against invasions of the sanctities of a man's home and privacies of life. This is a recognition of the significance of man's spiritual nature, his feelings, and his intellect.[1]

The "privacies of life" are, in Justice Brandeis' words, at the core of "man's spiritual nature, his feelings, and his intellect." Foreclose this area of protected freedom or autonomy to be oneself in the privacy of one's

DOI: 10.1057/9781137408211.0003

home, or to dispose of one's personal information as one sees fit, and one's very personhood and individuality—one's unique spiritual nature, feelings, and intellect—is chilled off. The quality of human dignity lies in the respect owed to persons by virtue of their ability to navigate their own ship of life. Dismantle this private sphere of freedom by refusing to leave people alone and an essential condition of their dignity—the ability to freely think and act—is also imperiled.

The threat posed by mass, warrantless surveillance technologies

Presently, such a threat to human freedom and dignity lies in the technological erosion of human privacy through the ever-evolving development and deployment of a global, government system of mass, warrantless surveillance. Taken to its logical conclusion, this is a systematic means of spying on, and ultimately manipulating and controlling, virtually every aspect of everybody's private life—a thoroughgoing, global dissolution of personal space, which is supposed to be legally protected. In such a governmental state of "total (or virtually total) information awareness," the potential for government control and manipulation of the people's deepest and most personal beliefs, feelings, and values can transform into an Orwellian reality—and nightmare. As will be discussed in Chapter 6, the technology that has the potential to remove such scenarios from the realm of science fiction to that of true science is currently being developed.

This is not to deny the legitimate government interest in "national security"; however, the exceptional disruption of privacy for legitimate state reasons cannot and should not be mistaken for a usual and customary rule of mass invasion of people's private lives without their informed consent. Benjamin Franklin wisely and succinctly expressed the point: "Those who surrender freedom for security will not have, nor do they deserve, either one." In relinquishing our privacy to government, we also lose the freedom to control, and act on, our personal information, which is what defines us individually, and collectively, as free agents and a free nation. In a world devoid of freedom to control who we are, proclaiming that we are "secure" is an empty platitude.

The power of technology to change who we are should not be underestimated. Few would deny the transformative influences of digital

DOI: 10.1057/9781137408211.0003

technologies on society. Through social media, such as Facebook and Twitter, many of us, especially those of the younger generations, regularly share even the most intimate details of their lives with masses of strangers. To the generation prior to the advent of the internet, a world in which one could speak to millions about a sexual relationship gone awry would have been (virtually) unthinkable. As new forms of digital technologies emerge, such as ones that blur the distinction between the real and virtual worlds; or wherein thoughts themselves, instead of text, can be tweeted; or wherein the "people inside the television set" can really see what you are doing in your living room, we can predictably expect the next generation, now in diapers, to buy into it. Through such successive stages of the technological decline of privacy, the distinction between the private and the public will itself evaporate. In this fishbowl existence, where government knows all (or virtually all), the next obvious step will be to apply this knowledge through more and more technologically sophisticated means of controlling our thoughts and our behavior (for example, downloading executable files into our brains).

How we got here and what to do about it

What drives this forward thrust toward increasing technological change is multifaceted. First, mass surveillance technologies have meant lucrative defense contracts for technology companies, which typically enjoy a revolving door with the US government. Second, the desire for immediate gratification (so-called short-term hedonism) leads us to overlook long-term losses for short-term gratification. Thus, we are more willing to tolerate being monitored as long as it does not affect the quality of our online experience. Third, we tend to downplay the dangers of new technology and play up their positive features. Thus, it is commonly believed that surveillance technologies can protect us by helping to foil terrorist plots, while, at the same time, we tend to play down the dangers of unleashing such technologies without proper privacy protections. Fourth, the so-called "Technological Imperative" speaks to us, "If we can build a new technology, we should build it." This appetite for technological innovation has led us to build weapons of mass destruction, such as biological warfare, even though, rationally, they portend greater evil than good. Indeed, life-altering, even planet-altering technologies have been produced and brought to market in advance of serious reflection

DOI: 10.1057/9781137408211.0003

on the ethical and legal questions they raise. From genetic engineering and nanotechnology to technologies of mass communication, we have moved toward global change on the assumption that the prudential questions about their costs and benefits will somehow be satisfactorily resolved after the fact.

Accordingly, this book attempts to systematically examine and provide rational responses to the ethical and legal quandaries that surround development and deployment of mass, warrantless, and global surveillance technologies. While the treatment here addresses the problem it presents for the American people, it also looks at it from a global perspective; that is, it considers what changes in the present system of surveillance policies and practice the world community would want, and even demand. In this age of Post-Snowden disclosure, much more is publicly available about the National Security Agency's (NSA) mass surveillance program; but this information has been "leaked" in the form of government documents, which have not themselves been systematically examined and connected in order to expose the functional relationships between various parts of a massive, integrated network of technologies. This book provides this systematization and draws out its legal and moral implications.

The President's challenge

In his January 17, 2014 speech on the NSA surveillance program, President Barack Obama indicated his intention to make changes in the program and admitted that there were problems with the system. While he claimed that "some of the worst excesses" that emerged after 9–11 were curbed by the time he took office, he admitted that, "a variety of factors have continued to complicate America's efforts to both defend our nation and uphold our civil liberties." He confirmed that "many routine communications around the world are within our reach"; that, "the government collection and storage of such bulk data also creates a potential for abuse"; that, "the power of new technologies means that there are fewer and fewer technical constraints on what we can do"; and that, "in the absence of institutional requirements for regular debate and oversight that is public as well as private or classified, the danger of government overreach becomes more acute."[2]

DOI: 10.1057/9781137408211.0003

The President has identified crucial issues that can raise substantial challenges to preserving privacy, freedom, and dignity. These problems are succinctly: collection of more data than what is necessary; the potential for abuse; lack of privacy constraints on the technology itself; lack of transparency of surveillance policies and practices. This book takes seriously President Obama's concerns and attempts to address them. In addition, it addresses other related issues including the problem of "backdoor" programs that operate without adequate judicial oversight; exaggeration of the efficiency of various legs of the surveillance network; needless reliance on mass surveillance technologies instead of conventional investigative methods; extending the reach of the program beyond the thwarting of terrorism attacks to "foreign affairs"; interception of privileged communication such as between attorneys and their foreign clients; the dangers of new technologies looming on the horizon.

Some of these problems call for legal changes; some, configuring the technology to better conform to existing law; others, the addition of meta-technologies (technologies to constrain the primary technologies); others, pre-emptive measures to head off the impending dangers of new technologies; and still others, the institution of new policies that promote greater government transparency.

Using content filters to protect privacy

Meta-technologies, which constrain and protect abuses of primary technologies, have been conspicuously lacking in the massive surveillance network that has emerged over several decades. At least documentation has yet to emerge to verify the use of such technologies to protect privacy. Yet, as explained in Chapter 2, such an automatic way to protect privacy is technologically feasible. This book, therefore, emphasizes the use of surveillance meta-technologies and the construction of regulative rules that mandate such use. In particular, it discusses how *content filtering* technologies can be used to guard against needless, unlawful, and unethical acquisition of data by government.

This author has long advocated the use of content filters to preserve privacy, although, historically, there has been a tendency to avoid such use. In 1996, I received one of the first US software patents on a network content filter entitled, *Offensive Message Interceptor for Computers*.[3] According to the background of the invention,

DOI: 10.1057/9781137408211.0003

> Private companies, state agencies, and schools providing electronic communication or mail services usually make clear in their user contracts that use of profane or offensive language is prohibited. However, enforcement of such "netiquette" is through human inspection of senders' messages upon complaint by a recipient of the offensive message. As a result, enforcement of these contracts is inconsistent and requires interference with senders' privacy inasmuch as senders have their private thoughts read by other persons.[4]

The invention, thus, provides an automated method to screen for messages with objectionable content using matching criteria, returning objectionable messages to senders so that the privacy of the sender is protected. Here is a method to protect the privacy of people's electronic communications against intrusion by government through the use of content filtering. Unfortunately, both government and private networks have generally utilized programs that do not consider the privacy of end users. The mass surveillance network operated by the NSA is no exception. Accordingly, it is a goal of this book to advocate for the use of such meta-technologies to aid in the protection of privacy of millions of people whose electronic communications are currently being vacuumed up by a colossal surveillance system.

As such, this book not only isolates the dangers of the current and future state of surveillance technologies; it also attempts to provide realistic solutions to it.

The import of the title

The title of this book, *Technology of Oppression*, is intended to strike a dissonant chord about the potential and actual dangers of the rising tide of surveillance technologies. At the same time, the positive note that should serve as an undercurrent is that there is now, more than ever before, public awareness that mass surveillance is really happening and has serious problems. The United States, no less than its citizens, and the people of the world connected to the internet have the opportunity to make authentic and honest change. Indeed, it is important for all civilized nations to have means of protecting themselves from foreign invasions. But it also needs to protect itself from the inside. Assuring safety from attack by terrorists is only one part of the equation for prosperity of the state, nation, and world order. The other part of the equation is the promotion and protection of the freedom to enjoy that

DOI: 10.1057/9781137408211.0003

safety. Accordingly, this book confronts the practical (and monumental) task of making concrete recommendations to ensure present and future sustenance of privacy, freedom, and dignity amid a vociferous technological expansion, which has the potential to undermine these essential human values.

Notes

1 Olmstead v. United States – 277 U.S. 438 (1928) (Brandeis, J., Dissenting).
2 Barrack Obama, "Speech on NSA reforms," *Washington Post*, January 17, 2014. Retrieved on June 18, 2014 from http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3–9556-4a4bf7bcbd84_story.html.
3 Elliot D. Cohen, Offensive message interceptor for computers, US 5796948 A, August 18, 1998. Retrieved on June 18, 2014 from http://www.google.com/patents/US5796948.
4 Ibid.

DOI: 10.1057/9781137408211.0003

1

A History of the Mass Warrantless Surveillance Network

Abstract: *This chapter discusses the historical progress of mass, warrantless surveillance technologies beginning in the late 1960s through the years of the George W. Bush and the Barack Obama administrations to date, in light of the recent Snowden disclosures. It describes the development of a single, integrated Mass Warrantless Surveillance Network (MWSN).*

Cohen, Elliot D. *Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.* New York: Palgrave Macmillan, 2014.
DOI: 10.1057/9781137408211.0004.

DOI: 10.1057/9781137408211.0004

The United States' mass warrantless surveillance network (MWSN) is a constantly evolving global set of integrated technologies. Over time, its code names and technologies have changed; it has grown new tentacles to suck up different types and greater amounts of information; and it has relocated its equipment to different corners of the earth; but, because it is possible to trace its growth and development through all these successive changes, it makes sense to think of this technological development as one massive, self-same system. The evolutionary history of this unified surveillance system has proven to be one of incremental encroachment on privacy with the development of increasingly more effective ways of spying on the electronic communications of the masses.

ECHELON

The origins of the MWSN can be traced to a transnational network code named ECHELON, which was deployed in the late 1960s, with the emergence of satellite technologies. ECHELON was a joint undertaking of the US and the UK, along with the Commonwealth nations of Canada, Australia, and New Zealand (dubbed "the Five Eyes"), which aimed largely at intercepting satellite communications by operating listening stations throughout the world; and filtering the captured signals through a dictionary of predefined search terms. As with later versions of the MWSN, the official purpose for ECHELON was that of national security, in this case, to gather signal intelligence that could be used to ward off the threat posed by the Soviet Union during the Cold War years. This system was operated by the National Security Agency (NSA) and its British counterpart, the Government Communications Headquarters (GCHQ). According to an August 1988 report in the *New Statesman*, it comprised "a network of monitoring stations in Britain and elsewhere," which was "able to tap all international and some domestic communications circuits, and sift out messages which sound interesting." Further, it states that, "Computers automatically analyse every telex message or data signal, and can also identify calls to, say, a target telephone number in London, no matter from which country they originate."[1]

The report chronicled how Margaret Newsham, a Lockheed software designer who worked at the listening post at Menwith Hill in North Yorkshire, England, could listen through earphones to telephone calls,

DOI: 10.1057/9781137408211.0004

including those of politicians, being monitored at the base. The report also alleges that investigations have produced documents revealing that the "targeting of US political figures would not occur by accident, but was designed into the system from the start".

ECHELON appears to have been just part of a broader set of spying technologies that were then operative. In addition to ECHELON, other clandestine projects connected to Menwith Hill include SILKWORTH, MOONPENNY, SIRE, RUNWAY, STEEPLEBUSH, and BIG BIRD. SILKWORTH was allegedly the code name for long-range radio monitoring; MOONPENNY, another system for monitoring satellite communications; RUNWAY, a control network for a spy satellite called VORTEX, orbiting the then Soviet Union; STEEPLEBUSH, a control center connected with overhead listening satellites; BIG BIRD, a low-orbiting, photographic reconnaissance-carrying listening equipment.

The satellite-based technologies of ECHELON and its sister systems were, however, soon to become outdated. Beginning in the late 1970s, fiber optic cables began to replace copper wiring in telephone networks because they were more cost effective and could carry more data and much faster (at the speed of light). Since fiber optic cables transmit digital signals (light signals switching on and off to send bits of information), analog telephones (ones that work by sending electrical signals) had to be replaced or interfaced with digital telephone networks over fiber optic cables. Computer networks also began to use fiber optic cables instead of copper phone lines, thus allowing transmission over longer distances without regeneration and increased bandwidth (data transmission rates).

Starting in 1988, fiber optic cables connected continents through undersea installation, which largely replaced the use of satellites in intercontinental communications. Because fiber optic cables made communications more secure (they were harder to hack than radio and microwaves), the latter presented a new challenge for the MWSN. Thus, the changing face of technology changed the realities of mass surveillance.

Because underwater fiber optic cables, especially the emerging generations of them, were very difficult, dangerous, and costly to tap (through the use of specially equipped submarines),[2] they were usually tapped when they surfaced on dry land at routing switches. This meant that the switches located at telecommunication companies needed to be the junctures for connecting up transnational, mass spying equipment.

DOI: 10.1057/9781137408211.0004

The Total Information Awareness Project

Converging with this technological reorientation, geopolitics also began to shift from focus on what was left of the old Soviet Union (disbanded in 1991) to greater interest in the Middle East as a focal point of US military involvement. In particular, the Project for the New American Century (PNAC), a neoconservative political action organization, founded in 1998, consisting of many of the soon-to-be cabinet members of the George W. Bush administration, launched an aggressive campaign for removing Saddam Hussein from Iraqi leadership. This campaign was brought to a head when, on September 11, 2001, the World Trade Center in New York City and the Pentagon in Washington were attacked, thus giving the Bush administration its "official" reason for invading Iraq. Here was a new geopolitical rationale for an even more aggressive MWSN, in the name of national security.[3] But this time it was to be anchored to the administration's proclaimed "war on terror" rather than to the prior "cold war" with the Russians.[4] Because terrorists could be plotting anywhere and everywhere, there was now an argument for expanding the tentacles of the MWSN to cover all communications, both domestic and foreign. This alleged need became the catalyst for the "The President's Surveillance Program," also known as the "Total Information Awareness" (TIA) project, which was authorized by George W. Bush within a couple weeks of the September 11 attacks.[5]

Subsequent to this presidential authorization, in January 2002, the Department of Advanced Research Projects Agency (DARPA), a branch of the US Department of Defense (DOD) established the "Information Awareness Office" (IAO) to direct the research and development of the TIA project. The IAO's mission was accordingly to "imagine, develop, apply, integrate, demonstrate, and transition information technologies, components and prototype, closed-loop, information systems that will counter asymmetric threats by achieving *total information awareness.*" In other words, it sought to take the earlier MWSN to the next logical step, by building a massive network of integrated computer technologies for intercepting, storing, searching, monitoring, reading, and analyzing all private, computerized records of 300 million Americans in addition to the electronic messages of millions of foreign users passing through it switches.

Former Reagan National Security advisor, John Poindexter, was named the director of the TIA project. It was, in fact, Poindexter along

DOI: 10.1057/9781137408211.0004

with Hicks & Associates executive, Brian Sharkey, who had proposed the idea of this all-seeing spy network to the DOD after the 9/11 attacks. Poindexter attained notoriety when, in 1990, he had been convicted of multiple felonies in the Iran-Contra scandal. Although these convictions were later reversed, his appointment to oversee this massive, spy operation did not help to foster a positive public perception of this already ethically contentious program when it soon came to public attention.

The IAO and TIA were publicized in February 2002[6] when *The New York Times* published an article about it. The article stated,

> One component of the new computer information system that is being emphasized by Mr. Poindexter's new office are 'data mining' techniques intended to scan through vast collections of computer data, which may include text, images, sound and other computer data, and find significant patterns.

On November 21, 2002, the American Civil Liberties Union (ACLU) began an aggressive campaign against TIA, stating,

> Recent news reports have revealed the development of a new federal program dubbed "Total Information Awareness". The program will create a computer system that will search through a vast centralized database that contains information about your purchases, your medical history, your school records, and more. Help stop this domestic spying program.[7]

As a result of adverse publicity, in 2003, Congress allegedly defunded the TIA project and closed the IAO; but the project had instead been secretly transferred to the Advanced Research and Development Activity (ARDA), a branch of the NSA.[8]

In fact, in late 2002 and early 2003, the NSA had already begun to deploy the TIA technologies that were transferred to it. One veridical source of such NSA deployment at this time is former AT&T technician and whistleblower, Mark Klein, who, like Edward Snowden in 2013, based his claims on official design documents.[9]

The Klein disclosures

In October 2003, Klein was chief technician for the AT&T WorldNet Internet room at AT&T's Folsom Street facility in San Francisco. According to Klein's sworn legal declaration filed on June 8, 2006,[10] this

DOI: 10.1057/9781137408211.0004

room contained routers, modems, and other telecommunications equipment that was used to direct electronic communications such as emails and web browsing requests sent to or from AT&T WorldNet internet customers. Klein disclosed an "SG3 [Study Group 3] Secure Room" (room number 641A) built in January 2003 at the Folsom facility, admission to which required NSA clearance. As corroborated by 2002 and 2003 AT&T documents obtained by Klein, the in-service fiber optical circuits in the WorldNet Internet room on the 7th floor of the Folsom facility were connected to a "splitter cabinet," which used fiber optic splitting technology to split the light signals going through the fiber optic cables thereby sending copies of the signals to the SG3 Secure Room on the 6th floor. These circuits, which were tapped, included "peering links" that connected WorldNet to national and international internet networks of non-AT&T telecommunications companies.

According to Klein's declaration,

> Starting in February 2003, the "splitter cabinet" split (and diverted to the SG3 Secure Room) the light signals that contained the communications in transit to and from AT&T's Peering Links with the following Internet networks and Internet exchange points: ConXion, Verio, XO, Genuity, Qwest, PAIX, Allegiance, Abovenet, Global Crossing, C&W, I6 UUNET, Level3, Sprint, Telia, PSINet, and MAE-West.[11]

According to Klein, inside the SG3 Secure Room was equipment such as Sun servers and Juniper (M40e and M160) "backbone" routers as well as a Narus STA 6400 Semantic Traffic Analyzer.[12] This was the equipment for capture, storage, analysis, and routing of masses of electronic information, which was being diverted to this secret room by the NSA. As Klein concluded, "Based on my understanding of the connections and equipment at issue, it appears the NSA is capable of conducting what amounts to vacuum-cleaner surveillance of all the data crossing the internet—whether that be peoples' e-mail, web surfing or any other data."[13]

Klein's assessment is borne out by the nature of the technology he had identified. Narus'[14] STA (Semantic Traffic Analyzer) 6400 was a high-speed content filter capable of monitoring 622 Megabits per second as of May, 2000.[15] It could scan packets of information in real time, as they traveled past a tap point, searching for predefined key terms including web browser search terms, IP addresses, phone numbers, email addresses, and (as in the case of VoIP) phone numbers.[16] Once it captured data

DOI: 10.1057/9781137408211.0004

satisfying its predefined matching criteria, it could reconstruct, store, and create an actionable database, including the contents of email messages, IMs, internet searches, VoIP phone messages, and other electronic communications, which could then be queried and analyzed. According to Narus, its capabilities included "playback of streaming media (i.e. VoIP), rendering of web pages, examination of e-mail and the ability to analyze the payload/attachments of e-mail or file transfer protocols."[17] In other words, the Narus STA did not merely collect "metadata" (data about data such as telephone numbers, header information, dates, times, and addresses) but also the content of electronic communications that filtered through and met its matching search criteria.[18]

However, the Folsom facility, with its elaborate content filtering and analysis capabilities, appears to have been just one tentacle of the NSA spy network. Klein also maintained that other "splitter cabinets" had been installed at other AT&T facilities including Seattle, San Jose, Los Angeles, and San Diego. Corroboratively, in 2006, Salon disclosed that, according to two anonymous former AT&T workers, AT&T had also maintained a secret room in its Bridgeton facility in St. Louis, which was the main hub of AT&T's WorldNet.[19]

The New York Times' report of December 16, 2005, is often credited with having brought the Bush MWSN to public light. After one year of holding onto the story, due to pressure from the Bush administration, before finally publishing it, the *Times* wrote,

> Under a presidential order signed in 2002, the intelligence agency has monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible "dirty numbers" linked to al-Qaeda, the officials said. The agency, they said, still seeks warrants to monitor entirely domestic communications.[20]

However, the *Times*' characterization of the Bush MWSN was palpably inconsistent with Klein's characterization, which, based on design documents, was consistent with a much wider search than international traffic. "These installations, said Klein, "only make sense if they're doing a huge, massive domestic dragnet on everybody, in the United States."[21] Further, according to the 2009 Report on the President's Surveillance Program, other surveillance activities besides those published in the *Times* were also authorized by the President but the details of those activities remained classified. This is consistent with

DOI: 10.1057/9781137408211.0004

the wider scope of the Klein declarations, which included vacuuming up of all internet data passing through AT&T switches.

In the aftermath of the Snowden disclosures, we have seen that the program did more than just monitor international calls. It also sucked up masses of domestic electronic messages; and it included both archival as well as real-time monitoring. But Snowden was not simply describing the evolution of the program after Bush left office; his report was corroborated years earlier by Mark Klein, who also produced design documents to prove it. Indeed, given that the design documents obtained by Klein make clear that *all* data from the peering links of the WorldNet Network were being copied by the optical splitters, there is only one consistent conclusion that can be drawn. This conclusion is that, with reference to such facilities as the AT&T Folsom facility, all internet traffic, not just international traffic, was being monitored by the NSA. Moreover, the monitoring was not just of archived data; for the Narus STA filters all data as it passes through the tap point.

While Klein's disclosures addressed *internet* monitoring, he maintained that even telephone calls placed through the public switched telephone network (PSTN), which is now almost entirely digital, as well as cell phone calls, were also being swept up and routed to NSA computers via optic splitters.[22] This would have included the content of the phone calls. However, there is other personal information that can be mined from phone calls besides their content.

The domestic phone call metadata program

On May 11, 2006, *USA Today* leaked a further surveillance program operated by the NSA along with international call monitoring and Internet surveillance. Also begun shortly after the September 11, 2001 attacks, this additional program monitored all domestic phone calls, that is, all calls originating and terminating in the US, by collecting call "metadata" such as phone numbers, duration, times, and dates. *USA Today* wrote, "With access to records of billions of domestic calls, the NSA has gained a secret window into the communications habits of millions of Americans."[23] Allegedly, this metadata program, conducted with cooperation from Verizon, BellSouth, and AT&T, was aimed at identifying and tracking suspected terrorists. However, it is questionable at first blush as to how the amassing of such call data could *itself* have proven effective in

DOI: 10.1057/9781137408211.0004

identifying and tracking particular individuals. In fact, in December 2013, a White House review panel on surveillance concluded that there was "absolutely" no evidence that the bulk collection of phone records prevented *any* terrorist attacks.[24]

It would be presumptuous to assume, however, that the various tentacles of the MWSN have been parallel rather than intersecting. Thus, the metadata collected through the metadata collection system (say caller names cross referenced with particular metadata such as phone numbers[25]) could provide key words for content filtering performed by the Narus STA. In this way, an interesting pattern of metadata (one that did not fit the average domestic caller) could, potentially, provide input for an internet search, which, in turn, could connect the phone metadata with other *content data*. Thus, the popular assumption that the metadata program was "only" collecting metadata could be very misleading. "[N]obody's listening to the content of people's phone calls,"[26]maintained President Obama, referring to the present program of bulk metadata collection. However, while technically true, this can be misleading, inasmuch as the monitoring of bulk domestic call metadata is and has always been part of an integrated system of technologies that does, indeed, look at content.

Furthermore, in a footnote to an October 2011 heavily redacted Foreign Intelligence Surveillance Court decision (released in 2013), the Court informed that in March 2009, it had concluded that its prior authorization of the NSA's bulk phone records program had been based on "a flawed depiction of how the NSA uses [the acquired] metadata," and that "[t]his misperception by the FISC existed from the inception of its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime." In particular, contrary to government assurances, the NSA had been regularly "running queries of the metadata using querying terms that did not meet the required standard for querying".[27] Such a standard required that a "reasonable articulable suspicion" exist that the search term, such as a phone number, was associated with one of certain identified international terrorist organization such as al-Qaeda. On the other hand, it had not given government permission to conduct "wholesale data mining or browsing".[28] As such, the Court concluded that the government's own requirements for conducting queries had been "so frequently and systemically violated that it can fairly be

DOI: 10.1057/9781137408211.0004

said that this critical element of the overall . . . has never functioned effectively".[29]

With reference to bulk metadata collection, Obama also stated, "if the intelligence community then actually wants to listen to a phone call, they've got to go back to a federal judge, just like they would in a criminal investigation".[30] These words mirror those of former President George W. Bush, who, on April 20, 2004, assured the American public that, "*any time* you hear the United States government talking about wiretap, it requires—a wiretap requires a court order. Nothing has changed, by the way".[31] And while Bush tried later to get out of it by claiming he was only referring to roving wire taps and not FISA searches, the writing was indelibly on the wall—he said "any time" the government talks about wiretaps. And, well before this statement, in July 2002, James A. Baker, counsel for Bush's Department of Justice, swore under oath before the Senate Intelligence Committee during its hearings regarding proposed amendments to the Foreign Intelligence Surveillance Act (FISA), that, before connecting up surveillance equipment and potentially engaging in physical searches, "you would have had a finding by a neutral and detached magistrate, and indeed in this case a sitting federal judge, district court judge . . .".[32]

The words of both Bush and Baker were indisputably betrayed by the July 10, 2009 report on the President's Surveillance Program prepared by the Office of Inspectors General of the intelligence community. According to the report, the "President's Surveillance Program" was authorized by President George W. Bush shortly after the 9–11 attacks, and James A. Baker was one of the privileged few who had knowledge of the program from its very inception in October 2001.[33]

So, clearly, mass government deception has been a persistent part of the history of mass warrantless surveillance in the US, and, in the aftermath of the Snowden disclosures, it does not appear that much has changed.

PRISM

As disclosed by Snowden, in 2007, George W. Bush began another tentacle of the MWSN, code named PRISM. This system downloads internet and voice over IP data "directly from" the servers of nine major internet companies—Microsoft (Hotmail, etc.), Google, Yahoo,

DOI: 10.1057/9781137408211.0004

Facebook, Paltalk, YouTube, Skype, AOL, and Apple. This also includes real-time data.[34] More particularly, data retrieved from this system includes email, chat (video and voice), videos photos, stored data, VoIP, file transfers, video conferencing, notification of target activities (logons, etc.), online social networking details, and special requests.[35]

The PRISM program is supposed to be conducted in accordance with Section 702 of the Foreign Intelligence Surveillance Act Amendments Act of 2008, which provides that US citizens not be targeted. However, the reality is that an analyst can gain access to entire data bases with a so-called, "reasonable belief" that a subject is engaged in terrorism, espionage, or related activities.[36] According to one NSA slide, when an NSA analyst "tasks" the PRISM system for information about a new surveillance target, the request goes to a supervisor who must approve the analyst's "reasonable belief," which is defined as "51 percent confidence, that the specified target is a foreign national who is overseas at the time of collection".[37] Obviously, this leaves much room for error (49%) even if an objective probability assessment can be made in the first place, which is doubtful.

According to a "User's Guide for PRISM Skype Collection," conversations utilizing a conventional telephone on one end can be monitored for audio; and when the connection is entirely through a computer, the conversation can be monitored for any combination of "audio, video, chat, and file transfers". Monitoring of Google includes "Gmail, voice and video chat, Google Drive files, photo libraries, and live surveillance of search terms". According to Snowden, "They quite literally can watch your ideas form as you type."[38]

UPSTREAM programs

Alongside PRISM, is a set of programs called "UPSTREAM," which intercept and upload domestic and international telephone and internet traffic at switches inside telecommunication companies while it is in the process of being routed to and from servers throughout the world. The first stage of filtering is done by the telecommunication companies themselves.[39] This prescreening phase is allegedly conducted according to NSA algorithms, which aim at collecting data involving at least one person "reasonably believed" to be outside the US that may have foreign intelligence significance. The NSA, in turn, can access this information

DOI: 10.1057/9781137408211.0004

and apply finer filtering algorithms aiming at capturing data involving particular persons or organizations.[40]

Whereas the earlier UPSTREAM programs such as the one reported by Mark Klein in 2005 used analytics such as that provided by the Narus STA 6400, the technologies for filtering and analysis appear to have evolved considerably. To filter the stream of data flowing past a tap point, the NSA now utilizes filters code named TURMOIL. This collection system works in conjunction with another program code named XKEYSCORE (developed with help from military contractor Science Applications International Corporation [SAIC]), which takes in the captured data and conducts "deep packet" inspection and analysis of the data. The system can store unprocessed data in local caches for up to three days and it can store locally processed metadata for up to 30 days.

Consisting of approximately 700 servers distributed throughout the world (with 150 location sites), the system searches for and analyzes "soft selectors"—content of communications such as email, chats, and web searches. It also searches for "strong selectors"—metadata including phone numbers, e-mail addresses, logins, and user activity; and it contains a series of specialized plug-ins that "extract and index" metadata into tables. It also answers queries without having strong selectors. For example, using the system, the NSA claims to be able to locate terrorist cells or find the email address of a terrorist by looking for "anomalous" events such as "someone whose language is out of place for the region they are in; someone who is using encryption; someone searching the web for suspicious stuff".[41]

One problem with the earlier Narus system was that the more precise the search criteria were, the less data could be filtered. XKEYSCORE has apparently greater ability to search through more data using more precise definitions. This appears to be due to its ability to store more unprocessed data in local caches.[42] In an interview on January 26, 2014, with German broadcaster Nord Deutscher Rundfunk, Edward Snowden described the capacity of XKEYSCORE in stark terms:

> You could read anyone's email in the world. Anybody you've got email address for, any website you can watch traffic to and from it, any computer that an individual sits at you can watch it, any laptop that you're tracking you can follow it as it moves from place to place throughout the world. It's a one stop shop for access to the NSA's information. And what's more you can tag individuals using "XKeyscore". Let's say, I saw you once and I thought what you were doing was interesting or you just have access that's interesting to

DOI: 10.1057/9781137408211.0004

> me, let's say you work at a major German corporation and I want access to that network, I can track your username on a website on a form somewhere, I can track your real name, I can track associations with your friends and I can build what's called a fingerprint which is network activity unique to you which means anywhere you go in the world anywhere you try to sort of hide your online presence hide your identity, the NSA can find you and anyone who's allowed to use this or who the NSA shares their software with can do the same thing.[43]

Using XKEYSCORE, an analyst need only enter the target's email address into an online search form, the time periods to be searched, and the "justification" for the search. Forms also exist to monitor other online activities including social media such as Facebook.[44] As part of the system, the NSA also operates a program codenamed QUANTUM, which works cooperatively with the telecommunication companies to place NSA routers and servers at key places on the internet backbone. When a targeted individual attempts to access a website, a covert server (codenamed FOXACID) reacts faster than the other website server (due to its proximate location within the internet backbone), thereby connecting the target to an NSA server (so-called, "man in the middle" attacks). This, in turn, enables the NSA to download cookies and other malicious code onto the target's computer from the NSA website. There is also a program codenamed MARINA that takes photos from a targeted computer's webcam.[45] Because this attack mode is automated, it can be launched en masse. Thus, the potential (if not the reality) exists for having masses of internet users, including any US citizen, hooked into, aggressively monitored, and manipulated by the MWSN.[46]

UPSTREAM programs include BLARNEY, which is a set of internet and telephone monitoring systems including an internet system resembling the one described by Mark Klein that was set up in the SG3 Secure Room 641A at the AT&T Folsom Street facility in San Francisco. The main targets of BLARNEY allegedly involve counter proliferation, counter-terrorism, foreign diplomats and governments, and economic and military targets.[47] Another UPSTREAM program is STORMBREW, which is an internet and telephone monitoring system that is allegedly operated in cooperation with Verizon and has "global" targets.[48] Still another UPSTREAM program is MADCAPOCELOT, which is allegedly for collecting internet content and metadata with key targets involving Russia and European counter-terrorism, thus connecting it, at least in its target, to ECHELON. FAIRVIEW is another collection of UPSTREAM

DOI: 10.1057/9781137408211.0004

programs, including BLARNEY, which is supposed to collect intercontinental email and telephone messages.[49]

UPSTREAM programs intercept a data stream "in transit" at a tap point before it reaches its destination, whereas PRISM receives data that has already reached the server. While PRISM has received the most press, it is actually the lesser known UPSTREAM programs that comprise a global system that can intercept data on both public switched telephone networks (PSTN) as well as Internet Protocol (IP) Networks.[50]

UPSTREAM programs whose collection occurs at telecommunication companies inside the US (such as FAIRVIEW, BLARNEY, and STORMVIEW) are supposed to operate pursuant to the 2008 Foreign Intelligence Surveillance Amendments Act. This means that they are not supposed to collect information from any US person, either inside or outside the US. However, there is clear indication from the Foreign Intelligence Surveillance Court itself that these programs have not done so in the past. In a 2011 decision, the Court found reason to believe that the NSA's UPSTREAM collections had not been operating pursuant to the FISA and the Fourth Amendment:

> Indeed, the record before this Court establishes that NSA's acquisition of internet transactions likely results in NSA acquiring annually tens of thousands of *wholly domestic communications*, and tens of thousands of *non-target communications* of persons who have little or no relationship to the target but who are protected under the Fourth Amendment. Both acquisitions raise questions as to whether NSA's targeting and minimization procedures comport with FISA and the Fourth Amendment.[51]

Notwithstanding its findings, the Court concluded that UPSTREAM collections are limited by the technological inability to restrict collections entirely to 702 compliance requirements. This is because UPSTREAM collections proceed in terms of "Multiple Communication Transactions" (MCTs), which like the contents of an email inbox, include a number of unrelated messages. As such, there is a substantial probability of collecting communications from persons who are not targeted or which are between two US persons inside the US or its territories. Thus, pursuant to the FISA, the Court focused instead on recommending changes to "minimization procedures," that is, procedures "reasonably designed…to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting United States persons…".[52] This meant that the Court elected to allow the NSA

DOI: 10.1057/9781137408211.0004

to continue to acquire information that is prohibited in the first place from being collected pursuant to FISA, and to address minimizing its retention and dissemination after the fact.

Unfortunately, such "minimizing" does not begin to address the problem of legal protections, because the UPSTREAM component of the MWSN has also grown tentacles that have entirely outstripped legal oversight and operate completely beneath the radar of any privacy protections or "minimization standards" whatsoever. This component of the system, which collects data outside the US (and thus outside FIS Court oversight[53]), has received the least publicity to date. One such set of programs is code named WINDSTOP, and one of its programs is code named MUSCULAR, which is operated jointly by NSA and GCHQ of Great Britain.[54]

WINDSTOP/MUSCULAR and INCENSOR

MUSCULAR intercepts data passing between the internal data storage centers of Yahoo and Google. An unnamed overseas telecommunication company is providing access through a switch or cable it controls. The access point is known as DS-200B.[55] According to a March 14, 2013 issue of *Special Source Operations Weekly*, an internal NSA publication, MUSCULAR is collecting "too much" data from Yahoo "Narchive email traffic" (a proprietary data transfer format) that has little intelligence value. This massive amount of data (181 million records from December 2012 to January 2013[56]) is said to constitute one quarter of the daily collection sent to PINWALE, one of NSA's main storage, search, and retrieval systems for email and chat data located in Fort Meade, Maryland.[57] This data is also filtered through TURMOIL, the technology that handles other UPSTREAM data collections.[58] This data includes the contents, not just the metadata, of personal email messages. In addition, these messages are so formatted such that, when collected, any attachments to them are included within the body of the messages themselves. In addition, these messages are not presently encrypted, thereby making them softer targets for data collection purposes.[59] Encrypting data streams may not prove to be a solution (at least in the long-term) inasmuch as the NSA appears to be building a "Quantum" computer infinitely faster than the standard computer and capable of breaking even the strongest encryption algorithms.[60]

DOI: 10.1057/9781137408211.0004

Further, while the collection point is located in the United Kingdom, this does not mean that the personal information of US persons is not being collected. In fact, because purely domestic digital communications is often routed through and stored on overseas servers, such communications and their cloud storage "do not usually adhere to national boundaries".[61] As a consequence, MUSCULAR, in addition to other overseas collects have "amassed content and metadata on a previously unknown scale from US citizens and residents".[62] Further, MUSCULAR is one of several other WINDSTOP programs. Another program in this group, code named INCENSOR, collects billions more records than MUSCULAR, which presumably also includes masses of records of US persons. According to an NSA slide, INCENSOR had collected over 14 billion records from December 2012 to January 2013.[63]

Instant message and email contact collections

Yet a further tentacle of this colossal umbrella of surveillance programs within the ever-expanding MWSN includes one that collects instant message and email contact lists.[64] As part of its overseas (and therefore judicially unregulated) collections, the NSA also collects hundreds of millions of contact lists from personal e-mail and instant messaging accounts which are projected to include tens of millions of contact lists belonging to US persons. Such data, therefore, has the potential for allowing government to create profiles of American citizens by connecting their personal, professional, political and religious activities and beliefs.[65] In such a case, the danger goes beyond the obvious abridgment of privacy by opening up the possibility of creating false or misleading associations with persons with whom one may not have had any substantive relationship, for example, a Facebook "friend" whom one does not really know.

The legal quandary

As is evident from the historical survey and timeline in this chapter, technological development of the MWSN, from the late sixties to date, largely spawned by the digitization of mass communication, has made it increasingly easier to collect and store masses of data, much of which

DOI: 10.1057/9781137408211.0004

has had no value for foreign intelligence gathering purposes, and much of which, as in the case of purely domestic messages, has been unlawfully collected pursuant to FISA and the Fourth Amendment. This has left the US government in a quandary about how to legally justify such massive quantities of acquisitions. Unfortunately, the technology has dictated the changes in law rather than the law having dictated the changes. The next chapter addresses the legal context of this problem.

Notes

1 "Somebody's Listening," *New Statesman*, August 12, 1988. Accessed on June 17, 2014, from http://cryptome.org/jya/echelon-dc.htm#echelon.

2 Neil, Jr., "Spy Agency Taps into Undersea Cable," *ZDNet*, May 23, 2001. Accessed on June 17, 2014, from http://www.zdnet.com/news/spy-agency-taps-into-undersea-cable/115877.

3 Although, according to a 2006 *Bloomberg* article, in court papers filed in New York federal court, lawyers in a suit against three major telecoms, including AT&T, claimed that the NSA had asked AT&T to "help it set up a domestic call monitoring site seven months before the Sept. 11, 2001 attacks." Also, according to the article, the NSA said on its website that in June 2000, it was seeking bids for a project to "modernize and improve its information technology infrastructure" as part of the NSA's "Pioneer Groundbreaker" project. These allegations appear to undermine the rationale advanced by the George W. Bush administration for building a more aggressive MWSN. If true, the Bush administration had planned to "modernize and improve" its system of surveillance several months before the 9–11 attacks. See Andrew Harris, "Spy Agency Sought US Call Records Before 9–11, Lawyers say," *Bloomberg*, June 30, 2006. Accessed on June 17, 2014, from http://www.bloomberg.com/apps/news?pid=newsarchive&sid=abIVocO64zJE.

4 It is not unreasonable to conjecture that, recent events in Ukraine, including the blowing up of a commercial Boeing 777, with 298 passengers on board, allegedly by pro-Russian separatists using a Russian-made aircraft missile, may increase US spying on Russia and its allies. Sabrina Tavernise, Eric Schmitt, and Rick Gladstone, "Jetliner Explodes Over Ukraine; Struck by Missile, Officials Say," *New York Times*, July 17, 2014. http://www.nytimes.com/2014/07/18/world/europe/malaysian-airlines-plane-ukraine.html .

5 In September and early October 2001, Department of Justice Attorney, John Yoo, prepared several opinions about "hypothetical random domestic electronic surveillance activities;" but the opinion that addressed the legality of these surveillance activities was not even drafted until after the program

DOI: 10.1057/9781137408211.0004

had been authorized by President Bush in October 2001. Subsequently, when the opinion was drafted, it was found constitutionally deficient. Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, Office of the Director of National Intelligence, "Unclassified Report on the President's Surveillance Program," July 10, 2009. Accessed on June 17, 2014, from https://www.fas.org/irp/eprint/psp.pdf.

6 John Markoff, "Chief Takes Over New Agency to Thwart Attacks on U.S.," *New York Times,* February 13, 2002. Retrieved on June 9, 2009, from http://www.ratical.org/ratville/JFK/JohnJudge/linkscopy/PoindyToIAO.html.

7 American Civil Liberties Union, Action Alert, November 21, 2002, cited in Mass Surveillance and State Control: The Total Information Awareness Project. New York: Palgrave Macmillan, 2010, p. 21.

8 Cohen, Mass Surveillance and State Control.

9 "Declaration of Mark Klein In Support Of Plaintiffs 'Motion For Preliminary Injunction," *Hepting v. AT&T*, North District of California, June 8, 2006. Retrieved on June 17, 2014, from https://www.eff.org/node/55051.

10 Ibid.

11 Ibid., paragraph 31.

12 Ibid.

13 "Wiretap Whistleblower's Account," *Wired*, April 2006. Retrieved on June 17, 2014 from http://www.wired.com/science/discoveries/news/2006/04/70621.

14 Narus is now a subsidiary of Boeing.

15 Bewert, "All about NSA's and AT&T's Big Brother Machine, the Narus 6400," *Daily Kos*, April 7, 2006. Retrieved on June 17, 2014 from http://www.dailykos.com/story/2006/04/08/200431/-All-About-NSA-s-and-AT-T-s-Big-Brother-Machine-the-Narus-6400.

16 Sean Gallagher, "What the NSA can do with "big data", *Ars Technica*, June 11, 2013. Retrieved on June 17, 2014 from http://arstechnica.com/information-technology/2013/06/what-the-nsa-can-do-with-big-data/.

17 Bewert, "All about NSA's and AT&T's Big Brother Machine, the Narus 6400." Retrieved on June 17, 2014 from http://www.dailykos.com/story/2006/04/08/200431/-All-About-NSA-s-and-AT-T-s-Big-Brother-Machine-the-Narus-6400#.

18 In 2013, Narus's had capacity for chaining, merging, and contextualizing data; learning as data increased; making predictions, and creating profiles of targets. The term "Semantic Analyzer" suggests that the earlier versions also had the same or similar *meaning* analysis capabilities although probably less efficient in their functionality. "NARUS n SYSTEM," Narus website. Retrieved on June 17, 2014 from http://narus.com/images/pdf/Narus_nSYSTEM_brochure.pdf.

DOI: 10.1057/9781137408211.0004

19 Kim Zetter, "Is the NSA spying on U.S. Internet traffic?" *Salon*, June 21, 2006. Retrieved on June 17, 2014 fromhttp://www.salon.com/2006/06/21/att_nsa/.

20 James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005. Retrieved on June 17, 2014 from http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=print&_r=0.

21 Mark Klein, "Domestic Surveillance and AT&T" (Video), *CSPAN*, November 2007. Retrieved on June 17, 2014 from http://www.c-span.org/video/?201508–6/domestic-surveillance-att.

22 Ibid.

23 Leslie Cauley, "NSA has massive database of Americans' phone calls," *USA Today*, May 11, 2006. Retrieved on June 17, 2014 from http://usatoday30.usatoday.com/news/washington/2006–05–10-nsa_x.htm.

24 Michael Isikoff, "NSA program stopped no terror attacks, says White House panel member," *NBC News*, December 20, 2013. Retrieved on June 17, 2014 fromhttp://investigations.nbcnews.com/_news/2013/12/20/21975158-nsa-program-stopped-no-terror-attacks-says-white-house-panel-member?lite.

25 While it has been claimed that the bulk metadata collection system disclosed in 2006 did not retrieve caller names and addresses, it was also clear that such data could easily be obtained by cross-referencing phone numbers with other existing databases. Leslie Cauley, "NSA has massive database of Americans' phone calls."

26 "Transcript: Obama's Remarks on NSA Controversy," *Wall Street Journal*, June 7, 2013. Retrieved on June 17, 2014 from http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/.

27 U.S. FIS Court, Memorandum Opinion, April 22, 2011, note 14. Retrieved on June 17, 2014 from https://ia601003.us.archive.org/1/items/775440-fisc-opinion-unconstitutional-surveillance-0/775440-fisc-opinion-unconstitutional-surveillance-0.pdf.

28 "U.S. FIS Court, Amended Memorandum Opinion, October, 2011, note 7. Retrieved on June 17, 2014 from https://www.aclu.org/files/assets/br13–09-primary-order.pdf.

29 U.S. FIS Court, Memorandum Opinion, April 22, 2011, note 14.

30 "Transcript: Obama's Remarks on NSA Controversy," *Wall Street Journal*, June 7, 2013. Retrieved on June 17, 2014 from http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/.

31 "Bush defends NSA spying program," *CNN.com*, January 1, 2006. Retrieved on June 17, 2014 from http://www.cnn.com/2006/POLITICS/01/01/nsa.spying/.

32 Glenn Greenwald, "The Administration's pattern of deceit re: eavesdropping," *Unclaimed Territory*, January 31, 2006. Retrieved on June 17, 2014 from http://glenngreenwald.blogspot.com/2006/01/administrations-pattern-of-deceit-re.html.

DOI: 10.1057/9781137408211.0004

33 Offices of Inspectors General of the Department of Defense, et al, "Unclassified Report on the President's Surveillance Program," July 10, 2009, p. 10.

34 "Depending on the provider, the NSA may receive live notifications when a target logs on or sends an e-mail, or may monitor a voice, text or voice chat as it happens (noted on the first slide as "Surveillance")." "NSA slides explain the PRISM data-collection program," *Washington Post*, June 6, 2013. Retrieved on June 17, 2014 from http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

35 Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *Washington Post*, June 7, 2013. Retrieved on June 17, 2014 from 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.

36 Ibid.

37 "NSA slides explain the PRISM data-collection program," *Washington Post*, June 6, 2013. Retrieved on June 17, 2014 from http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

38 Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *Washington Post*, June 7, 2013. Retrieved on June 17, 2014 from 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.

39 Siobhan Gorman and Jennifer Valentino-Devries, "New Details Show Broader NSA Surveillance Reach," *Wall Street Journal*, August 20, 2013. Retrieved on June 17, 2014 from http://online.wsj.com/news/articles/SB10001424127887324108204579022874091732470.

40 Siobhan Gorman and Jennifer Valentino-Devries, "What You Need to Know on New Details of NSA Spying," *Wall Street Journal*, August 20, 2013. Retrieved on June 17, 2014 from http://online.wsj.com/news/articles/SB10001424127887324108204579025222244858490.

41 National Security Agency (NSA), XKEYSCORE Slide, February 25, 2008. Retrieved on June 17, 2014 from http://www.documentcloud.org/documents/743244-xkeyscore-slidedeck.html. See especially slide labeled, "Finding Targets." The problem of false positives generated by such searches is a serious problem, however. See Chapter 3.

42 Sean Gallagher, "Building a panopticon: The evolution of the NSA's XKeyscore," *Ars Technica*, August 9, 2013. Retrieved on June 17, 2014 from http://arstechnica.com/information-technology/2013/08/building-a-panopticon-the-evolution-of-the-nsas-xkeyscore/.

DOI: 10.1057/9781137408211.0004

43 Edward Snowden, Interview with Hubert Seipel, *NDR News*, January 26, 2014. Retrieved on June 17, 2014 from http://www.commondreams.org/headline/2014/01/27–1.

44 Glenn Greenwald, "XKeyscore: NSA tool collects 'nearly everything a user does on the internet'," *The Guardian*, July 31, 2013. Retrieved on June 17, 2014 from http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

45 Jason Mick, "Tax and Spy: How the NSA Can Hack Any American, Stores Data 15 Years," *Daily Tech*, December 31, 2013. Retrieved on June 17, 2014 from http://www.dailytech.com/Tax+and+Spy+How+the+NSA+Can+Hack+Any+American+Stores+Data+15+Years/article34010.htm.

46 Spiegel Staff, "Inside TAO: Documents Reveal Top NSA Hacking Unit," *Spiegel International*, December 29, 2013. Retrieved on June 17, 2014 from http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969–3.html. Mike Masnick, "How The NSA Pulls Off Man-In-The-Middle Attacks: With Help From The Telcos," *Techdirt*, October 4, 2013. Retrieved on June 17, 2014 from http://www.techdirt.com/articles/20131004/10522324753/how-nsa-pulls-off-man-in-the-middle-attacks-with-help-telcos.shtml. Sean Gallagher, "Quantum of pwnness: How NSA and GCHQ hacked OPEC and others," *Ars Technica*, November 12, 2013. Retrieved on June 17, 2014 from http://arstechnica.com/information-technology/2013/11/quantum-of-pwnness-how-nsa-and-gchq-hacked-opec-and-others/.

47 "Slides about NSA's Upstream collection," Top Level Telecommunications, January 17, 2014. Retrieved on June 17, 2014 from http://electrospaces.blogspot.com/2014/01/slides-about-nsas-UPSTREAM-collection.html.

48 Ibid.

49 Ibid.

50 "BOUNDLESSINFORMANT only shows metadata ," *Top Level Telecommunications*, October 22, 2013. Retrieved on June 17, 2014 from http://electrospaces.blogspot.com/2013/10/boundlessinformant-only-shows-metadata.html.

51 U.S. FIS Court, Memorandum Opinion, April 22, 2011.

52 U.S. Code 50 (1978), Section1801. Retrieved on June 17, 2014 from http://www.law.cornell.edu/uscode/text/50/1801.

53 Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *Washington Post*, October 30, 2013. Retrieved on June 17, 2014 from 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.

DOI: 10.1057/9781137408211.0004

54 The set of programs code named "OAKSTAR" also appear to operate intercept facilities outside the US. Both OAKSTAR and MUSCULAR are UPSTREAM programs operating outside the US, but any further connections, if any, are not clear. "Slides about NSA's Upstream collection," *Top Level Telecommunications*, January 17, 2014.

55 "How the NSA's MUSCULAR program collects too much data from Yahoo and Google," *Washington Post*, October 30, 2013.

56 "One month, hundreds of millions of records collected," *Washington Post*, November 4, 2013. Retrieved on June 17, 2014 from http://apps.washingtonpost.com/g/page/world/one-month-hundreds-of-millions-of-records-collected/554/.

57 "How the NSA's MUSCULAR program collects too much data from Yahoo and Google," *Washington Post*, October 30, 2013. Retrieved on June 17, 2014 from http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/#document/p2/a129323.

58 Andrea Peterson, "How we know the NSA had access to internal Google and Yahoo cloud data," *Washington Post*, November 4, 2013. Retrieved on June 17, 2014 from http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/.

59 This Yahoo "Narchive" email traffic message carries unrelated data streams that travel with the message data, which must be "demuxed" (separated) from the relevant data. "How the NSA's MUSCULAR program collects too much data from Yahoo and Google," *Washington Post*, October 30, 2013.

60 Jason Mick, "Tax and Spy: How the NSA Can Hack Any American, Stores Data 15 Years," *Daily Tech*, December 31, 2013.

61 Barton Gellman and Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *Washington Post*, October 30, 2013.

62 Ibid.

63 "One month, hundreds of millions of records collected," *Washington Post*, November 4, 2013.

64 "The NSA's problem? Too much data," *Washington Post*, October 15, 2013. Retrieved on June 17, 2014 from http://apps.washingtonpost.com/g/page/world/the-nsas-overcollection-problem/517/.

65 Barton Gellman and Ashkan Soltani, "NSA collects millions of e-mail address books globally," *Washington Post*, October 14, 2013. Retrieved on June 17, 2014 from http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9–11e3–80c6–7e6dd8d22d8f_story.html.

DOI: 10.1057/9781137408211.0004

2

Foreign Intelligence Surveillance Law

Abstract: *This chapter provides the legal context for the development and deployment of the various tentacles of the system. It shows how these "total information awareness" technologies have been honed; how changes in the law such as the FISA Amendments Act and the Patriot Act have kept pace with these technologies, opening up the floodgates for the continued curtailment of privacy rights. It shows how "legal" teeth have been given to what was previously considered violations of Fourth Amendment protections against warrantless search and seizure. It discusses the diminished role of the Foreign Intelligence Surveillance Courts in providing legal oversight. Importantly, it proposes legal reform to harmonize with constitutional rights, and to stop the steady policy creep threatening the demise of privacy, freedom, and dignity.*

Cohen, Elliot D. *Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.* New York: Palgrave Macmillan, 2014.
DOI: 10.1057/9781137408211.0005.

DOI: 10.1057/9781137408211.0005

The history of the growth of the MWSN is clearly one of progressing from greater to lesser judicial oversight. As discussed in Chapter 1, the secret FIS Court has itself admitted the abuses of FISA by the NSA with respect to its targeting and minimization procedures concerning US persons. Additionally, the Court was only addressing data collections conducted in the US over which it has jurisdiction. Thus, the MWSN currently conducts massive overseas collections such as WINDSTOP and OAKSTAR, which vacuum up millions of electronic communications of US persons without any judicial oversight whatsoever.[1] Such "back door" collections also appear to be conducted without the consent of the internet companies whose data pipes are being tapped, such as Google and Yahoo. This should, therefore, concern even the most ardent supporters of big business who may be inclined to see the MWSN as an opportunity for corporate expansion through the allocation of government defense contracts to such corporations. For example, in response to the revelation that the NSA had access to its private, overseas internal server network, David Drummond, the chief legal officer for Google, said that the company was "outraged" and that it has been working to prevent such abridgment of privacy in the future. Such alleged "outrage," even by these powerful members of the corporate sector, provides a barometer to measure the extent to which the MWSN has gone beyond the limits of public tolerance. The adequacy of present legal protections should, therefore, be of concern to all, whether the chief legal officer of Google, a US citizen, or a citizen of any other (digitized) nation. Accordingly, this chapter examines the current legal climate for the purpose of suggesting necessary changes.

The Foreign Intelligence Surveillance Act (1978)

A brief history of US foreign intelligence gathering laws in the past five decades, coinciding with the steady expansion of the MWSN, suggests such a decline in protections against the encroachment of Fourth Amendment rights. The first surveillance law to permit *warrantless* surveillance was the Foreign Intelligence Surveillance Act (FISA) of 1978. Signed into law by President Jimmy Carter, this law was in response to government spying that took place during the sixties and seventies, including the Nixon Whitehouse's activities of spying on perceived political enemies. The law aimed at providing protection

DOI: 10.1057/9781137408211.0005

against Fourth Amendment violations arising from domestic as well as international surveillance by providing greater judicial oversight. Accordingly, it set up a secret Foreign Intelligence Surveillance (FIS) Court to hear ex parte government requests for purposes of issuing search warrants.

The Act permitted the President, acting through the Attorney General, to authorize warrantless electronic surveillance *only if* (1) the surveillance was directed to electronic communications between two "foreign powers"; (2) there was no "substantial likelihood" of capturing the electronic communications of a US person; and (3) proposed "minimization procedures" with respect to the surveillance met the Act's stipulated definition of minimization.[2]

According to the Act's definitions, a "foreign power" was a foreign government (or a group associated with one), international terrorist organization, foreign-based political organization, or an entity engaged in international proliferation of weapons of mass destruction.[3] And "minimization procedures" were defined as ones "reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[4]

Amendments to the Foreign Intelligence Surveillance Act

However, as seen in Chapter 1, shortly after 2001, the George W. Bush administration conducted mass warrantless spying on millions of US citizens, notwithstanding the provisions of the 1978 FISA Act. Thus, in 2007, it was not surprising that the George W. Bush administration sought to make his "President's Surveillance Program", "legal," albeit after the fact, by amending FISA to widen the scope of warrantless surveillance to permit the targeting of persons "reasonably believed" to be outside the US. According to this act, known as the Protect America Act, "Nothing in the definition of electronic surveillance . . . shall be construed to encompass surveillance directed at a person reasonably believed to be located outside of the United States."[5] In effect, this removed the targeting of such persons from the jurisdiction of the FIS

DOI: 10.1057/9781137408211.0005

Courts since the latter courts only regulated "electronic surveillance" as defined by the 1978 FISA. This meant that the government was free to collect such foreign intelligence even if the person outside the US turned out to be a US person or the communication involved persons in the country. Furthermore, it needed only to be claimed that "a "significant purpose" of the acquisition was to obtain foreign intelligence information. Unfortunately, this was consistent with other "significant purposes," including collecting the personal information of US persons. In addition, the Act included provisions to require telecommunication companies to participate in government surveillance but granted them retroactive and prospective immunity to civil suits for violation of customers' privacy. This effectively cancelled a number of class act suites that had been filed against such companies as AT&T for helping the government to spy on its customers. While this Act was short-lived, having sunset in six months, it set a serious precedent for a subsequent amendment of FISA in 2008.

Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, now the law of the land, permits warrantless surveillance as long as it targets a non-US person "reasonably believed" to be outside the US. This means that it could still capture the communications of US persons as long as the overseas target itself is a non-US person. Like its predecessor, the Protect America Act, the 2008 Act requires that only a "significant purpose" for the surveillance be the acquisition of foreign intelligence information. In addition, it also grants retrospective and prospective legal immunity to the telecommunication companies, thereby locking in their mandatory participation in the MWSN.[6] And, in 2012, the Obama administration passed through Congress the FISA Amendments Act Reauthorization Act, which reauthorized the 2008 Act until 2017.[7]

Regarding the rules for querying the data that NSA acquires pursuant to Section 702, in 2008 the FIS Court "effectively impose[d] a wholesale bar on queries using United States-Person identifiers". However, in 2011, the government expanded these rules to allow NSA "to query the vast majority of its Section 702 collection using United States-Person identifiers, subject to approval pursuant to internal NSA procedures and oversight by the Department of Justice."[8] Pursuant to Section 702, all such queries using United States-Person identifiers are supposed to be limited to those "reasonably likely to yield foreign intelligence information."

DOI: 10.1057/9781137408211.0005

According to the NSA's 2011 minimization procedures, its UPSTREAM collections are exempt from using United States-Person identifiers.[9] According to these procedures,

> Identifiers of an identifiable U.S. person may not be used as terms to identify and select for analysis any Internet communication acquired through NSA's upstream collection techniques. Any use of United States person identifiers as terms to identify and select communications must first be approved in accordance with NSA procedures… The Department of Justice's National Security Division and the Office of the Director of National Intelligence will conduct oversight of NSA's activities with respect to United States persons that are conducted pursuant to this paragraph.[10]

This effectively means that the government is currently conducting oversight of itself regarding the searching of US persons' personal electronic communications captured through its UPSTREAM programs, rather than placing this onerous responsibility on the judicial branch. Thus, the system of checks and balances established by the US Constitution on the power of the executive branch of government is being circumvented for "national security" purposes. In addition, UPSTREAM programs such as MUSCULAR are, in the first place, collecting voluminous streams of information containing the communications of US persons without any judicial oversight whatsoever—since these collections are made on foreign soil outside FISA jurisdiction.

According to the 2011 NSA minimization standards, for 702 collections that contain "multiple discrete communications" (also known as "Multiple Communication Transactions [MCTs]"[11]), NSA analysts who want to use a certain communication within the set of internet communications for 702 targeting or other purposes,

> will assess whether the discrete communication: 1) is a communication as to which the sender and all intended recipients are located in the United States; and 2) is to, from, or about a tasked selector, or otherwise contains foreign intelligence information.[12]

As such, the analyst is, in effect, charged with the responsibility of examining the personal communications of US persons that may coincidentally be bundled with another communication/s related to a "tasked selector". This means that the analyst will indeed examine US persons' personal communications (which may include content as well as metadata), and make a judgment that the juxtaposition is merely circumstantial and not relevant to an investigation, including a criminal

DOI: 10.1057/9781137408211.0005

investigation. At this juncture it may be edifying to ponder the language of the Fourth Amendment, which states that, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated". Yet, searches and seizures of the sort just described, which are done merely on the basis of happenstance would clearly qualify as "unreasonable" in any sense pertinent to the rights of US persons.

Further, with respect to 702 collections, the 2011 NSA minimization procedures stipulate that it can retain the communications of or related to US persons that have been "inadvertently acquired" for up to five years after the certification authorizing the collection expires; and that its personnel will "exercise reasonable judgment" in determining whether such information must be minimized and will destroy it at "the earliest practicable point in the processing cycle at which such communication can be identified either: as clearly not relevant to the authorized purpose of the acquisition . . . or, as not containing evidence of a crime which may be disseminated under these procedures". However, it is not clear why (or how) such a massive amount of data could ever be identified "as clearly not relevant to the authorized purpose of the acquisition" since it was "inadvertently acquired" in the first place. Moreover, the vagueness of the language ("the earliest practicable point in the processing cycle") is tantamount to giving the NSA carte blanch to retain such "inadvertently acquired" information of US persons for the maximum allowable time "just in case" it subsequently turns out to be relevant. But, pursuant to the Fourth Amendment, searches and seizures are only supposed to be conducted based on *probable cause*. "Inadvertently acquired" personal information is, ipso facto, not acquired based on probable cause. And, in the very least, searches and seizures, pursuant to the Fourth Amendment, are not supposed to be conducted *prior to* having probable cause in the unlikely event that such evidence is later discovered.

Other pertinent law besides Section 702 of the FISA Amendments Act also appears to be problematic. In particular, Section 215 of the US Patriot Act, which amended the 1978 FISA, permits the Director of the Federal Bureau of Investigations or a designee to make an application to the FIS Court for an order

> requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person . . . provided that such

DOI: 10.1057/9781137408211.0005

> investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.[13]

For example, Section 215 was, in fact, used by the Obama administration to get a FIS Court order to collect billions of phone records from Verizon customers.[14] Presumably, the George W. Bush administration's bulk collect of telephone metadata that was authorized by the FIS Court in May 2006 was also authorized according to the same provision. In the latter case, the Court found that "contrary to the government's repeated assurances," it had been "running queries of the metadata using querying terms that did not meet the required standard for querying".[15] This is hardly surprising since it is difficult to see how the collection of such a massive amount of phone records of US persons could even be *relevant* to a specific investigation. Instead, such an order amounted to a blanket warrant to examine the phone records of every US person. This means that, under current law, no US person is protected by the Fourth Amendment, which, again, requires that warrants be issued based on probable cause. In the current system, it is instead the case that we are all suspect, and only after the NSA's "reasonable judgment" that the communications of US persons that have been "inadvertently acquired" are not relevant to "the authorized purpose of the acquisition" (whatever exactly that may mean for such a massive data sweep) or to a crime, can they be adjudged not guilty.

Further, the FIS Court itself has been complicit in the Fourth Amendment abridgment. As confirmed by the FIS Court in its 2011 ruling, the Court itself has given the green light to the NSA to utilize its UPSTREAM programs to capture tens of thousands of electronic communications of wholly domestic communications and tens of thousands more of non-targeted individuals having no significant relationship to targeted individuals. Instead of prohibiting such collections, the Court has focused instead on "minimizing" the misuse of the information *after* it is collected. The Court so ruled because it merely accepted the claim that the technology was inherently incapable of *not* capturing so many unauthorized communications. It states,

> Given that NSA's upstream collection devices lack the capacity to detect wholly domestic communications at the time an Internet transaction is acquired, the Court is inexorably led to the conclusion that the targeting procedures are "reasonably designed" to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.

DOI: 10.1057/9781137408211.0005

> This is true despite the fact that NSA knows with certainty that the upstream collection, viewed as a whole, results in the acquisition of wholly domestic communications.[16]

However, the Court's argument is a non-sequitur. Because the present technology lacks the capacity to filter out wholly domestic communications, it does not follow that the NSA's targeting procedures are "reasonably designed" to prevent intentional acquisition of such communications. This conclusion does not follow because the government has intentionally chosen not to build necessary safeguards into existing technologies. The Court seems to be assuming that it has done a reasonable job in designing targeting procedures *given* that the present technology is inherently incapable of avoiding such unauthorized collections. *Here, however, the Court has allowed the technology to drive the legal determination rather than conversely.* Indeed, instead of raising the question as to whether there was a technological solution, it simply accepted the claim that there was no possible way of minimizing the unauthorized collections in the first place. On the part of government, the real issue for not addressing privacy concerns may have been reticence to appropriate the money to do the research and development to fix the problem. Or, it may have been driven to collect as much information as possible just in case a US person was complicit. In any event, the failure to address privacy concerns was not likely due to an inability to develop the technology to more efficiently protect the privacy of US persons—or that of foreign persons too. For example, it would be possible to "design" a filter that would work "reasonably" well to automatically filter out wholly domestic electronic communications. In the case of phone messages, calling codes for phone numbers (1 for the United States) could be used to identify calls placed to and from persons in the US. In the case of internet communications (email exchanges, chats, etc.), the IP address of the person could be used to identify the location of the person within the US. When the "to" and "from" fields are both identified as within the US, the filter could be configured to delete the communication. As such, wholly domestic electronic communications would not show up in multiple discrete transactions.

Such technological safeguards could support and provide reasonable assurance that privacy protections that are already legally required would be enforced. Thus, pursuant to Section 702 of the 2008 FISA Amendments Act, an acquisition to acquire foreign intelligence, "may not intentionally acquire any communication as to which the sender and all

DOI: 10.1057/9781137408211.0005

intended recipients are known at the time of the acquisition to be located in the United States…". Since storing implies acquisition, it is currently illegal to save wholly domestic communications on a government server let alone parse through them looking for foreign intelligence or criminal activity. Thus, even according to the amended FISA (not to mention the Fourth Amendment), the NSA is currently illegally collecting such domestic traffic. Development and deployment of an appliance to filter out and prevent acquisition and storage of wholly domestic electronic communication is therefore necessary if the NSA is to be compliant with existing law.

The Defense Advanced Research Projects Agency privacy appliance

However, the privacy of electronic communications, once "seized" (or "acquired"), also needs to be legally protected against "unreasonable searches" pursuant to the Fourth Amendment. One possible "privacy appliance" with the potential to address this constitutional requirement was actually being developed in 2002 by the Defense Advanced Research Projects Agency (DARPA), a research and development arm of the US Defense Department, but it appears to have been defunded by Congress in 2003. The technology was originally conceived by former Regan National Security Advisor, John Poindexter. At a 2002 DARPA conference in Anaheim, California, Poindexter described an automated process that would conceal identifying information, such as names and addresses from those having access to the masses of collected data. If a pattern matching search matches a pattern of data evidencing an impending terrorist attack, authorization could be sought to release the specific identifying information related to the given data pattern. The appliance would also have left an electronic trail of any unauthorized attempt to gain access to the stored identifying information.

According to Poindexter and Popp,

> Our privacy appliance concept involves the use of a separate tamper-resistant, cryptographically protected device placed on top of databases. The appliance would be a trusted, guarded interface between the user and the database analogous to a firewall, smart proxy, or a Web accelerator. It would implement several privacy functions and accounting policies to enforce access rules established between the database owner and the user. It would also

DOI: 10.1057/9781137408211.0005

> explicitly publish the details of its technology, verify the user's access permissions and credentials (packaged with the query in terms of specific legal and policy authorities), and filter out queries not permitted or that illegally violate privacy. Finally, it would create an immutable audit log that captures the user's activity and transmits it to an appropriate trusted third-party oversight authority to ensure that abuses are detected, stopped, and reported. (Granted, our privacy appliance concept assumes the third party is trusted, which is often the hardest problem to solve.) The privacy appliance's operation must be automated to respond to the dynamic, time-sensitive nature and scale of the problem and to ensure the privacy policy's implementation.[17]

As conceived, this appliance would "anonymize" the data by substituting generalized or obfuscated data replacements (e.g., a first name instead of first and last name) and would selectively reveal identities depending on how strong the case was for releasing the information.

However, there is a difference between anonymous data and de-identified data. In de-identified data, all explicit references to identifying data such as name, address, social security numbers, and telephone number, are removed, generalized, or replaced with a made-up alternative. The process of de-identification does not guarantee anonymity because it is possible, through the use of data linking with other data bases and information sources, to re-identify a de-identified individual. Thus, scrubbing an email or an attachment of identifying information such as names and addresses would not foreclose the possibility of re-identifying a scrubbed individual. For example, the author of a de-identified email might have written about a subject (for example, scientific data or insider information for a certain organization) that only a small subset of individuals could even know, and then the other possible individuals (if any) could be eliminated through further queries. In the case of data that contains fields such as phone metadata (addresses, call times, etc.), it is possible to link this information with other databases such as reverse phone number databases to find out the name of a queried individual.

One way to increase the level of anonymity is to generalize, remove, or replace the information in metadata fields in such a way as to attain a specific bin number, that is, a certain number of individuals in each field with matching data. Inasmuch as the higher the bin number the greater the anonymity, the level of anonymity (probability ratio) can be controlled. Programs can also control the amount of information that is disclosed to any given analyst based on the profile of the analyst. As a further safeguard, on the assumption that the anonymity of the data is

DOI: 10.1057/9781137408211.0005

"in the eye of the beholder," each analyst with access to the system would thus have a file that stores the profile information, which regulates the data returned by the system.

As such, there does not appear to be any absolute assurance of anonymity consistent with a useful database. Instead, the goal of anonymity (wherein the person cannot be re-identified) appears to be a matter of probability. Thus, techniques need to be built into the technology making highly probable a high degree of anonymity. Such techniques include creating and utilizing algorithms that adjust (remove, replace, generalize) metadata in data fields and content of communications consistent with maximizing anonymity within a functional foreign intelligence gathering system.

While the idea of such a filter, situated between the NSA analyst and its database containing masses of personal information, could potentially preserve a substantial amount of privacy, it could also be used as a way of merely pacifying public concern over privacy violations unless the technology were designed, configured, and operated in a manner that truly protected privacy. As Poindexter and Popp concede, there would ultimately need to be a trusted third party to oversee that the privacy filter was not abused. However, such a trusted third party would need to be an independent authority, not the Attorney General who is part of the President's cabinet and/or the National Director of Intelligence who serves under the President. Since such oversight would require a legal authority, this authority would properly be vested in the judiciary. The FIS Court would be an obvious candidate, but it would need to overcome its appearance of having served as a rubber stamp for government.[18]

Recall that, in 2008 the FIS Court "effectively impose[d] a wholesale bar on queries using United States-Person identifiers". However, also recall that, notwithstanding, in 2011 the government gave itself permission "to query the vast majority of its Section 702 collection" using US persons as identifiers. Such policy creep—toward increased abridgement of privacy rights of US persons (as well as non-US persons)—would need to be prevented through technological means. Thus, the use of US persons as identifiers might be rejected by the technology itself. When a query was made using a US person's name or other "strong selector," the system could check the selector against a list of protected selectors and when a match was found, it could reject the query as unauthorized. Such automated rejection of unauthorized queries could help to ensure that such queries were not successfully executed and only later caught

DOI: 10.1057/9781137408211.0005

(if at all) by searching for policy violations in an "audit log" such as the one proposed by Poindexter. In cases where the use of US persons was authorized by a court warrant based on probable cause, a permission code to override the protected selectors could be provided to an approved NSA analyst.

Three levels of privacy safeguards

As such, instead of accepting the claim that the NSA's minimization procedures were "reasonably designed" to prevent intentional acquisition of the data of persons within the US, the FIS Court could have found the current state of technology lacking in appropriate privacy safeguards. Indeed, it could have stood its ground against the pressure of government to expand its surveillance arm beyond that legally permitted. Pursuant to the Fourth Amendment, the following three levels of privacy protection appear to be technologically feasible, and should be required:

1. Acquisitions should be limited to communications that are not wholly between persons inside the US pursuant to the 2008 FISA Amendments Act. Filters should be added to all data collection systems of the MWSN, including all UPSTREAM programs and domestic, bulk, metadata phone programs, which are configured to filter out without saving all such wholly domestic transactions.
2. A de-identification privacy filter should be placed between the search engines of the MWSN and all of its databases. The filter should remove, generalize, or replace personal identifiers in the metadata and content of all electronic communications of persons located inside the US, or US persons outside the US, when a pattern matching search is conducted. The filter should provide maximum anonymity consistent with a functional foreign intelligence gathering system. A court warrant based on probable cause pursuant to the Fourth Amendment should be required to access the personal identifiers in the electronic communications of US persons and persons residing in the US at the time of the communication. To guard against tampering, the technology should also generate an "audit log" that is checked periodically by an independent judiciary authority.

DOI: 10.1057/9781137408211.0005

3 The MWSN including all UPSTREAM and PRISM programs should automatically reject strong selector searches of all electronic communications from all persons inside the US. Such a search concerning persons inside the US would require a court warrant, based on probable cause pursuant to the Fourth Amendment, before the system could authorize the search.
4 The FIS Court can play an important role in overseeing that the aforementioned privacy safeguards are satisfactorily implemented. For instance, Section 702 of the 2008 FISA Amendments Act requires that the Attorney General and the Director of National Intelligence seek approval from the FIS Court that appropriate minimization standards are in place. This can include documentation to show precisely how content filters, including de-identification filters, have been configured to assure that US persons and persons inside the US cannot be targeted without a court order.

Such a role is paramount to any effective use of meta-technologies to safeguard privacy. However, the establishing of a system of checks on the FIS Court itself is crucial to provide a level of assurance to the public that the Court is doing its job. Some efforts have already been made to establish some assistance to the FIS Court in reaching its decisions. For example, the so-called "USA Freedom Act" (HR 3361) passed by the House in 2014 provides that the presiding judges of the FIS courts (the FIS Court and the FIS Court of Review) appoint at least five individuals "who possess expertise in privacy and civil liberties, intelligence collection, telecommunications, or any other area that may lend legal or technical expertise to the courts…".[19] This is a step in the right direction, however, such a provision falls short of providing the assurance needed that the FIS Court is doing its job to protect privacy in cyberspace. Indeed, the fact that the members of the committee are appointed by the very court for which they serve raises issues about a real or apparent conflict of interest. Further, the appointed individuals serve as amicus curiae to the Court. This means that, although they may serve as valuable resources, they lack any oversight authority. Thus, the Court can easily, even if tactfully, pay lip service to the counsel of the committee. Therefore, what is needed is real oversight by an external, independent set of experts. These individuals could be appointed by Congress (instead of the FIS courts themselves) and have the authority to notify Congress if these courts

DOI: 10.1057/9781137408211.0005

fail to adequately fulfil the role of safeguarding privacy in cyberspace. In contrast to the committee created by HR 3361, such a committee would have "teeth" and its counsel would therefore be taken seriously.

Indeed, establishing adequate legal protections of privacy and appropriate judicial oversight is crucial. This chapter has provided some guidelines toward these goals. However, such protections and oversight become all the more urgent when it is seen that the primary technologies that are legally regulated are themselves seriously flawed, prone to produce hundreds of thousands of false positives, and are presently being used in ways that are unconstitutional and/or highly unethical. These problems of network applications are addressed in the next chapter.

Notes

1 See Chapter 1.
2 U.S. Code 50 (1978) Section 1802(a)1(B)-(C). http://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf.
3 Ibid., Section 101(a).
4 U.S. Code 50 (1978), Section 1801(h)(1).
5 S. 1927, Protect America Act, Sec. 105(A) Retrieved on June 18, 2014 from https://www.govtrack.us/congress/bills/110/s1927/text.
6 Electronic service providers do have the option of challenging a government order by going before the secret FIS Court, but the Court will grant the petition "only if the judge finds that the directive does not meet the requirements of this section, or is otherwise unlawful". HR 6304, Sec. 702 (h)(4)(C). Retrieved on June 18, 2014 from https://www.govtrack.us/congress/bills/110/hr6304/text.
7 HR5949, FISA Amendments Act Reauthorization Act of 2012, Section 2(a)(1). Retrieved on June 18, 2014 from http://www.fas.org/sgp/crs/intel/R42725.pdf.
8 US FIS Court, Memorandum Opinion, April 22, 2011. Retrieved on June 18, 2014 from https://archive.org/stream/775440-fisc-opinion-unconstitutional-surveillance-0/775440-fisc-opinion-unconstitutional-surveillance-0_djvu.txt.
9 "Identification of a United States person means (1) the name, unique title, or address of a United States person; or (2) other personal identifiers of a United States person when appearing in the context of activities conducted by that person or activities conducted by others that are related to that person." National Security Agency, *Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information pursuant to Section 702 of the Foreign Intelligence Surveillance Act as Amended*, October

DOI: 10.1057/9781137408211.0005

31, 2011. Retrieved on June 18, 2014 from https://www.aclu.org/files/assets/minimization_procedures_used_by_nsa_in_connection_with_fisa_sect_702.pdf.

10 Ibid.

11 See Chapter 1.

12 NSA, *Procedures Used By the National Security Agency*.

13 Section 15, US Patriot Act, U.S. Code 50 (2010), Section 1861. Retrieved on June 18, 2014 from http://www.law.cornell.edu/uscode/text/50/1861.

14 Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian*, June 5, 2013. Retrieved on June 18, 2014 from http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

15 U.S. FIS Court, Memorandum Opinion, April 22, 2011, p. 215, note 14.

16 U.S. FIS Court, Memorandum Opinion, April 22, 2011, p. 48.

17 John Poindexter & Robert Popp, "Countering Terrorism through Information and Privacy Protection Technologies," *Security and Privacy*, November/December 2006 (vol. 4 no. 6), pp. 18–27.

18 Dina Temple-Raston, "FISA Court Appears To Be Rubber Stamp For Government Requests," NPR, June 13, 2013. Retrieved on June 18, 2014 from http://www.npr.org/2013/06/13/191226106/fisa-court-appears-to-be-rubberstamp-for-government-requests.

19 HR 3361, Section 401(i)(2). Retrieved on June 18, 2014 from http://www.gpo.gov/fdsys/pkg/BILLS-113hr3361eh/pdf/BILLS-113hr3361eh.pdf.

DOI: 10.1057/9781137408211.0005

3
Network Searches and Applications

Abstract: *This chapter discusses problems inherent in the technologies themselves, such as their tendency to produce false positives, and it assesses the efficiency of various subprograms such as Section 702 (FISA) investigations and Section 215 (Patriot Act) investigations. It discusses conventional investigations and shows the relationship between these and available high-tech solutions. It also examines Section 702 programs operating without judicial oversight, such as MUSCULAR and INCENSOR. In addition, it examines lesser-known ways in which the NSA surveillance program is tapping into popular devices to sweep up personal information, such as smartphone applications, missed calls and contact lists, electronic business cards, chats, credit card transactions, and text messaging. Finally, it examines subprograms that transcend the original purposes of the system to prevent terrorism.*

Cohen, Elliot D. *Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.* New York: Palgrave Macmillan, 2014. DOI: 10.1057/9781137408211.0006.

The public perception of the NSA surveillance program, the one promulgated by government, has largely been that of a set of protocol fined tuned to the task of preventing terrorist attacks. However, less is known about the true nature of NSA data searches, their limitations, faults of the technology, and the comparative value of less high-tech investigative techniques. And while programs such as PRISM have received considerable press, other UPSTREAM programs, such as MUSCULAR and INCENSOR, which lack judicial oversight, have received much less attention. Nor is there common awareness of some of the ways the MWSN is being used to tap into popular technologies to collect personal information, for example, smartphone applications, call data logs, text messaging, internet chats, electronic business cards, and credit card transactions. This chapter will address these shortcomings and questionable applications.

The question of how efficient the MWSN is, or how well its technologies work, can be understood in terms of how accurate it is, which, in this context, means what percentage of the time it correctly identifies someone as a terrorist. However, for every such "true positive" the system returns, there can also be a vast number of "false positives," that is, numerous cases of falsely identifying someone as a terrorist. This is the problem of false positives and it permeates the entire MWSN. One salient instance of the problem is the use of pattern matching searches with UPSTREAM programs to identify terrorists.

Pattern matching searches

This particular type of search involves construction of algorithms that search for behavior patterns associated with a specific target group. In commercial advertising, this involves creating a profile of prospective consumers who are most likely to be interested in a product that is being marketed. For example, a magazine about hunting would attempt to target a demographic population that would most likely be interested in going hunting. Thus, according to a 2011 report of the Fishing and Wildlife Service, the most likely hunter would be white males between the ages of 55 and 64, living in rural regions of the southeast, with incomes between $50,000 and $100,000.[1] Given that, only 5.7 percent of the US population hunt, targeting this group would make it more likely to reach prospective subscribers. But even so, such bulk behavioral advertising tends to have

DOI: 10.1057/9781137408211.0006

a relatively low, single digit positive response rate. This means that the false positives range in the 90 percent range. However, it is not as easy to create a demographic of prospective terrorists as it is of prospective hunters. Indeed, in contrast to individuals who go hunting, there have been relatively few terrorist attacks on the US that enable construction of a terrorist demographic. Consequently, the pattern searches for prospective terrorists typically take an indirect approach. This involves looking for anomalous internet communication patterns, that is, cyber behavior that does not match the cyber behavior of average internet users, for example, atypical internet searches, sites visits, email exchanges, and credit card purchases. Unfortunately, the assumption that an unusual set of behaviors makes one a prospective terrorist is a questionable assumption, which has not been proven by the success of the MWSN to stop terrorist attacks.[2] On the contrary, it appears that conventional means of investigating possible terrorist attacks such as the use of informants, community tips, routine law enforcement, suspicious activity reports, and other non-NSA intelligence have been the most fruitful means of preventing such attacks.

Conventional investigations

According to a report prepared by the New American Foundation, a non-profit, non-partisan, public policy institute, the majority of the terrorism cases that occurred after September 11, 2001, have been identified by these more conventional modes of investigation, and the contributions made by the NSA's MWSN toward identifying terrorist plots before they happen have been "minimal". Further, the report states, "our review of the government's claims about the role that NSA 'bulk' surveillance of phone and email communications records has had in keeping the United States safe from terrorism shows that these claims are overblown and even misleading."[3] Based on its investigation of 225 individuals charged in the US with terrorism since September 11, 2001, the report concluded that the NSA's bulk telephone metadata program, operating pursuant to Section 215 of the US Patriot Act, played an identifiable role in initiating no more than 1.8 percent of such cases; and its other surveillance programs operating pursuant to Section 702 of the FISA Amendments Act, played some role in only 4.8 percent of these cases. According to the report, 60 percent of the cases were initiated by conventional

DOI: 10.1057/9781137408211.0006

investigative methods such as undercover informants, family member tips, traditional law enforcement methods, or CIA or FBI intelligence. In 5 percent of the cases, a violent incident preceded prevention, and in 28 percent of the cases the methods used to initiate the investigation could not be determined from available court or public records.[4]

Section 702 investigations

The report does not mention the millions of false positives that were probably generated by using the MWSN in order to identify (or help to identify) the relatively small number of true positives the government attributes to this bulk surveillance network. Consider just the Section 702 investigations, which are supposed to target only non-US persons outside of the US. In order to identify the said 4.8 percent of the 225 terrorists that is 11 terrorists), the system had to search through a database containing the documents of millions of non-terrorists. According to the FIS Court, the "NSA acquires more than two hundred fifty million Internet communications each year pursuant to Section 702."[5] Since the minimization standards used by the NSA permits records to be kept up to five years,[6] it is not unreasonable to suppose that the Section 702 database has considerably more than 250 million records in the years 2009 through 2012, which is the span of time in which the cases used by the government to justify its Section 702 program occurred.[7] So it is safe to assume that it has had *at least* 250 million communications at any time during this period. According to the New American Foundation report, there were 12 plots that were "not prevented prior to incident".[8] Five of these plots involved six non-US persons who would have been subject to Section 702 surveillance. The remaining plots appear to have involved "homegrown" terrorist attacks, which excludes them from Section 702 pursuant to the 2008 FISA Amendments Act. This suggests 17 true terrorists (11 + 6) that Section 702 surveillance programs might have identified. Since the US government has claimed that these programs identified 11 of the 17 terrorists, it will be assumed here that they had an accuracy rate of 65 percent (and therefore an inaccuracy rate of 35 percent).[9] Thus, there were presumably 17 true terrorists in the Section 702 databases, six of which the filters did not catch. This, in turn, means the system must have generated at least 87,500,000 false positives (250 million minus the 17 true terrorists, multiplied by 35 percent).[10] This means that at least

DOI: 10.1057/9781137408211.0006

87,500,000 people (including US and non-US persons) were falsely identified as terrorists. To be clear, this estimate has been constructed from data that may be incomplete, so it is an estimate only, although a modest one.[11] Given the extremely high rate of false positives, the results generated by the MWSN cannot be regarded as actionable intelligence.

In fact, the at least 87,500,000 false positives (plus the 11 true positives) have all presented as veridical, leaving it to the analysts to sort out the false positives from the 11 true positives. Finding this proverbially needle in a haystack requires more data. Inasmuch as the MWSN has played some role in identifying only 7 percent of the 225 terrorists identified since September 11, 2001, it is reasonable to think that it was more conventional methods of investigation that helped to screen out these needles from the haystack. That is, the conventional methods such as using informants, community tips, routine law enforcement, suspicious activity reports, and following up on other non-NSA outside leads are likely what direct attention to specific "positives" returned by the MWSN.

An example is the 2009 foiled plot by Najibullah Zazi and two co-conspirators to bomb the New York City subway system.[12] While the government has claimed the case as an NSA bulk surveillance success, conventional means of investigation supported the use of bulk surveillance. Allegedly, the case was initiated by British intelligence, which used a conventional targeted investigation to obtain an email address of an al-Qaeda operative in Pakistan with which Zazi was communicating. British intelligence, in turn, shared the address with US intelligence, which then chose to use this email address as a selector in the NSA Section 702 surveillance system to conduct warrantless surveillance of Zazi's email exchanges. Hence, it was due to a conventional investigation that the NSA was able, in the first place, to use the MWSN to thwart a potential terrorist plot. However, as the New American Foundation Report makes clear, US intelligence could also have chosen to use conventional means of investigation such as an individual FISA or criminal warrant to place Zazi's email exchanges under surveillance.[13]

There is an old computer adage that appears to be relevant in this context, namely, "Junk in, junk out". That is, ordinarily, to construct an intelligent inquiry, information is needed, which is typically gleaned from sources outside the MWSN. Algorithms used to look for terrorist plots are not much help because they produce too many false positives. Useful queries are more often driven by metadata such as phone

DOI: 10.1057/9781137408211.0006

numbers, e-mail addresses, names, and other "strong selectors". But in order to know what specific metadata to enter, an analyst must already have some outside leads. So, in order for the MSNW to be of any genuine use as an adjunct in terrorism investigations, more conventional investigative means need ordinarily to be employed first. Otherwise, in conducting pattern matching searches based on anomalous behavior patterns encapsulated in complex algorithms, analysts are inundated with false positives and are left without a reliable way of distinguishing the true from the false positives.

The point can be put in terms of a dilemma. Either the NSA's Section 702 programs (as well as other mass warrantless programs) rely on conventional investigative means or they do not. If they do rely on such conventional means, then these programs are not necessary in the first place (as the Zazi case suggests) to identify terrorists. On the other hand, if they don't rely on such conventional means, then they lead to an unmanageable amount of false positives, making it virtually impossible to identify the true positives. Therefore, either these programs are not necessary in the first place (because conventional means can be used instead) or they are not useful in identifying terrorists (because they are inundated with millions of false positives). In either case, it may be argued, relying on such bulk mass, warrantless programs have little or no value to offset the violations of privacy they produce. So what value, if any does the MWSN have?

Clearly the MWSN is capable of using "strong selectors" to find corroborative evidence *after* a conventional investigation turns up some data that may be used as selectors. This is not an indispensible use because conventional means could also be used, as the Zazi case suggests. Nevertheless, having such a massive system of data along with its search engines on hand still may be more expedient in the sense that it is likely to be faster than going forward using conventional investigative means. The question of justifying the existence and use of such technology is whether the expedience of gaining access to information quicker is worth the investment of billions of dollars and the cost to human privacy. The affirmative response is that time is of the essence when it comes to the possibility of thwarting potential terrorist attacks. But this does not preclude requiring that the Attorney General or his or her designee go before the FIS Court with the preliminary data gleaned from conventional investigative means to get a warrant to search this system when the names, email addresses, phone numbers or other metadata of

DOI: 10.1057/9781137408211.0006

US persons is being used in the search.[14] If an emergency exists, then the petitioner can always file the authorization within 24 hours of implementing the search pursuant to the 1978 FISA or within seven days according to the 2008 FISA Amendments Act. Here lies the strong argument for requiring search warrants based on probable cause pursuant to the Fourth Amendment before the massive data system can be searched. If the system is useful only if strong indicators are used, then standard search warrants can still be used, thus assuring judicial oversight without defeating any useful function of the system.

Patriot Act, Section 215 investigations

The NSA's Patriot Act, Section 215 metadata phone surveillance program appears to have had even less success than its Section 702 programs, and, at the time of this writing is under revision.[15] According to the New American Foundation report, "Surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group."[16] Allegedly, the single case the government has produced to justify the program, the case of Basaaly Saeed Moalin, raises some questions about the necessity of the program. Moalin was convicted, in 2013, along with three co-conspirators, of conspiring to provide material support in the amount of $8,500 to a foreign terrorist organization, namely al-Qaeda. However, in 2003, Moalin had been suspected of being associated with terrorists, but no connections were then found and the case was closed. Since, the domestic bulk metadata phone program was operative in 2003, it is unclear why the system was unable to show any terrorist links at that juncture. Yet in 2007, the government claims to have connected a number in Somalia linked to Aden Hashi Ayrow, an al-Qaeda operative in Mogadishu, Somalia, to Moalin's phone number in the US. (Ayrow had unsuccessfully attempted to call Maolin.) However, it seems clear that, (1) the government already had Ayrow's phone number and knew that he was an al-Qaeda operative, and (2) the government already had suspected Moalin of terrorist links (in 2003). As such, one reasonable hypothesis is that Ayrow's phone number was used as a strong selector in the Section 215 system, which linked it to Moalin's phone number, which was, in turn, cross referenced with a database including Moalin's name.

DOI: 10.1057/9781137408211.0006

If so, then the investigation into Moalin was initiated through the use of information most likely gained through more conventional means. This is not to say that the Section 215 program did not play a role in uncovering Moalin's activity of supporting a terrorist organization; but, on the present hypothesis, it would be disingenuous to give the program full credit as though the technology successfully replaced the need for conventional investigations in the first place.

Further, after receiving Moalin's phone number from the NSA, the FBI waited two months before it began to wiretap Moalin's phone calls. But as the New American Foundation report explains, this destroys the credibility of the government's claim that the Section 215 program is necessary to expedite the investigative process, since "it clearly didn't expedite the process in the single case the government uses to extol its virtues".[17] Assuming what is contrary to fact, that the program might have been used in the Moalin case to expedite the investigative process, the fact that it was not so used, suggests that this case was not viewed by the government as being high priority at the time. Thus, its later use as the poster child of the NSA's domestic bulk metadata phone surveillance system is rather curious indeed.

Perhaps the utility of the Section 215 system in the case in question was in pinpointing the location of Ayrow through the call he placed to Moalin. According to one FBI email, this permitted the government to use a drone to target and kill him.[18] However, this value does not justify the amassing of telephone metadata of calls that are *wholly* domestic. That is, the call in question (made to Moalin from Ayrow) was not a wholly domestic call since it was placed from Somalia to the US. This raises serious questions about why this case could even justify the surveillance of *all wholly domestic calls*. As discussed in Chapter 2, such calls can (and should) be filtered out to avoid abridgment of Fourth Amendment rights. Including wholly domestic phone records in the NSA bulk phone metadata database is not only unnecessary, it is also unlawful pursuant to both the 2008 FISA Amendments Act, which is supposed to target only non-US persons outside the US, and the Fourth Amendment, which requires a search warrant based on probable cause. Further, the fact that, even as an adjunct to conventional investigative means, this program has such an unimpressive past track record, makes this breach of a legally protected right of US persons "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" that much more salient—and inexcusable.

DOI: 10.1057/9781137408211.0006

This clear appearance of being needless invasion of the privacy of US persons explains why the Obama administration has decided to revise the Section 215 program. Currently, the US House of Representatives (HR3361) has passed the "USA Freedom Act,"[19] which revises the domestic bulk metadata program by having the telephone companies collect masses of phone metadata, and then permits the government to get a court order to query data utilizing a "specific selection term". According to the proposed legislation, the latter term is defined as

> a discrete term, *such as* a term specifically identifying a person, entity, account, address, or device, used by the Government to *limit the scope* of the information or tangible things sought pursuant to the statute authorizing the provision of such information or tangible things to the Government (emphasis added).[20]

A positive aspect of the proposed law is that it places a level of judicial protection between the collection data and the NSA by requiring a FIS Court order. However, the devil is in the detail and a clear problem lies in the definition of "specific selection term". The words "such as" placed before "a discrete term" means that a specific selection term may be, but need not be, limited to a specific person, entity, account, address, or device. In fact, according to the given definition, the term can be *anything* that "limits the scope" of the information sought. Unfortunately, with such a vague definition, a query could be about virtually anything, since all terms have boundaries or scopes. For example the term "US person" does not include everyone who is not a US person. Thus, this provision is consistent with bulk acquisition of domestic telephone metadata by government.

As such, HR 3361 appears to do little to remediate the problematic nature of Section 15 investigations. The program was largely inefficacious to begin with, and by legalistically leaving it open for government to acquire mass quantities of telephone metadata from telephone companies, it gives only any appearance of doing away with this ineffective program. More transparently, the government should have admitted that the program was effective and unequivocally discontinued it.

In fact, in early 2012, the Obama Justice Department acted on a subpoena to secretly obtained two months of telephone metadata from telephone lines assigned to the Associated Press (AP) and its journalists, including an AP general phone number in New York City, and AP bureaus in New York City, Washington, D.C., Hartford, Connecticut, and

DOI: 10.1057/9781137408211.0006

at the House of Representatives. These records also included records from AP journalists' homes. Indeed, such a broad-based collection of press records, regardless of whether or not they were relevant to an ongoing investigation, was an egregious violation of the First Amendment protection of the press's freedom to gather and report the news.[21] Government collection of such metadata could impede the AP's ability to gather the news by exposing its sources; for without assurance that one's identity would be kept confidential, potential sources would not venture to speak candidly to the press.

Now, had the same AP records been acquired by the NSA rather than the Justice Department under a broad-based FIS court search warrant pursuant to a specific selection term as defined in HR3361, the violation of the First Amendment right to freedom of the press would be even more egregious. This is because the NSA would not have to disclose, in advance, and negotiate with the news organization the terms of the acquisition of phone records as is now required under the newly revised *Code of Federal Regulations*.[22] Thus, the vague limitations of HR3361 could well provide the government with a way around the stricter media privacy protections of the newly minted CFR rules.

"Back Door" UPSTREAM programs

As discussed in Chapter 1, there are also UPSTREAM programs such as MUSCULAR and INCENSOR, which are clearly not subject to objective scrutiny because they are clandestinely conducted without any judicial (or congressional) oversight and therefore leave no court or public records to assess. However, it is clear that these programs, which are jointly operated by the US and Great Britain, are regularly sweeping up and storing billions of electronic communications containing both US and non-US persons.[23] It would also appear that the technologies being used to search these records are the same technologies being used in the Section 702 programs, in particular, XKEYSCORE.[24] As such, there are likely also hundreds of millions of false positives being generated by these technologies with no judicial or congressional system of checks and balances to guard against usurpation of legally protected rights. This new "wild west" of surveillance calls for immediate attention by the US government. For if it is not addressed, not only will innocent people be targeted and placed on watch lists. Given the vast amount of individuals

DOI: 10.1057/9781137408211.0006

on the radar, it is likely to result in false arrests and prosecutions without any means of legal redress for those so subjected. As proposed in Chapter 2, such renegade programs need be brought under FISA and protected pursuant to the Fourth Amendment.

OPTIC NERVE

Unfortunately, the vast wingspan of the MWSN embraces other overseas UPSTREAM programs, which utilize technologies that raise special privacy concerns. One particularly Orwellian example is that of OPTIC NERVE, a program conducted by the GCHQ, which processes webcam data from the Yahoo chats of millions of users, including those of US persons.[25] The program, which allegedly began in 2008 (and was still active in 2012) processes still image of chatters every five minutes. Much of the data collected contains nude still pictures of Yahoo users, which therefore violates the privacy of users in a profoundly intimate sort of way. The NSA has not disclosed how much of this photographic data it has received, but it can be reasonably inferred that it has had relatively unfettered access to it.

What is known is that OPTIC NERVE uses NSA's XKEYSCORE as its data search and retrieval system, which is an international network of approximately 700 servers located at 150 locations throughout the world.[26] Since the program can process data at local caches for up to 30 days, it is likely that the NSA itself has had access to the Yahoo photo data acquired in Great Britain by GCHQ through OPTIC NERVE and XKEYSTROKE. According to Edward Snowden, by using the latter program, "any computer that an individual sits at you can watch it".[27] Likely, then, Snowden himself (and therefore tens of thousands of his NSA co-workers) had access to sexually explicit photos of Yahoo chatters when he worked for the NSA.

Allegedly, GCHQ analysts were able to search OPTIC NERVE using facial recognition software looking for persons resembling GCHQ targets. According to the Federal Bureau of Investigation's *System Requirements Document* governing its use of its "Next Generation Identification" (NGI) system in criminal investigations, "NGI shall return an incorrect candidate a maximum of 20% of the time, as a result of facial recognition search in support of photo investigation services."[28] This means that the facial recognition software utilized in the NGI system can give

DOI: 10.1057/9781137408211.0006

false positives 20 percent of the time. Assuming similar software was run through the MWSN to troll through millions of chat images looking for terrorist suspects, as much as 20 percent of the images returned could have been falsely matched to the targets under investigation.[29] For instance, in just one six-month period in 2008, the GCHQ collected still videos from 1.8 million Yahoo users, which, when scanned by facial recognition software, could have return as much as 360,000 false positives. Actionable intelligence cannot tolerate such a large false positive ratio; nor can respect for the rights of the innocent, who may be falsely targeted.

There also appears to be a racial bias built into facial recognition technology itself. According to one study, "white subjects are harder to recognize than Asian, African-American or other [Arab, Indian, Hispanic, mixed] subjects, even when the system is trained with racially balanced data sets."[30] As such, we could expect there to be more non-whites identified by facial recognition algorithms than whites. Thus, when metadata is added to a search, for example, the inclusion of a Middle Eastern name, non-whites (such as Arabs) are more likely to be identified than whites. All things being equal, this also means that there are likely to be more non-whites (Arabs, blacks, Hispanics, and mixed) *falsely* targeted. Programs such as OPTIC NERVE are therefore seriously in need of careful scrutiny pursuant to the Equal Protection Clause of the Fourteenth Amendment.

Other "unofficial" uses of the MWSN

When programs such as OPTIC NERVE and other invasive tentacles of the MWSN are used under the banner of stopping another 9–11 attack from happening, it may be easier to overlook at least some of the violations of civil liberties perpetrated in the name of "national security". However, when these programs are used for other purposes not clearly related to stopping prospective terrorist attacks, then this apparent vindication or tolerance for such a system of mass warrantless surveillance begins to lose its semblance of justification. Yet, the MWSN may actually be better suited for some of its current "unofficial" uses than it is for stopping prospective terrorist attacks. Unfortunately, at least some of these uses are legally as well as morally doubtful.

DOI: 10.1057/9781137408211.0006

Monitoring of confidential lawyer-client communications

One example with substantial constitutional implications is the case of surveillance involving collection of confidential communications between lawyers and their clients. As torrents of information, including that of US persons, are vacuumed up by the NSA, so too are confidential attorney-client electronic communications. Because the Sixth Amendment of the US Constitution provides a right to counsel in criminal cases, the NSA is supposed to protect information regarding those who are accused of a crime. However, given the secrecy under which the NSA operates and the lack of judicial oversight, this leaves little assurance that the information acquired through tapping into confidential emails and phone/fax messages between lawyers and their clients will not surreptitiously be used against these clients in order to prosecute them. In the case of clients who are not accused of any crime, there is no Sixth Amendment protection, and thus the NSA is not obligated to protect confidential communications between attorneys and their clients.[31]

Consequently, there has been a chilling of confidential communications between lawyers and their clients, especially overseas clients, and, in particular, clients allegedly involved in terrorism cases. Some lawyers have thus been reticent to take on terrorism cases because of government surveillance of otherwise confidential communications. Some lawyers have avoided the problem of governmental violation of confidentiality by flying long distances to have face-to-face meetings with their clients for matters that could have easily been addressed via email, phone, or fax. Some lawyers have admonished their clients about disclosing confidential information through electronic communications.[32]

The American Bar Association (ABA) has also amended Rule 1.6, "Confidentiality of Information," of its code of ethics to include a paragraph that states, "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[33] And in its comment on the rule, the ABA has provided some guidance for assessing whether or not an attorney has made reasonable efforts to avoid unauthorized access to the protected information. These factors include, but are not limited to, "the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards,

DOI: 10.1057/9781137408211.0006

and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)."[34] However, especially in cases of clients likely to be NSA targets, it is not clear how NSA surveillance could not significantly impair the lawyer's representation of the client by chilling the lines of electronic communication.

The problem is far from "speculative"[35] and has been documented. For example, in one case reported by *The New York Times*, communications involving trade talks between Mayer Brown, a Chicago law firm, and officials of the Government of Indonesia were monitored by the Australian Signals Directorate (Australia's analog of the NSA), and the information was shared with the NSA.[36] In this and other cases like it, where there are economic and/or political interests at stake but not ones involving terrorism, the usual justification for deploying the MWSN are not available. Nevertheless, the government has not exercised due constraint against so utilizing the system to gain "foreign intelligence". At least part of the problem may stem from the fact that the 1978 FISA included in its definition of "foreign intelligence information" information necessary to "the conduct of the foreign affairs of the United States".[37] Since trade agreements could have an effect on US foreign affairs, the confidential attorney-client communications about such matters could arguably fall within this province. However, the 1978 FISA also required that the acquisition of the contents of electronic communications be "exclusively between or among foreign powers"; moreover, there could be no "substantial likelihood" that the surveillance would acquire the contents of "any communication to which a United States person is a party". Unfortunately, the weakening of the language in the 2008 FISA Amendments Act to permit acquisitions as long as the target was a non-US person "reasonably believed" to be outside the US, can now be used to sidestep lawyer-client confidentiality, between a US law firm and a foreign client, in acquiring their confidential electronic communications. Pursuant to the 2008 FISA Amendments Act, even though the law firm may be located in the US, the NSA can still acquire its electronic communications with a foreign client "reasonably believed" to be outside the US.

The remedy to such violations of lawyer-client confidentiality is apparent, which is to make explicit in the FISA law the requirement that confidential lawyer-client information between a US law firm and a foreign or domestic client cannot be acquired pursuant to Section 702 of the 2008

DOI: 10.1057/9781137408211.0006

FISA Amendments Act. Instead, a court order would need to be issued to the law firm for the information to be produced, thereby assuring adequate judicial oversight when exceptions were made to privileged communication. This would be in concert with Rule 1.6 of the ABA *Model Rules of Professional Conduct*, which presently permits disclosure of privileged information pursuant to a court order. Such tightening up of FISA would also need to be technologically supported by surveillance filters to assure that the privileged electronic communications are not vacuumed up by the MWSN. One way of building in such a safeguard would be to maintain a registry of law firm email addresses and phone/fax numbers, which would be used as search criteria to filter out and pre-empt collection of privileged electronic communications between lawyers and their clients. Such a system of legal and technological safeguards is not optional if the US is to maintain a justice system that assures due process. The argument that it is more expedient for purposes of protecting against terrorist attacks to have immediate access to all electronic information, even those of lawyer-client communications, is spurious. If this argument were taken seriously, then we would never have instituted a system of checks and balances and legal processes that provide for due process (consider, for example, the Miranda Rule); for it is, in general, more expedient not to have such an elaborate system of protections. But this is the price we pay for a system that respects human dignity and adheres to the rule of law.

Spying on bank transactions and credit card transactions

The NSA's reach on personal information worldwide also extends to the collection of credit card transactions. It appears that the NSA has similar arrangements with credit card companies such as VISA and Master Card as it has with the telecommunication companies enabling it to access their international networks.[38] For example, it uses XKEYSCORE to "skim regional data" from the Visa network.[39] Another NSA program code named DISHFIRE sweeps up Short Message Service (SMS) text messages including information on financial transactions, travel plans, information about meetings, missed calls, and other personal information. According to an NSA presentation leaked by Edward Snowden, the program collects over 800,000 financial transactions each day through "text-to-text payments or linking credit cards to phone users" as well as over 110,000 names from electronic business cards.[40]

DOI: 10.1057/9781137408211.0006

The focus of the NSA's financial monitoring initiative appears to be on international banking, payment, and credit card transactions through a global program known as "Follow the Money" (FTM). Collections are routed to the NSA's own financial databank, code named "Tracfin," which contained 180 million records in 2011, 84 percent of which was from credit card transactions. The NSA intercepts international banking transactions processed through the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which provides a "secure" network used by more than 8,000 banks worldwide for sending and receiving bank transactions.[41]

Apparently, the NSA has also found ways to tap into global credit card networks such as that of VISA and MasterCard;[42] and while the alleged goal of NSA has been to "collect, parse, and ingest transactional data for priority credit card associations, focusing on priority geographic regions" (such as Europe, the Middle East and Africa),[43] this goal is compatible with NSA's acquiring millions of credit card transactions by US persons. Indeed, in a global economy, it is impossible to bifurcate the international from the national, especially since the routing of domestic transactions can occur through switches located anywhere in the world. In any event, the bulk collection of credit card information in order to try to find transaction made by terrorist suspects is beyond the pale of rationality. As previously explained in this chapter, productive searches of colossal databases ordinarily require entry of search terms that use information *already* acquired by conventional investigative methods. This suggests that collection of and sifting through torrents of irrelevant data may not even be necessary in the first place. Thus, wiring tapping the financial activity of a suspect already on NSA's radar might be more efficient while at the same time avoiding mass violation of privacy. Quite clearly, the charge of the government to justify such an intrusive system of financial data collection and analysis is to produce incontrovertible evidence showing that, whatever useful information this system has managed to acquire could not have also been collected through more conventional and less intrusive methods.

Cell phone acquisitions

Through ten different signal intelligence programs, including the one code named STORMBREW,[44] the NSA is collecting as much as five

DOI: 10.1057/9781137408211.0006

billion metadata records per day on the geographical locations of cell phones throughout the world.[45] This is possible because the data collected includes cell tower data typically from multiple cell towers (at least three), which permits relatively accurate calculation of location (within 100 feet) based on signal strength in proximity to each cell tower, and the time it takes for the signal from the cell to reach it.[46] Such mass location data collection is tantamount to tracking the whereabouts of everyone with a cell phone, which is most of us.

According to an anonymous senior collections manager of the NSA, "we are getting vast volumes" of location data from around the world by tapping into the cables that connect mobile networks globally and that serve US cell phones as well as foreign ones. "Additionally, data is often collected from the tens of millions of Americans who travel abroad with their cell phones every year."[47] The NSA utilizes analytics dubbed "Co-Traveler," which correlates the paths of unknown cell phone activity with known targets. Since the time and date a cell phone is located in a particular place can be determined from a cell phone just by virtue of its being turned on (the data includes cell tower designators), the NSA can check for intersecting patterns of activity and use this metadata in order to link prospective targets with known targets. Co-Traveler analytics can also calculate travel trajectory as well as travel speed. Disposable cell phones that turn on and off to make brief phone calls are flagged, and data showing a pattern of nearby devices powering off and on together can be used to determine associations between device users.[48]

Such data, however, establishes inductive (probabilistic) connections, which can be mistaken. Thus, a person and his or device might be "in the wrong place at the wrong time." This creates an irreducible risk factor. Moreover, inasmuch as no filters are currently being used to prevent the pairing of space-time coordinates of US persons (either traveling abroad or in the States) with known targets, there is risk of falsely linking US persons to potential terrorist plots or other criminal activities. These probabilities increase in proportion to the amount of location metadata of US persons collected. This danger increases substantially depending on the number of false positive possibilities divided by the number of total possibilities. However, these possibilities can be eliminated by using filters to filter out data generated by the devices of US persons. As discussed in Chapter 2, such phone data can be filtered out according to calling codes.

DOI: 10.1057/9781137408211.0006

Leaky app acquisitions

Smartphones, Blackberries, Voice over IP (VOIP), General Packet Radio Service (GPRS), and other mobile devices use applications that gather extensive amounts of personal user information. These applications, so called "leaky apps," are presently being exploited by the NSA and its British counterpart, the GCHQ, to acquire masses of personal data.[49] According to the NSA, such mobile devices have lead to "the gradual 'blurring' of telecommunications, computers, and the Internet," which has made them grist for targeting.[50] For example, the NSA describes "perfect target" as a user who takes a photo with his phone or other mobile device and uploads it to a social media sight such as Facebook. From this action, the NSA is able to collect large amounts of metadata including websites visited, buddy lists, documents downloaded, call logs, email addresses, unique identifiers, geographical locations, PIN numbers, and other personal data. According to the NSA, analysts should "make use of fingerprints in XKEYSCORE" by using its Exchangeable Image File Format (EXIF) metadata plug-in, which contains image metadata files such as photographs, presumably to select individuals for further targeting. Some "leaky" applications the NSA mentions include Visual Communicator (a free app integrating Instant Messaging, Photo-Messaging, and Push2Talk capabilities into a mobile platform), WinZip (popular compression and encryption program), Flixster (social networking site for sharing movie ratings, finding new movies and meeting others who share similar movie interests), Google Maps, and mobile Facebook apps for iPhone or Android.[51]

Clearly, such targeting operations encroach on personal privacy and treat the masses of ordinary US persons who use telecommunication devises (virtually all of us) as crime or terrorism suspects. As discussed, such mass targeting of US persons can classify millions of US persons as targets based on false positives. The collection of online and telephone activities of US persons must not be made in the first place if minimization standards of FISA are to be respected. Since mobile devices operating in the US and devices owned by US persons traveling outside the US are not supposed to be subject to foreign intelligence gathering, the mass data acquisitions being made by so-called "leaky apps" is arguably unlawful and should be discontinued.

However, there are some acquisitions of foreigners that are ethically questionable, even if not strictly speaking unlawful. In the next chapter,

DOI: 10.1057/9781137408211.0006

these cases will be considered and a system suggested that can create greater transparency in the global use of surveillance technology.

Notes

1 US Fishing and Wildlife Service, 2011 National Survey of Fishing, Hunting, and Wildlife-Associated Recreation. Retrieved on June 18, 2014 from http://www.census.gov/prod/2012pubs/fhw11-nat.pdf.

2 Jeff Jonas and Jim Harper, "Effective Counterterrorism and the Limited Role of Predictive Data Mining," *Policy Analysis*, Cato Institute, No. 584, December 11, 2006. Retrieved on June 18, 2014 from http://www.cato.org/sites/cato.org/files/pubs/pdf/pa584.pdf.

3 Peter Bergen, David Sterman, Emily Schneider, and Baily Cahall, "Do NSA's Bulk Surveillance Programs Stop Terrorists?" New America Foundation, January 2014. Retrieved on June 18, 2014 from http://www.newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1_0_0.pdf.

4 Ibid.

5 U.S. FIS Court, Memorandum Opinion, April 22, 2011. Retrieved on June 18, 2014 from https://archive.org/stream/775440-fisc-opinion-unconstitutional-surveillance-0/775440-fisc-opinion-unconstitutional-surveillance-0_djvu.txt.

6 National Security Agency, *Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information pursuant to Section 702 of the Foreign Intelligence Surveillance Act as Amended*, October 31, 2011, Section 3(c)(1). Retrieved on June 18, 2014 from https://www.aclu.org/files/assets/minimization_procedures_used_by_nsa_in_connection_with_fisa_sect_702.pdf.

7 Peter Bergen, et al, "NSA Analysis," New America Foundation. Retrieved on June 18, 2014 from http://natsec.newamerica.net/nsa/analysis.

8 Peter Bergen, et al., "Do NSA's Bulk Surveillance Programs Stop Terrorists?" New America Foundation, p. 5.

9 This accuracy rate estimate assumes that the NSA Section 702 bulk surveillance system initiated all 11 investigations of the identified terrorists; however, there are at least two cases in which the New American Foundation report alleges that conventional investigative means initiated the investigation and provided the selectors for the 702 search. These cases are the Zazi and Headley cases examined in the report. The Zazi case is discussed below. See also ibid., pp. 9–10.

10 This is an application of so-called "Baye's Theorem," which can be used to calculate the number of false positives likely to be generated by mass

DOI: 10.1057/9781137408211.0006

surveillance technology given information about the number of people in its data base, the number of true terrorists among these people, the accuracy rate of the technology, and its inaccuracy. See, for example, Sam Savage and Howard Wainer, "Until Proven Guilty: False Positives and the War on Terror: Bayesian Analysis." *Visual Revelations*. Retrieved on June 18, 2014 from http://www-stat.wharton.upenn.edu/~hwainer/Readings/Wainer%20Savage.pdf.

11 The FIS Court indicated that there were more than 250 communications. Further, e-mail exchanges, chats, etc. have both senders and receivers. It is therefore likely that the number of individuals who were falsely flagged as "potential terrorists," or at least associated with terrorist plots, is much more than what is here estimated.

12 Peter Bergen, et al., "Do NSA's Bulk Surveillance Programs Stop Terrorists?" New America Foundation, p. 9.

13 Ibid., p. 10.

14 As discussed in Chapter 2, the system itself should be locked in order to require a search warrant when strong indicators involving US persons are used in search queries.

15 H.R.3361, USA Freedom Act, May 22, 2014. Retrieved on June 18, 2014 from http://www.gpo.gov/fdsys/pkg/BILLS-113hr3361eh/pdf/BILLS-113hr3361eh.pdf.

16 Peter Bergen, et al, "Do NSA's Bulk Surveillance Programs Stop Terrorists?" New America Foundation, p.2.

17 Ibid., p. 2.

18 Peter Bergen, et al, "2010 San Diego Shabaab Support Network," New American Foundation. Retrieved on June 18 from http://natsec.newamerica.net/terror-plot/2010-san-diego-shabaab-support-network.

19 HR 3361, USA Freedom Act. Retrieved on June 18, 2014 from http://www.gpo.gov/fdsys/pkg/BILLS-113hr3361eh/pdf/BILLS-113hr3361eh.pdf See also Chapter 2.

20 HR3361, Section 701(K)(2).

21 Gary B. Pruitt, President & CEO, Associated Press to Attorney General Eric Holder, May 13, 2013. Retrieved on June 18, 2014 from http://www.ap.org/Images/Letter-to-Eric-Holder_tcm28–12896.pdf.

22 Jonathan Bloom, "Department Of Justice Issues Revised News Media Subpoena Policies," Corporate Counsel, October 2, 2013. Retrieved on June 18, 2014 from http://www.metrocorpcounsel.com/articles/24621/department-justice-issues-revised-news-media-subpoena-policies.

23 See Chapter 1.

24 "How the NSA's MUSCULAR program collects too much data from Yahoo and Google," *Washington Post*, October 30, 2013. Retrieved on June 18, 2014 from http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/.

DOI: 10.1057/9781137408211.0006

25 Spencer Ackerman and James Ball, "Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ," *The Guardian*, February 27, 2014. Retrieved on June 18, 2014 from http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

26 See Chapter 1.

27 Edward Snowden, Interview with Hubert Seipel, *NDR News*, January 26, 2014. Retrieved on June 17, 2014 from http://www.commondreams.org/headline/2014/01/27–1.

28 FBI, *Next Generation Identification: System Requirements Document,* Version 4.4, October 1, 2010, p. 244. Retrieved on June 18, 2014 from http://epic.org/foia/fbi/ngi/NGI-System-Requiremets.pdf.

29 Since OPTIC NERVE was begun in 2008 and the NGI statistic of up to a 20% false positive rate was gleaned from a 2010 report, this is probably a reasonable, even modest, projection of the accuracy rate of facial recognition software in 2008. However, there may have been some improvements in the accuracy of the software between 2010 and the present.

30 G. Givens, J. R. Beveridge, B. A. Draper, and D. Bolme, "A Statistical Assessment of Subject Factors in the PCA Recognition of Human Faces," Proceedings of the 2003 Conference on Computer Vision and Pattern Recognition Workshop, 8 (2003), p. 7.

31 Kevin Gosztola,"Supreme Court Declines to Hear Case That Would Have Challenged NSA Warrantless Surveillance of Lawyers," *The Dissenter*, March 4, 2014. Retrieved on June 18, 2014 from http://dissenter.firedoglake.com/2014/03/04/supreme-court-declines-to-hear-case-that-would-have-challenged-nsa-surveillance-of-lawyers/.

32 Ibid.

33 American Bar Association (ABA), Model Rules of Professional Conduct, Rule 1.6(c). Retrieved on June 18, 2014 from http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html.

34 ABA, Model Rules of Professional Conduct, Comment on Rule 1.6, Retrieved on June 18, 2014 from http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6.html.

35 Gosztola, "Supreme Court Declines to Hear Case That Would Have Challenged NSA Warrantless Surveillance of Lawyers," *The Dissenter*, March 4, 2014.

36 James Risen and Laura Poitras, "Spying by N.S.A. Ally Entangled U.S. Law Firm," *The New York Times*, February 15, 2014. Retrieved on June 18, 2014 from http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html?_r=3.

DOI: 10.1057/9781137408211.0006

37 U.S. Code 50 (1978), Section1801(e)(2)(B). Retrieved on June 17, 2014 from http://www.law.cornell.edu/uscode/text/50/1801.
38 Siobhan Gorman, Evan Perez, "U.S. Collects Vast Data Trove," *Wall Street Journal*, June 7, 2013. Retrieved on June 18, 2014 from http://online.wsj.com/news/articles/SB10001424127887324299104578529112289298922.
39 Laura Poitras, Marcel Rosenbach and Holger Stark, "'Follow the Money': NSA Monitors Financial World," *Spiegel International*, September 16, 2013. Retrieved on June 18, 2014 from http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430–2.html.
40 James Ball, "NSA collects millions of text messages daily in 'untargeted' global sweep," *The Guardian*, January 16, 2014. Retrieved on June 18, 2014 from http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.
41 Poitras et al, "'Follow the Money': NSA Monitors Financial World," *Spiegel International,* September 16, 2013.
42 Ibid.
43 Ibid.
44 See Chapter 1.
45 Barton Gellman and Ashkan Soltaini," NSA tracking cellphone locations worldwide, Snowden documents show," December 4, 2013. Retrieved on June 18, 2014 from 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.
46 L. Scott Harrell, "Locating Mobile Phones through Pinging and Triangulation," *Pursuit*, July 1, 2008. Retrieved on June 18, 2014 from http://pursuitmag.com/locating-mobile-phones-through-pinging-and-triangulation/.
47 Gellman and Soltaini, "NSA tracking cell phone locations worldwide, Snowden documents show," December 4, 2013.
48 Ibid.
49 James Glanz, Jeff Larson and Andrew W. Lehren, "Spy Agencies Tap Data Streaming From Phone Apps," *The New York Times*, January 27, 2014. Retrieved on June 18, 2014 from http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html?_r=0.
50 National Security Agency (NSA), "(U) Converged Analysis of Smartphone Devices: Identification/Processing/Tasking - All in a day's work [Slides]," May 2010. Retrieved on June 18, 2014 from https://www.documentcloud.org/documents/1009660-nsa.html.
51 Ibid.

DOI: 10.1057/9781137408211.0006

4

Transparency of Policies and Practices

Abstract: *This chapter discusses the problem of transparency about government policies and practice in governing cyberspace. Drawing from social contract theorist, especially Immanuel Kant, it argues for relinquishing the quest for power and control over cyberspace, which is by its nature a "global commons," and instead moving toward international cooperation (a "community of ends") in transparently creating the regulations governing cyberspace. To this purpose, a global internet forum is proposed for creating a comprehensive set of policies and practices in cyberspace, which rational beings would be accept. The chapter concludes with a discussion of the role of the media in informing open, international dialog.*

Cohen, Elliot D. *Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.* New York: Palgrave Macmillan, 2014.
DOI: 10.1057/9781137408211.0007.

While the Snowden leaks have facilitated greater dialog concerning the policies and practices that are now governing cyberspace, the operations of NSA spying is still largely conducted in secrecy. Nations do have a right to protect themselves from attacks by foreign invaders (whether through physical assaults or cyber attacks). However, there is a distinction between disclosing the policies and practices of conducting a surveillance network, and disclosing the details of a particular terrorist investigation. Secrecy concerning the latter for national security purposes is a reasonable premise. However, it cannot reasonably be inferred that, therefore, the former should also be a secret. Indeed, in order to respect the rights of those who are under surveillance, the government has an obligation to disclose this information, including the nature of the technology being deployed. Unfortunately, fueled by an ideology aimed at power and control of cyberspace, the US and its allies have maintained an atmosphere of secretiveness about these surveillance technologies, and have used this clandestine environment to pursue an aggressive, nationalistic stance, including economic espionage. This chapter maps the ethical justification for a change in ideology toward reframing cyberspace, not as a "wild west" to be conquered and controlled, but instead as a shared global space ("global commons") to which all inhabitants have a right to democratically co-exist. This new way of thinking, it is argued, is a game changer for the US's approach to surveillance, and moves toward a new "social contract," with the people of the connected world, to create an infrastructure, including a "global forum," in cyberspace, that is free and democratic.

Economic espionage

The 1978 Foreign Intelligence Surveillance Act broadly defines "foreign intelligence information" to include "information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to . . . the conduct of the foreign affairs of the United States". This purpose of foreign intelligence gathering is listed as distinct from the national defense or security of the United States. The term, "conducting of foreign affairs," however, is not itself defined by the Act, which, therefore, gives it broad latitude of interpretation. Within this penumbra of meaning, the US has clearly considered it to include information that bears on the US's economic interests. According to National Intelligence Director, James Clapper,

DOI: 10.1057/9781137408211.0007

> It is not a secret that the Intelligence Community collects information about economic and financial matters, and terrorist financing. We collect this information for many important reasons: for one, it could provide the United States and our allies early warning of international financial crises which could negatively impact the global economy. It also could provide insight into other countries' economic policy or behavior which could affect global markets.[1]

Although Clapper presents his justification for "economic espionage" in terms of the welfare of the global market and economy, it is clear that the US, at least, seeks to serve its own interests and those of its allies when it collects information about economic and financial matters through the MWSN. In pursuing these interests, the veneer of pursuing global interests can be used as a morally respectable reason for spying on others who do not pose a national threat. Without clear legal limits on what can count as "conducting of foreign affairs," such economic and market-driven spying can degenerate to self-aggrandizing eavesdropping.

This appears to have been the case with regard to spying on state officials throughout the world, including those of US allies such as France and Germany. For example, Britain's GCHQ and the NSA have cooperated in monitoring the communications of senior European Union officials; foreign leaders, including the former Israeli Prime Minister and Defense Minister, the presidents of Brazil and Mexico, and the Chancellor of Germany; an official of the Economic Community of West African States (organization consisting of 15 countries that seek to promote economic and industrial activity); officials of United Nations relief programs in Geneva such as UNICEF and the United Nations Institute for Disarmament Research; officials at the German Embassy in Rwanda, a French ambassador, and a Skype security team in Estonia.[2]

The NSA has also targeted businesses. For example, NSA documents reveal that the NSA has targeted French oil and gas company Total, which is the fifth largest oil and gas company in the world; the Brazilian oil giant, Petrobras, which also produces biofuels and other forms of alternative energy; and Thales, a French-based conglomerate with aerospace, space, defense, transportation, and security divisions. Such companies as these, among others, seek competitive advantages in their respective markets through trade secrets and other confidential information. When the NSA hacks private networks of foreign (no less than the US) companies and acquires confidential information, it creates the potential to destroy the competitive edge these companies might have.

DOI: 10.1057/9781137408211.0007

For example, Petrobras allegedly has had knowledge of the locations of oil rich regions.[3] If the US were to gain such highly coveted information, it could give it to a US competitor and thereby gain an unfair advantage over Petrobras. Since Petrobras is, in fact, partly owned by the Brazilian government, such unauthorized access to company information is also tantamount to acquiring government information, not for national defense purposes but for purposes of advancing its own economic interests and possibly those of US corporations.

The issue is not the evidentiary one of proving that the US seeks to acquire information from a foreign company such as Petrobras in order to give it to one of its own companies. In fact, there does not appear to be evidence to support this hypothesis, but there is also no evidence to support the contrary. And this is precisely the point. Such plots to steal company secrets for self-aggrandizing purposes are within the realm of possibility. They are within the realm of possibility because the MWSN has been deployed by the NSA and its affiliates for purposes of industrial espionage, under the banner of "conducting foreign affairs". If such possibilities are not sealed off, they will, predictably, become (if not already) actualized possibilities. As wars for territorial expansion have throughout history been justified on the basis of national defense, hacking into industrial networks may analogously be justified in the name of preserving the global economy, when the real reason is to advance the US's geopolitical dominance.

Of course, looking at the matter from the bias of a US person, this may seem to be a rational argument for breaching the privacy of foreign corporations. The logic in this case is a self-serving one, but nonetheless there is logic to it. And this justification can even be broadened to include the utilitarian rationale proclaiming that, a world in which the US and its allies dominate is a world in which everybody is better off. However, such an argument lacks empirical support and is based largely on a nationalistic bias.

Global surveillance and the control of cyberspace

The nationalistic stance regarding global power and control largely defined US foreign policy during the George W. Bush administration and it also appears to have largely defined the Obama administration's foreign policy. Its ideological roots were shaped in 1997, with the founding

DOI: 10.1057/9781137408211.0007

of the Project for the New American Century (PNAC), a Washington, DC-based political action association consisting of many of the soon-to-be members of the George W. Bush administration, including Vice-President Richard Cheney and Secretary of Defense Donald Rumsfeld.[4] The stated goal of PNAC was to maintain and advance the US as "the world's preeminent power" by "preserving and extending an international order friendly to our security, our prosperity, and our principles."[5] PNAC's vision included the militarization of the US, including its ability to control cyberspace and the internet, which it referred to as "emerging elements in global commerce, politics and power"[6]; and it maintained that "any nation wishing to assert itself globally must take account of this other new 'global commons' ".[7]

Under the thrust of the PNAC ideology, the internet has come to be viewed by the US and its allies as a frontier to be dominated, controlled, and manipulated for not only national security purposes but also for purposes of "global commerce, politics, and power". The US has accordingly attempted to exploit the MWSN for such broad purposes. As such, unless the US (in cooperation with its allies) reassesses its ideological commitment to the exercise of power and control over cyberspace, it is unlikely that there will be any changes in its surveillance practices and tendencies concerning foreign politics and commerce.

Cyberspace as a "global commons"

Such change in ideology is necessary if the US is to reestablish its image as a moral leader as distinct from a military power. The proviso "if the US is to reestablish its image as a moral leader . . ." is, of course, important. The US must be committed to this objective and must take steps that prove *to the world* that it is so committed. This idea of universal validation can itself pave the way to a new ideology to replace the PNAC standards of power and control. For, as the PNAC ideologues themselves (paradoxically) expressed it, cyberspace is a "global commons," which must, therefore, necessarily exclude policies of domination and control. Inasmuch as cyberspace is (globally) *shared* space, all of us have an interest in how it is governed, not just the US or its allies. Thus, from an enlightened moral perspective, just how, when, where, why, and for what purposes the MWSN is deployed in cyberspace is not a matter to be determined by any single nation or

DOI: 10.1057/9781137408211.0007

subset of nations; for, again, this is *the province of shared governance of shared space*.

In cyberspace, there is, therefore, need of an ethics that recognizes everyone's interest and voice in this "global commons". Such a standard of universality can be found thematically in the social contract theories of the Age of Enlightenment, including that of Hobbes, Locke, Rousseau, and Kant. Here, as with contemporary contract theorists such as Rawls, the key question is what constraints would reasonable people accept on their personal liberty within a state of nature, that is, a state where there are no restrictions on personal liberty? Cyberspace may itself be conceived as such a state of nature and thus the question is what constraints on civil personal liberties in cyberspace would reasonable people accept?

In his treatise on *Perpetual Peace*, as an antidote to war and the establishment of universal, unconditional peace, Immanuel Kant argued that the world needed to move toward a confederation of loosely related nations, each of which had representative governments wherein the people could freely decide whether or not they were willing to invest their personal resources (including life, liberty, and limb, as well as economic means) in fighting a war.[8] Kant believed that if the people rather than their governors were placed in the position of deciding such crucial matters, they would eventually move toward a state of "perpetual peace". Such a confederation was not, according to Kant, intended to undermine the authority of the state but was instead limited to the specific purpose of protecting states against despotic control of the people's right to decide matters of peace and security.[9]

Such a model to protect against despotic control over cyberspace and to ensure peace and security to operate inside it can provide a useful way of reframing US cyberspace policy. The idea is, analogously, to give the people of the nations of the world who operate in cyberspace the right to decide what personal liberties they may be willing to relinquish in order to attain peace and security in cyberspace.

Kant's mirror of rational choice was reflected in his idea of a categorical imperative according to which one acts rationally only if one can will one's "maxim" or reason for action to be a universal law of nature.[10] The idea here is that when one conceives oneself of deciding for all humankind what is acceptable, one's own self-aggrandizing double standards, so placed in the light of universality, are seen to be unacceptable. Thus, lying to others for self-serving purposes loses its allure when one considers it

DOI: 10.1057/9781137408211.0007

in the light of a universal law of nature wherein everyone would lie to everyone else. For in such a universe, no one would believe anyone else and the condition of trust, upon which lying itself depends for its efficacy, would break down. Accordingly, no rational person would accept such a universe, as implied by universalizing self-serving lying; and, as such, on the Kantian standard, self-serving lying is morally wrong.

As applied to the operation of the MWSN, no rational person would be willing to accept the maxim of eavesdropping on others' private conversations whenever it was to one's own advantage since, if such a practice were made into universal law, the condition of privacy upon which such personal disclosures depends, would itself be undermined. Yet, the US policy on eavesdropping on the private communications of foreign companies and their governments amounts to such a maxim of self-interested, systematic violation of privacy; which is not a universal law to which rational US politicians or corporate officers would themselves be willing to be subjected.

From such a universal law perspective, a condition of successful communication is that of transparency, that is, open and honest discourse. For without some reasonable expectation of transparency in communication, the possibility of communication breaks down; for, if one individual (or nation) does not accept that the other is being honest, then no belief is formed, and hence no information is transmitted. As such, if the US wishes to attain credibility concerning its policies and practices in cyberspace, then it must be more transparent about these policies and practices.

This is a two-way street. The people of the world must be able to speak and argue freely about rational policies and practices governing international surveillance of cyberspace, and the US and its allies must be prepared to listen, and to be reasonably transparent about its policies and practices. Here, the term "reasonably" is an important caveat because a nation does have a right to some measure of privacy itself, especially when it concerns national security. However, this proviso should not be permitted to consume the transparency rule. This appears to have happened in the past under a pretense of "national security". Indeed, if the body of heretofore classified information leaked by Edward Snowden shows anything, it is that the mass, systematic, and global deception perpetrated by the US government and its allies surrounding the operation of the colossal MWSN was not necessary to protect national security. In the aftermath of the Snowden leaks, no breakdown in national

DOI: 10.1057/9781137408211.0007

security occurred. Rather, in the aftermath, new possibilities for opening up healthy public discourse on the current and future disposition of this giant surveillance network have emerged.

The internet as host to a global forum

The internet itself can supply a natural medium for facilitating such public discourse on a world-wide basis. In cyberspace, there are no geographical boundaries. On the net, language translation software makes possible dialog between speakers of diverse languages. Messages are transported instantaneously from across the globe, thereby breaking down temporal barriers. As a result, it makes sense to speak of the connected world as one world community. True, there are still cultural, religious, and ethnic distinctions within the diverse groups so united. Nevertheless, all are human beings.

Kant referred to such a community of human beings as a "kingdom of ends" in order to mark its members out as bearers of human rights. According to Kant, chief among these rights is the right of self-determination. By virtue of being rational, human beings or persons are capable of choosing and deciding for themselves, unlike objects or mere things. Consequently, to manipulate, use, and deceive persons is to treat them as though they were mere things. It is, therefore, to violate their fundamental right of self-determination.

The US and its allies, therefore, owe it to the world community to be open and honest about its surveillance of cyberspace. Transparency is not just being nice. It is a moral obligation. In monitoring and eavesdropping on peoples' personal communications in cyberspace without their knowledge or consent, the US and its allies violate the fundamental human right of self-determination by treating the people of the world like objects manipulated. Here, respect for the self-determination of human beings requires *informed consent*, not deception and lack of information about how their personal information is being acquired, stored, analyzed, or otherwise processed. For example, one is not given informed consent when one is not told about the extent of the problem of false positives in searching for criminal and terrorist suspects; or the possibility that sex acts performed during a private Yahoo chat will be acquired or viewed by the NSA; or that one's legal defense in a high profile criminal case will be acquired or examined by the NSA; or that one's company trade

DOI: 10.1057/9781137408211.0007

secret will be intercepted by the US government; or that, by virtue of one's role (for example, foreign diplomat or journalist), one may end up on an NSA target list.

Being informed about these and many other possibilities is essential to informed consent; and informed consent is essential to the exercise of the fundamental human right of self-determination. Conversely, inasmuch as cyberspace is a "global commons," the world community should also be given a voice in the policies that govern this shared space. Despotic control of cyberspace is no more respectful of the fundamental human right of self-determination than it is of physical space. As underwriters of freedom and democracy, it is essential that the US and its allies also underwrite freedom and democracy in the manner in which the rules governing cyberspace are created and implemented. This portends a world forum in which ideas are respectfully submitted and subjected to the scrutiny of the world community, rationally discussed and debated, and accepted or denied by a majority voice.

Given the ubiquitous, democratic character of the internet, the host of such a world forum would naturally be the internet. From its inception, the internet has been distinguished from other means of mass communication by its ability to support communication by the many to the many—as distinct from other mass media such as TV and radio, which involve communication from some to the many. This democratic, net neutral architecture of the internet naturally supports a world forum in which the many can speak to the many about how they believe the internet should be governed.[11] Here is where the fate of the MWSN can and should be decided. When the US conducts mass dragnets of foreigners without regard to their guilt or innocence and consequently treats everyone as criminal or terrorism suspects, it sets a precedent for other nations to do the same to US persons. The term "foreigner" is, after all, a relative term. US foreign intelligence collects data on persons outside of the country. But US persons are foreigners to nations outside the US, which means they are also entitled to collect intelligence on US persons. Therefore, everyone, US person or non-US person alike, has a stake in what policies are implemented globally in conducting surveillance of cyberspace.

As discussed in Chapter 2, the MWSN currently abridges the constitutional rights of US citizens because the NSA acquires information from millions of US citizens that contravenes minimization standards pursuant to the 1978 Foreign Intelligence Surveillance Act. MWSN data

DOI: 10.1057/9781137408211.0007

collection by the US must therefore be curtailed as a matter of US law. Clearly, US citizens should not be subjected to unreasonable searches and seizures that contravene the Fourth Amendment. These protections are there because a citizen of a nation has no other protections against unjust encroachment of personal liberty by that nation except for those protections afforded by the nation itself. Thus, all democratic states should protect its citizens against state encroachment of civil liberties by building in legal protections. However, this still leaves wide open the question of what protections a given state may expect against encroachment of personal liberties by foreign governments. Thus, while US citizens are entitled to protection by the Fourth Amendment against unreasonable searches and seizures, non-US citizens outside the US do not similarly enjoy such protections. And, conversely, while non-citizens may enjoy protections against encroachment of civil liberties by the laws of their nations, US citizens may not also enjoy such protections against unreasonable encroachments of personal liberties by their nations.

This is why the world community needs to supplement the laws of their nations with other international constraints on surveillance in cyberspace that protect "foreigners"—realizing that we are all foreigners to another nation. These international constraints should be decided on the basis of a democratic forum of the sort suggested, for we all have the same concerns as citizens of the world community.

It may be contended that the US exercises primary control over the MWSN and therefore the problem is not universally shared but falls flatly on the US. This, however, is short-sided. It cannot be assumed that the US should remain the chief power broker in the control of cyberspace; for this is the same PNAC ideology that has led the US down an oppressive road that has diminished its moral standing in the eyes of the world community. Further, the US cannot be assumed to have a monopoly on technological expansion because other nations that do not currently possess access and control of the MWSN may aspire to such status. Thus, the rules that govern cyberspace cannot assume any controlling interest in cyberspace. We all have a common interest in this globally shared space and its governance.

The Chinese government must also be part of this calculus. Presently, China has a massive internet police force that eavesdrops on Chinese persons to ensure that their opinions are "accurate".[12] Its political interests in monitoring US persons as well as the Chinese people should also not be dismissed. Thus, in 2012 the US House Intelligence Committee

DOI: 10.1057/9781137408211.0007

warned that two Chinese telecommunication equipment companies may be implanting devices into their routers enabling Chinese surveillance. The US warned that the equipment may, therefore, be violating US laws and international standards. Ironically, according to a 2010 NSA report, the NSA itself routinely intercepts routers and servers produced in the US before they are shipped to international customers. The NSA then implants surveillance tools into these devices, repackages them, and sends them on to the international customers, thereby allowing the NSA to monitor the international traffic passing through these devices.[13] As such, in its quest for power and control, the US has become precisely what it has warned against. In violating the same standards that it admonishes others not to violate, it has set itself up for international ridicule rather than respect.

On the other hand, in insisting on a consistent set of ethically as well as legally acceptable global standards for all to follow, it eliminates the problem of double standards. In relinquishing its zeal for power and control, it can help become the moral leader that is necessary for a global community that plays by the rules. True, it is a pipedream to expect that there will be no deceptive practices launched by power brokers such as China; however, the world community will be more likely to stand firm against such practices when the US and its allies are not engaging in the same deceptive practices. In giving up the quest for power and control of cyberspace, the US and its allies will effectively gain the most venerable sort of power, namely, the respect and cooperation of the world community.

The global forum set up on the internet can serve as a basis for drafting a consistent set of international standards governing surveillance and intelligence gathering. Hundreds of millions of people throughout the world can weigh in on the challenges confronting the ethical management of cyberspace. Here too is an opportunity for democratic deployment of programs that analyze data. From within the mass body of opinions and outlooks, a consensus can be defined. Indeed, there is no better moral compass than subjecting ideas to the court of public opinion. If democracy does work, it should work here to provide a set of common standards that regulate the gathering of foreign intelligence. Undoubtedly, there will be arguments that specific curtailments of surveillance powers will prevent a nation from adequately defending itself from terrorist attacks. However, in the light of public debate, the legitimate concerns can be taken seriously and the bogus attempts to

DOI: 10.1057/9781137408211.0007

gain unfair and unnecessary power and control of cyberspace can be dismissed. For example, it is doubtful that such a public court of international opinion would countenance the surveillance of foreign officials or corporations as is presently being performed by the US and its allies. Clearly, there would be need to provide evidence to document a claim.

Following Kant's model, this would not be a world government that would govern the laws of the land of nations that participate in the forum. This would be a special world organization for the purpose of regulating cyberspace. This means that the US would not be able to set up a "back door" tap point at an international location and thereby avoid legal and ethical constraints on collections as it presently does. International constraints would reasonably include quantitative (how much data can be collected, how long can it be maintained) as well as qualitative constraints (what sort of data can be collected) on bulk collection of data. Indeed, the question of whether bulk collection of data is itself a defensible tool for foreign intelligence gathering would be a question worthy of placing on the docket. Given a climate of transparency, such a defense would undoubtedly require adducing the empirical data to show that bulk data collection actually works to stop terrorism. After all, terrorism is a global problem and the world community is entitled to such veridical data if indeed it exists.

The media as a facilitator of international dialog

A global forum is no substitute for a vigilant media that informs the dialog, and would need to work synergistically with such a forum. Unfortunately, media consolidation has brought about a diminution of the number of corporations who hold the reigns of the mainstream media. Thus, while there may be numerous channels on cable TV, there are only a handful of monolithic corporations that control the programming on these channels. Thus, the amount of independent news and information sources are few.[14]

The bright side, however, is that, while net neutrality lasts, there are also many independent media sources that address pressing mass surveillance, among other issues.[15] These sources tend to provide substantial coverage of news stories that the mainstream corporate media have censored or failed to adequately cover. Such sites can and should become part of the steady news diets of every concerned citizen.

DOI: 10.1057/9781137408211.0007

Mainstream media, in particular network TV news, cannot and should not be relied upon to supply the full daily consumption of news for the average informed citizen. News shows on Fox or MSNBC, from *The O'Reilly Factor* to *The Rachel Maddow Show*, editorialize and dilute fact claims with network bias. Thus, during the George W. Bush administration, Maddow tended to be critical of Bush policies, while O'Reilly tended to defend these policies. During the Obama administration, the converse is now true with O'Reilly tending to be critical of Obama policies, and Maddow tending to defend them.[16]

These "news" talk shows tend to editorialize rather than to report the news. While codes of journalism typically enjoin that news organizations be clear as to which of these activities is being done, mainstream media often confuse the two. For example, the *Code of Ethics* of the Society for Professional Journalism (SPJ) prescribes, "Distinguish between advocacy and news reporting. Analysis and commentary should be labeled and not misrepresent fact or context."[17] Unfortunately, knowing whether coverage of a story on "Fox News" is really news or just editorializing is largely left to the viewer.

In the case of coverage of the MWSN by mainstream media, the facts are often buried in a maze of debate about marginal issues such as the illegality of Snowden's disclosures. These discussions tend to circumvent the serious questions regarding the content of Snowden's disclosures and what they mean for the survival of a democratic and free nation.

Organizations such as WikiLeaks can fill a gap in the provision of facts. Thus, a series of slides prepared by the NSA about the inner workings of the MWSN does not editorialize. Whether or not the described methods actually work as intended is one thing; however, such primary sources provide a clear window into the types of spy technologies that are being deployed for amassing data. However, much like listening to lengthy CSPAN events programming in order to gain information, reading leaked documents posted to WikiLeaks can often be quite time-consuming, tedious, and challenging to sift through in order to come to an informed conclusion. Unfortunately, the other extreme is the limited news hole of network evening news, which reports fragments of information lifted out of context and framed to the beat of network policy. Here, a helpful adjunct can be that of listening to BBC radio broadcasts, which tend to delve more deeply into issues like surveillance, and to give a wider global perspective beyond one confined to US interests. A healthy diet of both foreign as well as US press can definitely provide a more

DOI: 10.1057/9781137408211.0007

informed and sophisticated understanding of the way mass surveillance is affecting others outside the US. For example, it can be edifying to find that thousands have protested in Germany against US spying and the silence of the German government in condemning it.[18] Such information can be unifying across continents, thereby increasing the ability of people to come together to make global changes in the MWSN.

Newspapers such as *The Washington Post, The New York Times, The Guardian, Der Spiegel, USA Today*, and even *The Wall Street Journal* have, in this post-Snowden disclosure era, proven that they can make important contributions to greater transparency in US policy governing cyberspace. Hopefully, this trend will continue in the future.

Citizen journalism also holds much potential toward an informed, global policy regarding cyberspace. In consulting independent media sources, checking out credible foreign news organizations (for example, *Der Spiegel* and BBC), viewing mainstream media sources with care, looking into primary sources where relevant, reading the investigative reports of newspapers like the aforementioned, and listening to the informed judgments of others who are engaging in like activities, citizens of the world community can make important contributions to framing a rational, evidence-based policy about the governance of rules. A world forum on the internet can be a valuable vehicle for communicating and debating these ideas. The media, taken as a comprehensive package as described, can work synergistically to provide the informed judgment needed to make such a world forum work.

But it can work only if the people are willing to think freely and to distinguish between evidence-based claims and government propaganda. National security is an important consideration, but it can also be used as a buzzword to intimidate the masses into compliance. The key here is to avoid authoritarian thinking ("The government says so, therefore it must be true").[19] Strong, healthy, democratic societies question authority and ask for evidence. Blind adherence to government authority can lead to totalitarian, anti-democratic states as history has repeatedly demonstrated.

Notes

1 James Clapper, "Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage," September 8, 2013. Accessed

DOI: 10.1057/9781137408211.0007

on June 18, 2014 from http://icontherecord.tumblr.com/post/60712026846/statement-by-director-of-national-intelligence.

2 James Glanz and Andrew W. Lehren, "N.S.A. Spied on Allies, Aid Groups and Businesses," *New York Times*, December 20, 2013. Accessed on June 18 from http://www.nytimes.com/2013/12/21/world/nsa-dragnet-included-allies-aid-groups-and-business-elite.html?_r=0 Anthony Boadle, "U.S. spied on presidents of Brazil, Mexico - report," *Reuters*, September 2, 2013. Accessed on June 18 from http://in.reuters.com/article/2013/09/02/usa-security-brazil-mexico-surveillance-idINDEE98108U20130902.

3 "NSA Documents Show United States Spied Brazilian Oil Giant," *Fantastico*, August 9, 2013. Accessed on June 18, 2014 from http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html.

4 See also Chapter 1.

5 Project for the New American Century (PNAC), "Statement of Principles,"1997. Accessed on June 17, 2014 from http://cf.linnbenton.edu/artcom/social_science/clarkd/upload/PNAC---statement%20of%20principles.pdf.

6 Project for the New American Century PNAC), *Rebuilding America's Defenses*, September 2000, p. 57. Accessed on June 18, 2014 from http://www.informationclearinghouse.info/pdf/RebuildingAmericasDefenses.pdf.

7 Ibid.

8 Immanuel Kant, *Perpetual Peace: A Philosophical Essay*, London: Swan Sonnenscheine, 1903. Accessed on June 2018 from https://archive.org/details/perpetualpeaceaookantgoog.

9 "This league does not tend to any dominion over the power of the state but only to the maintenance and security of the freedom of the state itself and of other states in league with it, without there being any need for them to submit to civil laws and their compulsion, as men in a state of nature must submit." Kant, *Perpetual Peace*, p. 134.

10 Immanuel Kant, *Fundamental Principles of the Metaphysics of Morals*, 1785. Accessed on June 18, 2014 from http://www.gutenberg.org/ebooks/5682

11 Net neutrality is presently being threatened by the major internet gatekeepers, however. See Chapter 5.

12 "China employs two million microblog monitors state media say," BBC, October 2013. Accessed on June 18, 2014 from http://www.bbc.com/news/world-asia-china-24396957

13 Glenn Greenwald, "How the NSA tampers with US-made internet routers," *The Guardian*, May 12, 2014. Accessed on June 18, 2014 from http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden.

DOI: 10.1057/9781137408211.0007

14 Elliot D. Cohen, *News Incorporated: Corporate Media Ownership and Its Threat to Democracy.* Amherst, NY: Prometheus Books, 2005.

15 See, for example, the list of independent media sources published by *Project Censored* at http://www.projectcensored.org/independent-periodicals-webzines/.

16 Josh Feldman, "Former MSNBC Producer Skewers Hosts For Pro-Obama Bias: 'Official Network Of The Obama White House,'" *Mediaite*, July 8, 2013. Accessed on June 18, 2014 from http://www.mediaite.com/tv/former-msnbc-producer-skewers-hosts-for-pro-obama-bias-official-network-of-the-obama-white-house/.

17 SPJ, *Code of Ethics*, Principle 1. Accessed on June 18, 2014 from http://www.spj.org/pdf/ethicscode.pdf.

18 "Germans rally to condemn silence on US spy schemes," *PressTV*, June 19, 2014. Accessed on June 18, 2014 from http://www.presstv.com/detail/2013/08/01/316708/germans-slam-silence-on-us-spy-schemes/.

19 Elliot D. Cohen, "Digging Deeper: Politico-Corporate Media Manipulation, Critical Thinking, and Democracy," *Project Censored* 2014, November 13, 2013. http://www.projectcensored.org/digging-deeper-politico-corporate-media-manipulation-critical-thinking-democracy/.

DOI: 10.1057/9781137408211.0007

5
Democracy in Cyberspace

Abstract: *This chapter discusses the urgency of keeping the architecture of the internet free and democratic as a condition of ensuring transparency about government policies and practices in cyberspace. Accordingly, the chapter tracks the changing legal landscape of the internet toward increasing control by Internet Service Providers (ISPs) such as Comcast, Verizon, and AT&T. It examines the 2005* Brand X *Supreme Court decision, which permitted the Federal Communications Commission (FCC) to reclassify the internet, from a public utility to the private property of the ISPs. The chapter argues that, unless the FCC re-establishes the internet as a public utility, it is fated to become a private corporate network, thereby foreclosing the opportunity to build global consensus and transparency about government surveillance policies and practices.*

Cohen, Elliot D. *Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.* New York: Palgrave Macmillan, 2014.
DOI: 10.1057/9781137408211.0008.

As discussed in the preceding chapter, the US, along with its allies, can and should maintain transparency about its policies and practices governing cyberspace if it is to respect human rights, notably that of self-determination, and (re)establish itself, globally, as a moral authority. Toward this end, it was argued that, because cyberspace is a global commons, the world community has a legitimate interest and should have a voice in the establishment of the policies and practices governing it. Further, it was argued that the open architecture and neutrality of the internet (everyone has an equal voice so that the many can communicate directly with the many) presently makes it the most suitable medium for establishing such a global, democratic forum for helping to justify and establish, in the light of rational, public debate, morally responsible cyber policies and practices. Unfortunately net neutrality is itself under attack by the giant internet gatekeepers such as Comcast, Verizon, and AT&T. This chapter discusses the legal issues surrounding this attack and what needs to be done to preserve the democratic integrity of the internet.

The internet as a main source of worldwide news

The internet can and should come to play a vital role in preserving human rights in cyberspace. The good news is that reliance on the internet as the mainstay of worldwide news and information has already taken hold, and has been rapidly advancing, thereby making it the preferred vehicle for imparting news and information about government policies and practices in cyberspace.

According to a July 2013 Pew Research Survey, the internet has been incrementally surpassing all other media as an outlet through which people receive national and international news. According to the study, 50 percent of people cite the internet as their main source of national and international news as compared to 13 percent in 2001, 24 percent in 2007, and 40 percent in 2008. On the other hand, the trend to get one's news from newspapers has steadily diminished. According to the study, only 28 percent of people surveyed cited newspapers as their main source of news, as compared to 45 percent in 2001, and 35 percent in 2008. Further, while television is still, on average, the main source of news for 69 percent of those surveyed (as compared to 70 percent in 2008), the demographic trends are also starting to lean toward the internet over television. Thus,

DOI: 10.1057/9781137408211.0008

71 percent of people 18 through 29 years old cite the internet as their main source of news as compared to 55 percent who site television as their main source. Further, 63 percent of those 30–49 site the internet as their main source of news while those who are older still tend to prefer television to the internet as their main source of news.[1] It is, therefore, likely that as this trend continues, the internet will soon surpass television as the main source of national and international news.

More good news is that, in order to increase their subscriptions, newspapers have moved toward an online presence. In fact, *The Guardian US* and *The Washington Post* won Pulitzer prizes for their reporting on the NSA's mass spying program based on the Snowden leaks. *The New York Times* and *Der Spiegel* were also major sources of information on the program.[2] These news sources carried their "breaking news" stories online and, consequently, the Snowden leaks became widely disseminated across the net.

TV network news and telecommunication companies

Unfortunately, major TV news organizations such as MSNBC/Comcast, Fox News/News Corp, CNN/Time Warner, and CBS/National Amusements, and ABC/Disney have done a poor job covering the substance of the Snowden leaks, tending to concentrate more on whether Snowden was a hero or traitor, how much damage he has done, and how to bring him to justice.[3] Moreover, this shoddy coverage of Snowden is a symptom of a deeper, more pervasive problem. Presently, there is an expanding presence of major TV media corporations on the internet. So, the cited Pew Study may be less impressive if one were to learn that most people get their internet news from a mainstream corporate media website like *Fox.com* or *MSNBC.com*. What this suggests is that the absorption of TV into an expanding cyberspace may also mean greater and greater corporate control of internet content, and less and less diverse voices and representation of alternative views. Unfortunately, this is just what appears to be going on.

The evolving mainstream corporate landscape of the internet is complicated by the rise of telecommunication giants such as Comcast, which is now serving as a major gatekeeper of the internet in its capacity as internet service provider (ISP) while simultaneously having controlling

DOI: 10.1057/9781137408211.0008

interest in the giant media empire, NBC Universal (including MSNBC). Further, at the time of this writing, Comcast is also in the process of purchasing Time Warner (subject to FCC approval), which would give it control of the CNN newsroom. As a result, Comcast has a conflict of interest in reporting the news about the status of cyber practices and policies, its own as well as that of the US government.

First, pursuant to Section 703(c) 5(B) of the FISA Amendments Act of 2008, telecommunication companies such as Comcast are required to help the federal government in its foreign intelligence gathering operations by providing "the Government forthwith all information, facilities, or assistance necessary to accomplish the acquisition authorized under such order in a manner that will protect the secrecy of the acquisition…." In exchange, Section 702(h) (3) of this law provides legal immunity against law suits. Hence, in its capacity as a news media outlet, it has a blatant conflict of interest in reporting news about the MWSN that implicates it as a co-facilitator. Indeed, transparency about its role in helping the NSA spy on its customers would not be good for business.

Second, such news coverage by Comcast would be met with government disapproval, thereby making unlikely federal support for mergers and acquisitions such as the current one with Time Warner, as well as other government perks such as tax breaks and Department of Defense contracts. Hence, it is not surprising that it appears to have consistently downplayed, in its media coverage, the seriousness of the NSA's mass surveillance program in light of the information leaked by Edward Snowden.[4]

Third, Comcast has been remiss in its coverage of its own attempt, as well as that of other telecoms such as Verizon and AT&T, to dismantle net neutrality—again not surprisingly due to its conflict of interest. These giant telecoms have historically sought to control the internet pipes by determining what traffic can flow through them. In 2010, in *Comcast Corp. v. FCC*, a federal appeals court ruled that the FCC lacked authority over Comcast's network management policies. In this case, Comcast challenged a ruling by the FCC that it could not slow traffic to a particular file sharing website, Bit Torrent,[5] and it sent a clear message that the FCC lacks the legal authority to regulate and protect access to the internet. However, the legal seeds had already been set for dismantling the FCC's ability to pass rules to safeguard net neutrality.

DOI: 10.1057/9781137408211.0008

The *Brand X* case

On June 27, 2005, in a 6 to 3 decision in *National Cable & Telecommunications Association vs. Brand X Internet Service,*[6] the US *Supreme Court* ruled that giant cable companies like Comcast and Verizon are not required to share their cables with other Internet Service Providers (ISPs).[7] This decision changed the classification of the internet from a "common carrier" to a private facility. A common carrier is a public utility that everyone can use such as a highway, railway, or phone line. Effectively, this ruling changed the status of the internet from a public (information) highway to a private roadway, wherein travelers are trespassers without the permission of the owner (ISPs such as Comcast).

The Court accepted the FCC's conclusion, reached in 2002 under the George W. Bush administration, that cable companies do not "offer" telecommunication services according to the meaning of the 1996 Telecommunication Act, which defines telecommunication purely in terms of transmission of information among or between users. According to the FCC, cable modem service is not a telecommunications offering because consumers always use high-speed wire transmission as a necessary part of other services like browsing the web and sending and receiving e-mail messages. The FCC maintained that these offerings are information services, which manipulate and transform data instead of merely transmitting them. Since the act only requires companies offering telecommunication services to share their lines with other ISPs, the "common carriage" requirement, the FCC concluded that cable companies are not common carriers.

However, the FCC's conceptual basis for classifying cable modem services as informational was groundless. Not even the FCC could deny that people use their cable modems to transmit information from one point to another over a wire, regardless of whatever else they use them for. The FCC's classification could not possibly have provided a reasonable interpretation of the 1996 Telecommunication Act since it was inconsistent with it. Section 706 (C) (1) of this act defines "advanced telecommunications capability," without regard to any transmission media or technology, as high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology. Since broadband cable internet service offers "advanced

DOI: 10.1057/9781137408211.0008

telecommunications capability," pursuant to this legal definition, it must, legally, be regarded as a telecommunications service.

To classify it as an information service is instead to treat high-speed broadband internet as though it were similar to cable services such as Fox News and CNN. These networks send information down a one-way pipe unlike internet transmissions, which, in contrast, are interactive, two-way exchanges resembling telephone conversations. The 9th Circuit Court of Appeals made this quite clear in its decision in *AT&T v. Portland*:

> Accessing Web pages, navigating the Web's hypertext links, corresponding via e-mail, and participating in live chat groups involve two-way communication and information exchange unmatched by the act of electing to receive a one-way transmission of cable or pay-per-view television programming. And unlike transmission of a cable television signal, communication with a Web site involves a series of connections involving two-way information exchange and storage, even when a user views seemingly static content. Thus, the communication concepts are distinct in both a practical and a technical sense. Surfing cable channels is one thing; surfing the Internet over a cable broadband connection is quite another.

The Supreme Court placed the entire weight of its argument on the FCC's claim that cable companies do not "offer" the telecommunication aspects of their services to consumers. Instead, they "offer end users information-service capabilities inextricably intertwined with data transport." Justice Scalia, writing the minority opinion in *Brand X*, analogized, you might as well say that a pizza service doesn't deliver pizzas because it also bakes them! Countering with its own analogy, the majority responded that you might as well say that a car dealership "offers" engines to consumers because it offers them cars. According to the majority's perspective, since the finished product is the car and not the engine, it makes more sense to say they offer consumers cars rather than engines. Similarly, it argued, the finished product that cable modem customers seek is internet services, such as being able to surf the net, not simply a transmission over a wire.

The Court's analogy, however, obscures the scope of consumer motivation by assuming that consumers have just one, broad perspective that defines what a company "offers" them. Realistically, consumers are also interested in the quality of the engines they get when they purchase cars (whether it is a V-8, V-6, 3.8 liter, 2.0 liter, etc.). From *this* consumer perspective, the car dealer is indeed "offering" engines to consumers (and

DOI: 10.1057/9781137408211.0008

bucket seats, antilock brakes, dual air bags, and all other components that determine the car's drivability, safety, comfort, design, durability, speed, and so forth). Similarly, from the perspective of average cable internet consumers who care about how reliable and fast the cable connection they purchase is, the cable company can, in a very practical sense, be said to be "offering" a telecommunication service. The FCC's distinction that cable modem data-transmission service is inextricably bound up with information services—just as an engine is inextricably bound up with a car—is, in this instance, a distinction without a difference.

In the end, the Court found that the Telecommunication Act was ambiguous. So why did it side with the FCC's interpretation even though there was clear, prior legal precedent for classifying cable modem services as telecommunication offerings?[8]

Citing its own decision in *Chevron U.S.A. Inc v. Natural Resources Defense Council,* the Court maintained that "if a statute is ambiguous, and if the implementing agency's construction is reasonable,…a federal court [is required] to accept the agency's construction of the statute, even if the agency's reading differs from what the court believes is the best statutory interpretation."[9] Therefore, it argued, since the FCC's construction is reasonable, it should determine what counts as "offering" telecommunication services.

However, the Court provided no legitimate legal, moral, or conceptual basis to think the FCC's construction was reasonable. If it considered consumer welfare to be paramount, it would have determined what was reasonable *for purposes of regulating competition of an internet that was designed to provide free, unfettered access to information in a democratic society*. Instead, the Court rested its substantive case on a specious argument advanced by the FCC:

> The Commission concluded that…broadband services should exist in a minimal regulatory environment that promotes investment and innovation in a competitive market.…This, the Commission reasoned, warranted treating cable companies unlike the facilities-based enhanced-service providers of the past.…We find nothing arbitrary about the Commission's providing a fresh analysis of the problem as applied to the cable industry, which it has never subjected to these rules. This is adequate rational justification for the Commission's conclusions.[10]

However, it is questionable that giving cable companies monopolies on broadband internet cable service will spawn more competition. Neither the Court nor the FCC provided empirical evidence that would justify

DOI: 10.1057/9781137408211.0008

this claim. In giving cable companies the authority to prevent other ISPs from operating on their cable lines, such deregulation portends less competition, not more, from independent ISPs.

By deferring to the FCC instead of exercising its own judicial discretion in determining what really was reasonable, the Court defeated the point of having an independent, ultimate court of appeals in the first place. This is to provide checks and balances on the activities of the other two branches of government, and to settle controversial, politically significant cases with far-reaching social consequences. Instead, it abandoned its constitutional charge to protect the First Amendment right of all Americans to freedom of speech in cyberspace from encroachment by big businesses acting in tandem with federal government.

The "pay for play" plan

Brand X set the legal stage for a further maneuver in challenging the free internet. As a consequence of the *Brand X* decision, the giant telecom and telephone companies like Comcast, Verizon, and AT&T had overcome a major hurdle in gaining control of internet content, namely control over the conduit of transmission. Now these telecommunication companies want to set up fast and slow lanes on the internet.

In 2011, the FCC, under the Obama administration, revamped its rules in an effort to safeguard net neutrality by requiring that telecoms maintain transparency in their policies, avoid discriminatory practices, and obtain from blocking lawful content, applications, and services.[11] However, instead of returning the internet to common carrier status, its ruling was based on Section 706 of the Communications Act, which toothlessly required the FCC to "encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans".[12]

In 2014, in *Verizon Communications Inc. v. FCC*, the Washington, D.C. Court of Appeals sent the 2011 rules back to the FCC concluding that it overstepped its authority by preventing broadband providers from slowing or blocking selected web traffic because, pursuant to its 2005 *Brand X* decision, the internet is not a common carrier.[13] As a result, Comcast, Verizon, et al. are now poised to take their power to slow and block internet traffic to the next level, that of establishing a "pay for play" internet system.[14]

DOI: 10.1057/9781137408211.0008

According to this "pay for play" plan, only large content providers, such as News Corp, Viacom, and Disney, among other internet power brokers, would be allowed optimum internet connectivity (bandwidth). This would mean that Americans logging onto the internet would be able to connect quickly and securely to the websites of these rich and powerful companies, while leaving the rest of the internet community spinning out in cyberspace, unable to get their messages heard. The net result would be the demise of internet neutrality. No longer would all of us, including most independent news websites, have an equal voice within a free and democratic forum. The news Americans would receive online would instead resemble that of the corporate news networks that presently monopolize the cable, radio, and broadcast news.[15]

With such a system in place, smaller independent media sites that are not motivated by bottom-line interests will be slowed or blocked, diminishing their voice on the net. With net neutrality dead in the waters, internet gate keeps like Comcast that are already working cooperatively with government will be able to slow down or block companies that are delivering content detrimental to government policy.

This includes news and information about NSA policies and practices in cyberspace. Were it not for news organizations such as *The Guardian* and *The Washington Post*, most of what we now know about the NSA's operation of the MWSN would still not be known, notwithstanding the Snowden disclosures. Indeed, books like the present one, which offer suggestions for change in these policies and practice, could not be written. Without legal protection of net neutrality, online sources that challenge government policies and practices in cyberspace could be slowed or blocked.

The FCC will, again, in the near future, be revising its net neutrality rules. But these rules will be stillborn if the decision it made under the George W. Bush administration in 2002 to declassify the internet as a common carrier is not reversed. The FCC has the power to do this, but it is a highly politically contested move because there are powerful telecoms with strong congressional lobbies who would like to set up a lucrative system of pay for play. These companies are a formidable obstacle for the prospects of a morally and legally acceptable decision by the FCC regarding its stance on net neutrality. But one thing that is not controversial is that, without net neutrality intact, there are serious obstacles to transparency about the policies and practices governing cyberspace. Major internet gatekeepers like Comcast, who have serious conflicts of

DOI: 10.1057/9781137408211.0008

interest, cannot be relied upon to deliver this news, on the one hand, and satisfy its bottom line corporate appetite, on the other hand, especially given its role as a co-facilitator with the NSA in operating the MWSN.

Internet search engines and democracy in cyberspace

It is not likely we will wake up one day and discover that the internet is no longer free and democratic. We may never find out. Like *Alice in Wonderland*, a false "reality" can be constructed that is internally consistent even if it bears little resemblance to truth. Thus, few Americans saw through it when the Bush administration fabricated foreign intelligence to justify a war in Iraq, sent an army of "military analysts" into the mainstream media to confirm these "facts," and "edited" the reports of embedded journalists to fit the war policy.

Relatively few Americans were able to realize that they were caught in a web of deception. But those Americans who did realize it were kept informed largely through web-based news organizations, including alternative media websites and news from foreign websites. For example, the American mainstream media censored the Downing Street memo story, which had been leaked by the *London Times.* The Downing Street memo contained the minutes of a July 22, 2002, meeting of British officials discussing the Bush administration's attempt to fabricate a justification for going to war in Iraq—"the intelligence and facts," it said, "were being fixed around the policy". Were it not for the internet, which enabled access to the British press and independent media sites that picked up the story and ran it, even fewer, if any, Americans would have even known about it.

But what if the search engines did not search for independent media and foreign websites? While the internet comprises a vast sea of information, a search engine is usually necessary to find what one is looking for. Consider how much less resourceful the net would be if one could only access sites for which one knew the URL. So, what if search engines like Google, Bing, and Yahoo did not permit Americans to readily access foreign and independent news sites?

The latter question brings to mind Google China, a version of the Google search engine that, from 2005 served the People's Republic of China and was moved from mainland China to Hong Kong in 2010. Originally built in compliance with the block list of the Chinese

DOI: 10.1057/9781137408211.0008

government, when searches for keywords prohibited by the Chinese government were conducted, it displayed the message, "In accordance with local laws, regulations and policies, part of the search result is not shown"; and in some cases, the search results were blocked entirely.

In June 2009, the Chinese government ordered Google to suspend foreign web site searches entirely on the basis of a report by a Chinese government-backed internet watchdog, which claimed that Google was "disseminating pornography and vulgar information" from abroad. Unfortunately, Google capitulated.[16]

In December 2009, Google became the target of a sophisticated cyber attack aimed at accessing the Gmail accounts of Chinese human rights activists. While Google did not officially accuse the Chinese government of sponsoring these attacks, the Chinese government denounced Google for insinuating as much. On the other hand, the popular alternative Chinese search engine, Baidu, enjoyed the support of the Chinese government, making it difficult for Google to compete. Moreover, Baidu continued to show large growth, nearly 40 percent in 2009, and by February 2010 had captured 60.9 percent of the Chinese market share compared to Google's 31.8 percent.[17] In fact, Google characterized its own revenues from the Chinese market as "insignificant".[18] Thus, it was not surprising that, in March, 2010, Google shut down its search engine in mainland China.

Citing its discomfort with the Chinese government's censorship requirement as its official reason for discontinuing its mainland service, Google took its operation to Hong Kong where it could operate outside Chinese law, including the Chinese government's censorship requirement. Google then redirected all Google.cn traffic within mainland China to Google.com.hk in Hong Kong. So, all Google searches launched from inside the Chinese mainland must now pass through the "Great Firewall" operated by the Chinese government. That is, all traffic redirected from Google.cn to its unfiltered search engine, Google.com.hk, is now filtered by the Chinese government.

It remains to be seen how Google will respond in the future to the changing tide of the Chinese market. However, Google's past history of complying with the Chinese government in building and maintaining a government-censored search engine is a disturbing reminder of how corporate power can yield to the authority holding the purse strings. Google was willing to censor websites according to the demands of the Chinese government. So, what reason could there be to think that, as the world's largest internet search engine provider, it would not also be willing, for profit, to build a "Great Firewall," around the rest of the world?

DOI: 10.1057/9781137408211.0008

Clearly, how supportive of internet freedom Google or its competitors will be depends largely on a cost-benefit analysis. Thus, while Google has defended net neutrality over a tiered system, this could be predicted based on its narrow, self-interested profit incentive. If a tiered system were implemented, Google would have to pay ISP's like Comcast for play; and since Google is a major player, its operating costs would significantly cut into its profit. On the other hand, if Google were to find out that it could attain a special exemption due to its essential role as a search engine operator, it is predictable that Google would capitulate to a "pay for play system". Accordingly, profitability is an extremely fragile basis upon which to ground net neutrality. Without government regulations, it is unreasonable to expect behemoth corporations like Google (or Microsoft/Bing or Yahoo) to choose not to "be evil".

Here, again, the solution is a set of net neutrality rules with legal teeth; that is, one supported by an internet that is recognized as a common carrier. That way, no website operator, large or small, could pay for play, thereby assuring equal access to by all to what is, and should remain, a free, public information highway.

Keeping the internet free and open is the only efficient way to assure that there will be enough diverse voices on the net to promote transparency about government policies and practice in cyberspace. The abnegation of net neutrality would turn a "global commons" into a private space where only invited guests are welcome to air their views. This would be to re-invent the internet as a closed network resembling a cable TV network, which would assuredly preempt transparency and the possibility of informed, global consent to policies and practices in cyberspace. Indeed, a "global commons" must be a "common carrier"; anything to the contrary of which is a dangerous contradiction.

As discussed in the next chapter, amid new evolving technologies that threaten to subvert human privacy and freedom of thought and expression in some of the most intimate ways imaginable, there is immediate and urgent need for government transparency about its policies and practices in cyberspace.

Notes

1 "Amid Criticism, Support for Media's 'Watchdog' Role Stands Out," Pew Research Center for the People and the Press, August 8, 2013. Accessed on

DOI: 10.1057/9781137408211.0008

June 19, 2014 from http://www.people-press.org/2013/08/08/amid-criticism-support-for-medias-watchdog-role-stands-out/.

"Internet Overtakes Newspapers as News Outlet," Pew Research Center for the People and the Press, December 23, 2008. Accessed on February 26, 2010, from http://people-press.org/report/479/internet-overtakes-newspapers-as-news-source.

2 Damon Poeter, "*Guardian, Washington Post* Get Pulitzers for NSA Reporting," *PC*, April 14, 2014. Accessed on June 19, 2014 from http://www.pcmag.com/article2/0,2817,2456559,00.asp.

3 Jeff Cohen, "Snowden Coverage: If U.S. Mass Media Were State-Controlled, Would They Look Any Different?" *Huffington Post*, June 26, 2013. Accessed on June 19, 2014 from http://www.huffingtonpost.com/jeff-cohen/snowden-media-coverage_b_3503971.html.

4 "Glenn Greenwald, *Guardian* Reporter, Blasts Media, MSBNC Over Edward Snowden Stories," *Huffington Post*, June 16, 2013. Accessed on June 19, 2014 from http://www.huffingtonpost.com/2013/07/16/glen-greenwald-media-edward-snowden-stories_n_3600016.html Josh Feldman, "Former MSNBC Producer Skewers Hosts For Pro-Obama Bias: 'Official Network Of The Obama White House,'" *Mediaite*, July 8, 2013. Accessed on June 19, 2014 from http://www.mediaite.com/tv/former-msnbc-producer-skewers-hosts-for-pro-obama-bias-official-network-of-the-obama-white-house/.

5 Cecilia Kang, "Court rules for Comcast over FCC in 'net neutrality' case," *Washington Post*, April 7, 2010. Accessed on June 19, 2014 from http://www.washingtonpost.com/wp-dyn/content/article/2010/04/06/AR2010040600742.html.

6 *National Cable & Telecommunications Assn. v. Brand X Internet Services* (04–277) 545 U.S. 967 (2005) 345 F.3d 1120, reversed and remanded. Accessed on June 19, 2014 from http://www.law.cornell.edu/supct/html/04–277.ZS.html.

7 This section is an updated and expanded version of Elliot D. Cohen, "Web of Deceit: How Internet Freedom Got the Federal Ax, and Why Corporate News Censored the Story," *Buzzflash.com*, July 18, 2005. Accessed on June 19, 2014 from http://billtotten.blogspot.com/2011/01/web-of-deceit.html.

8 *AT&T Corporation vs. Portland* US Ct of Appeals for 9th Circuit, No. 99–35609, June 6, 2000. Accessed on June 19, 2014, from http://www.fcc.gov/ogc/documents/opinions/2000/99–35609.html.

9 *Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, decided June 25, 1984. Accessed on June 19, 2014, from http://www.law.cornell.edu/supct/html/historics/USSC_CR_0467_0837_ZS.html.

10 *National Cable & Telecommunications Assn. v. Brand X Internet Services.*

11 John P. Mello, Jr, "FCC Publishes Net Neutrality Rules," *PC World*, September 23, 2011. Accessed on June 19, 2014 from http://www.pcworld.com/article/240505/fcc_publishes_net_neutrality_rules.html.

DOI: 10.1057/9781137408211.0008

12 "Elliot D. Cohen, "Help Stop Destruction of the Free Internet Now," *Truthdig*, December 26, 2010. Accessed on June 19, 2014 from http://www.truthdig.com/report/item/help_stop_destruction_of_the_free_internet_now_20101226#.

13 Marguerite Reardon, "Appeals court strikes down FCC's Net neutrality rules," *Cnet*, January 14, 2014. Accessed on June 19, 2014 from http://www.cnet.com/news/appeals-court-strikes-down-fccs-net-neutrality-rules/.

14 Tara Seals, "Net Neutrality Watch: The FCC Reconsiders Toll Road Deals," *TMCNet*, May 13, 2014. Accessed on June 19 from http://zone.tmcnet.com/topics/articles/378549-net-neutrality-watch-fcc-reconsiders-toll-road-deals.htm.

15 See Chapter 6.

16 Owen Fletcher, "China Orders Google to Suspend Foreign Site Searches," *PC World,* June 19, 2009. Accessed on June 19, 2014, from http://www.pcworld.com/businesscenter/article/166996/china_orders_google_to_suspend_foreign_site_searches.html?tk=rel_news.

17 Elliot D. Cohen, *Mass Surveillance and State Control: The Total Information Awareness Project.* New York: Palgrave Macmillan, 2010.

18 "Clash on the Great Firewall," *Wall Street Journal*, January 14, 2010. Accessed on June 19, 2014 from http://online.wsj.com/article/SB10001424052748704586504574655232889222954.html.

DOI: 10.1057/9781137408211.0008

6
Next Generation Technologies

Abstract: *This chapter discusses new technologies on the horizon that are poised to replace existing ones, which are light years more intrusive, such as brain-machine computer interface (BCI) technologies in combination with inference engines designed to predict terrorism plots and other prospective crimes. Such technology adds new meaning to "sinning in one's heart," wherein even thinking about committing a crime could make one a government target.*

Cohen, Elliot D. *Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.* New York: Palgrave Macmillan, 2014.
DOI: 10.1057/9781137408211.0009.

The Greek philosopher Heraclitus proclaimed that one cannot "step into the same river twice". This can be no truer than in the case of digital technologies. Anyone who can remember back to the early days of computer programming where it took numerous lines of code just to move a cursor, can appreciate the incredible power of later generations of programming languages. Each successive generation of programming builds on the prior generation, and thereby augments its power to accomplish tasks that we would not have imagined were in our grasp. Thus, those who worked on Tandy Corporation TRS-80 computers with 60 megabyte hard drives and 5 ¼ inch floppy disks in the1980s may not have imagined that they would today be carrying around flash drives with terabits of storage space and navigating their way through both cyber and physical space using their cell phones.

In 1965, Gordon Moore, co-founder of Intel, predicted that, the transistors on a chip will double every two years (so-called, "Moore's Law"). This two-year marker has been used to determine the tendency of electronic devices to obsolesce, and it has served as a standard in the semiconductor industry; thus serving as a catalyst to help turn the two-year prediction into a self-fulfilled prophesy. Whether or not this trend will, in fact, continue into the distant future at this voluminous rate is indeterminable, but it seems clear that the face of technology (and consequently of human existence) will change dramatically with each successive decade.

Unfortunately, there has been little concern among developers of new technologies for the ethical implications of bringing them to market. By the "invisible hand" of the Technological Imperative (whatever *can* be built *should* be), coupled with the insatiable appetite of giant corporations for maximizing profit, technology has historically tended to proceed with little or no ethical forethought. For example, the present trend in the production of genetically modified crops has proceeded with little concern for what effects the introduction of new strains of biogenetically engineered plants might have on the biosphere—including human life. Yet, where corporations have predicted bottom line gains, the investment in new technologies has predictably proceeded with little or no regard for the potential danger inherent in the production. In the case of communication technologies, there are presently some technologies on the horizon that portend serious implications for the future of global mass surveillance and ultimately for the survival of the free world. This chapter considers two such types of technology that can potentially work

DOI: 10.1057/9781137408211.0009

synergistically to destroy privacy and end human freedom and dignity: (1) brain-computer interfaces (BCI) and (2) inference engines designed to predict future events.

Brain-computer interface technologies

Brain-computer interfaces consist of an array of electrodes implanted in the brain or attached to the scalp; an encoding device for translating a (analog) brain signal into a (digital) computer signal, and conversely; and a wireless transceiver that can send the processed information to/from a (biological) brain from/to a computer. Intel is again at the forefront of the prospective industry, predicting that by 2020 users will surf the web and download information using only their brain waves.[1] According to Dean Pomerleau, an engineer at Carnegie Mellon University who leads Intel's brain-computer initiative, "Eventually people may be willing to be more committed … to brain implants. Imagine being able to surf the Web with the power of your thoughts,"[2] and he looks forward to a "two-way direct-brain interface" which would "revolutionize human experience".[3]

Less intrusive modes of research are also underway. For instance, at Samsung's Emerging Technology Lab researchers are experimenting with tablets that can be controlled by the user's brain when wearing a cap containing monitoring electrodes. And there is indication that many other major corporations are taking a serious interest in this new kind of communication technology.[4]

BCI technologies have also been successfully used to control robotic arms in paralyzed subjects just by thinking certain commands.[5] Such controls require encoding of analog electrical brain circuits into digital signals via a brain-computer interface consisting of an array of electrodes implanted in the cerebral cortex of a human subject connecting to a computer for processing. Strides have been made in miniaturizing this equipment and adapting it for wireless transmission. Companies such as BrainGate[6] have emerged which have partnered with major research universities such as Brown University, Columbia University, and MIT in advancing BCI technologies.

Some companies have already emerged such as Emotiv[7] and Neurosky,[8] which produce commercial BCI technologies that can be used for gaming activities involving moving objects or computer cursers by

DOI: 10.1057/9781137408211.0009

thinking about the movements. Some applications have been successfully used to provide biofeedback for individuals who have Attention Deficit Hyperactivity Disorder (ADHD).[9] These technologies, which detect electroencephalograph (EEG) measurements of electrical brain activity from the scalp have also been applied to help individuals with locked-in syndrome (conscious but totally or almost totally paralyzed and unable to otherwise communicate) to communicate using their thoughts.[10] The companies producing these BCI products license development kits to developers, who can, in turn, develop their own applications.[11]

These commercial grade BCIs are fitted with headsets that contain "dry" electrodes, which non-intrusively measure electrical charges off of the scalp. Since such measurement receives artifacts ("noise") from the surrounding environment, including electrical charges in muscles, the brain signal received from such superficial electrodes is generally of relatively poor quality in comparison to "wet" electrodes that are implanted in the brain. There is, therefore, presently a major advantage to using implanted electrodes. In any event, as the ability to refine the quality of the signal improves, it is likely that such products will become more and more prevalent.

But, clearly, the biggest challenge for mainstreaming BCI technologies for both medical and non-medical applications is the translation (encoding) of brain circuits into thoughts that express propositions with meaning. In fact, the Obama administration's Brain Research through Advancing Innovative Neurotechnologies (BRAIN) initiative is presently addressing the problem having budgeted $100 m for the current year and a proposed $200 m for FY 2015 for research aiming at recording and mapping brain circuits to "show how millions of brain cells interact".[12] In encoding these brain circuits, the chief obstacle to direct brain-to-brain communication will have been circumvented, making a reality the prospect of BCI technologies that facilitate wireless transfer of thoughts from brain to brain over a network.

For FY 2015, the Defense Advanced Research Projects Agency (DARPA), a federal agency operating under the US Department of Defense, plans to invest 80 million of the allowed budget on the BRAIN initiative. It aims to improve understanding of the brain by promoting "advancements in data handling, imaging, and advanced analytics".[13] One part of its mission, named "Restoring Active Memory (RAM)," aims at developing "memory prostheses" as part of its broader goal "to identify how memories are encoded in the brain during learning and skill

DOI: 10.1057/9781137408211.0009

acquisition, with the ultimate goal of accelerating warfighter recovery after traumatic brain injury".[14] The idea of creating a memory prosthesis is both intriguing and chilling. As an artificial memory storage facility for the human brain, its content can be manipulated by downloading data not originally part of the person's memory.

Another one of DARPA's programs, called "Systems-Based Neurotechnology for Emerging Therapies" (SUBNETS) seeks to build "closed-loop medical devices able to measure and modulate networks of neurons in research participants with intractable psychiatric illness and alleviate severe symptoms of diseases like post-traumatic stress disorder and major depression".[15] This effectively means that the Defense Department would be able to use BCI technologies to reconfigure or alter the thought processes of a human being. While it is a noble end to find ways of helping a person overcome PTSD and major depression, there is a difference between providing support for the person doing this on his own and directly manipulating the brain to alleviate the perceived problem. This amounts to mind control and it can be just as easily applied when a subject simply thinks differently than others, for example, disagrees with government policies.

DARPA's neuroscience technologies program also seeks to "create interfaces for handling and analyzing large datasets of neural data, allowing investigators to rapidly and transparently solve complex problems of computation, generate new models, and model the brain in multiple dimensions and spatiotemporal scales."[16] In this case, such datasets of neural data represent the thoughts of a human being, many of which may be private and personal. Tapping into people's minds as though they were computer databases is dehumanizing and violates their right of self-determination by treating them like objects (machines) in need of repair.

Another program of DARPA is its Prosthetic Hand Proprioception and Touch Interfaces (HAPTIX), aiming at development of "human-ready implantable electronic microsystems that monitor and modulate information in motor and sensory fibers of peripheral nerves, enabling amputees to achieve advanced and intuitive control and sensory functions with prosthetic limbs".[17] Such prosthetic limbs presuppose the ability to encode actionable commands issuing from the neural circuits in the brain. It also involves closed looped system that provides sensory feedback to the brain. It, therefore, comprises a two-way translational pathway between the brain and the external world. The BCI translates

DOI: 10.1057/9781137408211.0009

outgoing motor signals from the brain into actionable commands and feedback sensory input to the brain which is encoded to the brain (for example, force, pressure, touch, and temperature), which in turn provides output for the issuance and encoding of further commands. This research has, in fact, been ongoing as evidenced by a patent supported by DARPA, which application was filed in October 2001 and issued in April 2007.[18]

It is therefore evident that the current government initiatives, while having seemingly useful purposes (such as helping amputees and persons with mental health issues) also raise substantial ethical issues that are not presently being addressed. Under the socially acceptable rationale of helping people with physical and mental disabilities, the US Department of Defense can also implement very intrusive programs that fly in the face of respect for human rights. It is obvious that the US military foresees very important gains for military purposes in such research. Indeed, soldiers who do not suffer from depression or PTSD, or can be fitted with prostheses after their limbs have been blown up by a land mind can make superhuman soldiers capable of functioning in the most inhumane and abhorrent conditions. But what price is paid in reducing human beings to such fighting machines? The upshot is that such technologies cannot be dressed up to hide the serious and dangerous abuses they portend.

These abuses are not likely to be restricted to the military, although this would be egregious enough to warrant immediate attention. With the commercialization of BCI technologies, all human beings will eventually become vulnerable to invasion of their most private, inner thoughts, especially if the Intel prophesy of permanent BCI implants comes to pass.

This potential for abuse becomes even more salient when it considered what implications it has for the mass warrantless surveillance of millions of people, globally. With commercialization of BCI technologies moving forward, connecting human brains directly to the internet, a government in possession of the means to manipulate and control these brains through brain-internet interfaces, portends a chilling reality. Thus, while backdoor programs such as MUSCULAR currently operating beneath the radar of legal and judicial oversight vacuum up masses of data from emails, internet searches, chats, and telephone communications, the next stage in the foreseeable future is mass, global collection of the private thoughts of human beings. If this happens, then the idea of freedom and democracy will become empty concepts.

DOI: 10.1057/9781137408211.0009

Here is the idea of mass warrantless surveillance is taken to its logical conclusion. Where the government's goal is to acquire as much information as possible, without leaving any (informational) stone unturned, and where the infrastructure exists to tap into human minds directly on a global scale, there will be no reason to think that the government will do otherwise. This is why the ethical discussion needs to occur now, before the mass commercialization of BCI technologies takes root.

It is not likely that this technology will not be developed and mainstreamed. As discussed above, the seeds have already been planted and are beginning to sprout. Under the Technological Imperative, we can expect this trend to continue, and the dangers discussed herein will become manifest. Currently, very few are aware of the dangerous trend and even less are thinking about its implication for the MWSN. However, this is why greater transparency is of monumental importance if the most ethical outcome—given the inevitability of the mainstreaming of BCI technologies and its consequent implications for the MWSN—is to be attained. What this outcome is should largely be decided by a public, global forum of the sort discussed in Chapter 4. However, there are some parameters that appear to be within reason at this juncture as food for thought.

Just as it has been argued in this book that content filters need to be used to filter data collected pursuant to codes of law and ethics, the upcoming generation of commercially available BCI technologies also need to be appropriately equipped with filters to guard against government acquisition of private or confidential thought data and the use of malicious code or software to acquire, coax, or manipulate human subjects. Such filtration should allow as output only the data that the sender intends to release, and allow as input only the information that the receiver wishes to receive. Thus, such technology should be configured to create an environment where the sending and receiving of data is much the same as it currently is now without brain-to-brain communication.

Usually, new technology is developed first and then the ethical discussion occurs after the fact. However, the ethical problems posed by BCI technologies are too immediate to postpone discussion. It is not a question of whether but of when human brains interface directly with computers that are connected to the internet. When this happens, the masses will be vulnerable to cyber-attacks that have the potential to

DOI: 10.1057/9781137408211.0009

download spyware and other forms of malicious code into human brains that could tap into and decode memory circuits, add memories, or issue commands. Personal or confidential thoughts and ideas will be subject to exposure through unintentional uploading or coaxing by others. These are not the sort of ethical problems that can wait until after these technologies are mainstreamed. It is one thing for a person's hard drive to "crash" and quite another for a functional human brain to be "fried". BCI technologies must, therefore, be equipped from their very inception with a viable capacity to filter for unwanted or unauthorized content in both sending and receiving messages; and to filter for spyware, viruses, malware, and other malicious code.

Further, standard forms of virus protection is unacceptable in this context because such systems work by using a list of predefined definitions as matching criteria to check for malicious code. Thus, this list constantly requires updating and, therefore, does not offer a bullet proof shield to protect against such destructive code from potentially infecting millions of interfacing human brains. Accordingly, what is needed is a filter for a neural network environment that offers a bullet proof shield.

Future crimes technology

The Orwellian idea of the "thought police," as captured by the use of BCI technology in the MWSN to tap into brains directly, is chilling enough; but what happens if this vast network is also equipped with the capacity to make predictions about future events, including human actions? This idea of a machine with such predictive powers has been recently been depicted in the television series, *Person of Interest*; but, in fact, such a capacity (or alleged capacity) has already become a part of the analytic tools used by the NSA in hunting for terrorist plots and presumably other criminal activity.

Recorded Future, a start-up company based in Cambridge, Massachusetts, that claims patented algorithms to predict the future, has been supported by In-Q-Tel, the investment arm of the Central Intelligence Agency.[19] There is also evidence that the NSA has been working directly with Recorded Future since as early as August 2010.[20]

Recorded Future claims to "provides the tools to explore and analyze information from the web about past, present, and future events reported to be happening in the world."[21] It claims, "You can explore the past,

DOI: 10.1057/9781137408211.0009

present, and predicted future of almost anything in a matter of seconds. Our analysis tools facilitate deep investigation to better understand complex relationships, resulting in actionable insights."[22] According to Recorded Future, its search engine is focused on finding entities. "The main search field in our web user interface centers on entities: people, places, companies and more (think, nouns)."[23]

It says that it collects data from the internet, including from news publications, blogs, social media, financial data basis, government websites, and "much more".[24] Its so-called "Temporal Analytics" engine, it claims, "goes beyond search and explicit link analysis, and adds IMPLICIT link analysis. Our software seeks the "invisible links" between documents that talk about the same, or related, entities and events."[25] Drawing on a Platonic distinction between "canonical events" and "instances" of these events, it starts by collecting documents and identifying entities referenced in these documents. It then constructs the "idea world' of "canonical events involving these entities". Then it looks for instances of these events in time and space, which can include past, present, and future times and places. The system's "Temporal Analytics" utilizes a program called "Momentum", which looks for similarities and differences between the identified events and entities and determines their degree of relevance and credibility (based on sources) in relating them. It also looks for such things as human sentiment, for example, being hostile toward someone or something; and it uses statistical and artificial intelligence models to make predictions about the future.[26]

Philosophically, this program raises questions about human freedom. If human actions can truly be predicted in advance, then it is not clear how human beings can possess free will and thus act autonomously in making choices. On the other hand, if human beings do possess free will, then such a project is likely to produce a statistically significant number of false positives. In either case, the program portends potentially oppressive consequences for the masses.

From a practical perspective, the assumption of free will is generally a better idea than its denial. Referring to a malicious and brutal murder of a wife by her husband "whose continued existence bored him," William James astutely spells out one consequence of denying free will:

> The judgment of regret calls the murder bad. Calling a thing bad means, if it means anything at all, that the thing ought not to be, that something else ought to be in its stead. Determinism, in denying that anything else can be in its stead, virtually defines the universe as a place in which what ought to be

DOI: 10.1057/9781137408211.0009

> is impossible, in other words, as an organism whose constitution is afflicted with an incurable taint, an irremediable flaw.[27]

In other words, in a wholly deterministic world, there is no point to having regrets because having regrets assumes that things could have been otherwise than what they were. And this can lead to a sort of complacency with the status quo.

The application of Recorded Future technologies can proceed in two different ways. One way is to use the millions of records acquired by the NSA to make predictions about the future. Another approach is to provide the results gleaned from scanning public documents on the internet and then providing the results to the NSA to be used as strong selectors for the MWSN. In the first scenario, the NSA would be potentially subjecting virtually everyone worldwide to predictions about their future actions based on information that includes personal information such as internet searches, phone and email messages, bank information, and other nonpublic information. In the second scenario, only public information would be scanned.

It is not clear which of these approaches is currently being used by the NSA. Clearly, the first is the most objectionable since it uses private and personal information to make predictions about the future actions of people. In the second scenario, people still have discretion in deciding what to post to the internet such as social media sites like Facebook. In the first scenario, the subjects of such predictions are having their privacy compromised for purposes of making the predictions.

It is also one thing to commit a criminal act and another to be considering committing one. If Recorded Future technologies were used in the first case scenario in conjunction with commercially available BCI technologies connecting millions of people to the internet, then the personal and private thoughts of millions of people could be used as a basis to target them as potential criminals or terrorists. For example, a person who thinks hostile thoughts about a political leader whose policies he or she finds abhorrent, may now become a target for an assassination investigation. Recall that the "Temporal Analytics" engine also looks for human sentiment. Such implications bode poorly for an environment that supports freedom. As John Stuart Mill made clear, there is an important difference between merely thinking about something and acting. "If any one does an act hurtful to others," he says, "there is a *primâ facie* case for punishing him, by law, or, where legal penalties are not safely applicable, by general disapprobation." However, "the appropriate

DOI: 10.1057/9781137408211.0009

region of human liberty," he admonishes, consists of "the inward domain of consciousness; demanding liberty of conscience, in the most comprehensive sense; liberty of thought and feeling; absolute freedom of opinion and sentiment on all subjects, practical or speculative, scientific, moral, or theological."[28] A surveillance network operated by government that acquires the private written (email) and oral (phone) opinions and sentiments of the masses and subjects them to a predictive analysis for law enforcement purposes files in the fact of the foundations of a free society. So too does a criminal justice system that criminalizes crimes not yet committed. But, even worse, what if the private and confidential thoughts and ideas of millions of people worldwide were also fodder for such predictive analysis and criminal investigation?

Under such circumstances where "thought police" predict future crimes, there are likely to be some people who elect to go offline. However, with each successive generation we have already been becoming increasingly more and more comfortable living in a world without privacy protections. Indeed, several decades ago we would not have imagined that the current generation would be disclosing intricate details of their sex lives to the world on a social media website. It is, therefore, predictable that the majority of those who are now in diapers or yet unborn will eventually make the transition from a cyber culture in which personal communications such as email messages and phone conversations are being monitored to one in which personal thoughts and ideas sent and received over the internet are also being monitored.

In this new cyber culture of brain-to-brain communication, filtering technologies that place a bullet proof fire wall between personal and private thoughts and the MWSN must be an indelible part of the landscape. Programs such as Recorded Future, which attempt to predict future events, seriously increase the potential for oppression. If they are to be used at all, they should only be applied to information from public websites, thus limiting the system's potential for incrimination of individuals who have not committed crimes.

To be sure, these are not the only privacy protections that need to be pursued now in addressing the emerging technologies discussed herein. There is immediate need for full transparency as we move into a world in which such technologies threaten to undermine our existence as autonomous agents. We need to question the value of such technologies in the light of a fully informed understanding of their nature and potential benefits and risks. Unfortunately, these technologies are on a collision

DOI: 10.1057/9781137408211.0009

course with basic human rights such as that of self-determination, quite unbeknownst to the greater part of humanity.

Notes

1 Sharon Gaudin, "Intel: Chips in brains will control computers by 2020," *Computerworld*, November 19, 2009. Accessed on June 19, 2014 from http://www.computerworld.com/s/article/9141180/Intel_Chips_in_brains_will_control_computers_by_2020.
2 Ibid.
3 Pagan Kennedy, "The Cyborg in Us All," *New York Times*, September 14, 2011. Accessed on June 19 from http://www.nytimes.com/2011/09/18/magazine/the-cyborg-in-us-all.html?pagewanted=all.
4 Nick Bilton, "Disruptions: Brain Computer Interfaces Inch Closer to Mainstream," *New York Times*, April 28, 2013. Accessed on June 19, 2014 from http://bits.blogs.nytimes.com/2013/04/28/disruptions-no-words-no-gestures-just-your-brain-as-a-control-pad/?_php=true&_type=blogs&_r=0.
5 David Orenstein, "People with paralysis control robotic arms using brain-computer interface," Brown University, May 16, 2012. Accessed on June 19, 2014 from http://news.brown.edu/pressreleases/2012/05/braingate2.
6 "About Braingate," Braingate website. Accessed on June 19, 2014 from http://www.braingate.com/.
7 Home page, Emotiv website. Accessed on June 19, 2014 from http://emotiv.com/.
8 Home page, Neurosky website. Accessed on June 19, 2014 from http://neurosky.com/.
9 Choon Guan Lim et al, "A Brain-Computer Interface Based Attention Training Program for Treating Attention Deficit Hyperactivity Disorder," *PLOS One*, October 24, 2012. Accessed on June 19 from http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0046692.
10 Katia Moskvitch, "Real-life Jedi: Pushing the limits of mind control," BBC, October 10, 2011. Accessed on June 19, 2014 from http://www.bbc.co.uk/news/mobile/technology-15200386.
11 "Develop for EPOC," Emotive website. Accessed on June 19, 2014 from http://emotiv.com/epoc/develop.php.
12 John Markoff and James Goreman, "Obama to Unveil Initiative to Map the Human Brain," *New York Times*, April 2, 2013. Accessed on June 19, 2014 from http://www.nytimes.com/2013/04/02/science/obama-to-unveil-initiative-to-map-the-human-brain.html.
13 "Obama Administration Proposes Doubling Support for the BRAIN Initiative," White House Office of Science and Technology Policy, March

DOI: 10.1057/9781137408211.0009

2014. Accessed on June 19, 2014 from http://www.whitehouse.gov/sites/default/files/microsites/ostp/FY%202015%20BRAIN.pdf.

14 Ibid.

15 Ibid.

16 Ibid.

17 "Obama Administration Proposes Doubling Support for the BRAIN Initiative," White House Office of Science and Technology Policy, March 2014.

18 Nicolelis et al, *Closed loop brain machine interface*, US7, 209, 788, April 24, 2007.

19 Recorded Future – Big Tom Groenfeldt, "Data From The Internet Sees Into The Future," *Forbes*, November 29, 2011. Accessed on June 19, 2014 from http://www.forbes.com/sites/tomgroenfeldt/2011/11/29/recorded-future-big-data-from-the-internet-sees-into-the-future/2/.

20 National Security Agency, Accounts Receivable Check (ARC) entry for Recorded Futures, August 4, 2010. Accessed on June 19, 2014 from http://www.scribd.com/doc/53042529/NSA-s-ARC-Entry-For-Recorded-Future.

21 "What is Recorded Futures," Recorded Futures website. Accessed on June 19, 2014 from http://support.recordedfuture.com/knowledgebase/articles/164332-full-documentation-and-help.

22 "How Our Software Works," Recorded Futures website. Accessed on June 19, 2014 from https://www.recordedfuture.com/web-intelligence/.

23 "What is Recorded Futures," Recorded Futures website. Accessed on June 19, 2014 from http://support.recordedfuture.com/knowledgebase/articles/164332-full-documentation-and-help.

24 "How Our Software Works," Recorded Futures website.

25 "Patented Software: Temporal Analytics Engine," Recorded Futures website. Accessed on June 19, 2014 from https://www.recordedfuture.com/temporal-analytics-engine/.

26 Staffan Truve, Recorded Futures: A White Paper on Temporal Analytics. Accessed on June 19, 2014 from https://www.recordedfuture.com/assets/RF-White-Paper.pdf.

27 William James, "The Dilemma of Determinism," *The Will to Believe and Other Essays.* London: Longman, Green, & Co., 1912, pp. 161–2. Accessed on June 19, 2014 from http://www.gutenberg.org/files/26659/26659-h/26659-h.htm#P145.

28 John Stuart Mill, *On Liberty.* New York: The Walter Scott Publishing Co., Ltd., 1989, p. 20. Accessed on June 19, 2014 from http://www.gutenberg.org/files/34901/34901-h/34901-h.htm.

DOI: 10.1057/9781137408211.0009

7
The Technological Imperative

Abstract: *This chapter shows how legal change is being driven by this thrust toward the development of new surveillance technologies, even when there are low tech solutions to matters of national security. Accordingly, the chapter advocates greater attention to conventional investigative methods such as informants, community tips, and routine law enforcement, and the use of mass surveillance technologies constrained by conventional investigative methods, and court warrants pursuant to the Fourth Amendment. It also advocates the use of meta-technologies to stay the tendency of the Technological Imperative to undermine privacy, freedom, and dignity.*

Cohen, Elliot D. *Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.* New York: Palgrave Macmillan, 2014.
DOI: 10.1057/9781137408211.0010.

DOI: 10.1057/9781137408211.0010

The preceding chapter examined next generation surveillance technologies that can tap the human brain directly in order to extract information. Undoubtedly, the impetus to build such technology, even without careful ethical analysis, has multiple sources. This chapter examines several sources that tend to promote the "Technological Imperative" to invest huge sums of money in creating high tech solutions to what are sometimes low tech problems; and it provides suggestions for curbing the thrust of the Technological Imperative toward a more balanced approach to protecting national security.

National security and the technological imperative

The building and deployment of a mass warrantless surveillance network (MWSN) is routinely defended on grounds of national security, in particular, on preventing another terrorist attack like that which occurred on September 11, 2001. However, as discussed in Chapter 1, development of the MWSN began in the late 1960s well before the 9–11 attacks. At that time, the enemy was the Soviet Union, not al-Qaeda; and it is predictable that, in the future, there will be other enemies sought to defend against through the use of mass warrantless surveillance.

Unfortunately the contributions of the MWSN in defending against terrorist attacks have been severely limited, as noted by the January 2014 New American Foundation report, which was carefully examined in Chapter 3. The contributions made by Section 215 bulk domestic metadata phone collections program have been meager while the limited utility of the Section 702 UPSTREAM program was largely due to the use of conventional investigative means. Hence, it is not surprising that NSA analysts have attempted to put the system to work for other purposes such as collecting information on foreign politicians and corporations. After all, it is understandable that, after billions of dollars have been invested, there would be a strong (even if sometimes misguided) desire to show some dividends.

This is not to diminish the importance of national defense or the dedication of most NSA officers to national security. The problem lies in the unwavering conviction (or mindset) that the continual development, refinement, and deployment of surveillance technologies can and will provide the most efficient means to keep the people of the United States and its allies safe and secure. The 9–11 attacks were accordingly perceived

DOI: 10.1057/9781137408211.0010

as, not disconfirmation of the efficacy of such technology to promote national security, but instead a reason to invest even more money in the technology to make it better and better. The idea that a low tech solution might be more effective in stopping potential terrorist plots from happening than a high tech one appears to have been dismissed a priori, with little attempt to dispassionately weigh the empirical evidence.

The idea that high tech is "better" than low tech

Driven by this "Technological Imperative" to produce more high tech solutions rather than to invest in improved low tech solutions (for example, air marshals on every commercial aircraft and increased border patrol), there has been an unflinching desire to refine our high tech solutions with even "better" surveillance technologies. However, in this context, the practical import of the term "better" usually includes greater capacity to diminish privacy. Thus, it is now not enough to wire tap a particular individual based on a tip from an informant; rather, it is better to have a colossal system of mass surveillance armed with algorithms that can identify the alleged potential terrorist automatically without relying on informant tips; and since this does not really work (because it generates millions of false positives), the answer has been thought to lie in refinement of the technology, such as increasing the amount of storage space, creating more powerful inference engines, or adding the ability to make predictions about future events.

Technology as dictating legal change

With each successive refinement in the technology, there has also been a new demand to revise existing law. For example, K. A. Taipale, Executive Director of the Center for Advanced Studies in Science & Technology Policy, went on record at the Senate Select Committee on Intelligence Hearing on The Foreign Intelligence Surveillance Modernization Act of 2007, declaring that the 1978 FISA Act was outdated. This, he said, was because of changes in communication technologies such as "the development of automated monitoring techniques, including data mining and traffic analysis."[1] So, because we could collect, store, and analyze data en mass, it was thought necessary to deploy these technological means,

DOI: 10.1057/9781137408211.0010

no questions asked; and in order to do so "legally," we then needed to change the laws to permit it.

While globalization of communication networks did make it likely that switches containing both foreign and US communications traffic would be located in the US, this really did not require a change in law permitting the collecting of collateral US communications in order to acquire the foreign traffic; for there were still wire taps that could be performed by getting a FISA warrant, which needed only to specify the target and show probable cause that the target was a "foreign power," and not even that he or she was a potential terrorist. Moreover, under emergency conditions, the spying could begin 72 hours prior to the application for a warrant.[2] So, the legal change permitting mass warrantless spying was largely a case of the technology driving the law rather than a reasonable approach to serving national security. The lack of judicial oversight was not factored into the calculus. Yet, the US Constitution is founded on the need for a judicial check on executive and legislative authority.

The bottom line as a contributing factor

Further, while the technology has driven legal change, the bottom line appears to be a major contributing factor in driving technological change. High tech solutions are costly and Department of Defense contracts are very lucrative to those companies who are awarded these contracts. In the case of a major MWSN component of NSA's UPSTREAM program, a number of contractors appear to have been involved including SAIC, Raytheon Applied Signal Technology, and General Dynamics.[3] SAIC (Science Applications International Corporation) is not a newcomer to the development of the MWSN. In fact, in 2002, Hicks & Associates, a subsidiary of SAIC, was awarded a US$19 million contract from the Defense Advanced Research Projects Agency (DARPA) to build the Information Awareness Prototype System,[4] which was the earlier version of the capture, inspection and analysis system that was replaced by XKEYSCORE. In addition, such companies as SAIC have revolving doors with the Department of Defense. For example, in 1993, former Secretary of Defense Robert Gates, under George W. Bush and Barack Obama, sat on the Board of Directors at SAIC. Presently, former President of the Technical and Engineering Sector at SAIC is the Secretary of the Air Force.[5] Clearly, this tight association of high tech companies with the

DOI: 10.1057/9781137408211.0010

Pentagon to the beat of multi-million dollar national defense contracts adds fuel to the technological imperative.

Trying low tech means first

High tech solutions also often tend to be favored over low tech solutions even in cases where low tech solutions can work. In its wisdom, the framers of the 1978 FISA anticipated this tendency by requiring that an order for foreign surveillance may be written only if the information sought "cannot reasonably be obtained by conventional investigative techniques."[6] Thus, electronic surveillance was conceived to be a tool of last resort and could not be used where other investigative methods were available such as the use of informants, undercover operations, interviewing subjects, family member tips, traditional law enforcement methods, and CIA or FBI intelligence.

Section 703 of the 2008 FISA Amendments Act on "Certain acquisitions inside the United States targeting United States persons outside the United States" has also included the requirement that "such information cannot reasonably be obtained by normal investigative techniques". However, this requirement could reasonably be extended to *all* foreign intelligence gathering in order to offset the tendency to use high tech solutions where low tech solutions exist. In doing so, privacy violations would be substantially curtailed. Thus, instead of acquiring and parsing through collateral communications of millions of US persons in order to locate one or two foreign persons, more selective, "normal" investigative techniques could be used first when available. The ease of deploying the system when such other techniques are available may not seem worth it to the average observer when exposed to a public forum for consideration. The more likely response would be that, in order to preserve a sphere of privacy and respect for the dignity of persons, mass spying should be avoided wherever and whenever possible.

The role of mainstream media in feeding the technological imperative

Unfortunately, government does not presently invite such an alternative perspective. What is most audible to the ears of US persons is the

DOI: 10.1057/9781137408211.0010

unavoidable, although regrettable, *need* to give up some civil liberties in order to be safe. The expectation is made clear while the evidence to justify the sacrifice is not also made clear. Here, part of the problem, as discussed in Chapter 5, is the failure of mainstream media to do its due diligence in serving its constitutional charge as government watchdog. Thus, the people need to know about alternative national security approaches and how reliable they are (or might be) based on careful argument, evidence, and analysis. Platitudes such as "Freedom is not free" are vacuous when it is not clear how much freedom we really need to relinquish in the name of national security.

People also need to know about conflicts of interest that may militate against an honest appraisal of the situation. If a host on an MSNBC show such as Lawrence O'Donnell's *The Last Word* claims that mass warrantless surveillance is not a threat to privacy because the information collected is too voluminous to be threatening, then the network should also mention that, pursuant to the 2008 FISA Amendments Act, Comcast is required by the US government to work cooperatively with the NSA in conducting its MWSN, that it is paid for its services, and that it also is granted full legal immunity so that none of its customers can file a civil suit against it. When a medical journal publishes a study, any conflict of interest the researchers have related to the study must also be disclosed to the public. This is because bias is a human tendency, and the readership has a right to know. Analogously, when the media or its representatives have a conflict of interest this information needs to be publically disclosed.

There is always a tradeoff when the government spends money on one thing rather than other. Such priorities need to be made clear if the people are to give informed consent to a program of mass warrantless surveillance. Thus, how much money is the government spending on medical research? How much for education? How much for various social programs? How much for space exploration? And, of course, how much is being spent on surveillance technologies? Short of knowing what tradeoffs are being made in supporting and growing the MWSN, it is not possible to judge whether it is worth it. Yet, this is just what transparency requires.

Given the current state of the media, the quid pro quo between government and the corporate sector, including technology companies like SAIC and Raytheon, it is unlikely that the facts about the MWSN will be sufficiently aired to make a sound decision about the costs and benefits

DOI: 10.1057/9781137408211.0010

of the program. This book has attempted to add some momentum to this goal. But, the Technological Imperative piloted by a drive for corporate profit is unavoidably a fact of life that must be addressed by those who are affected by it. This includes the world community. Accordingly, in Chapter 4 it was proposed that the internet provide a world forum for addressing the challenges of the MWSN. The best scenario is for the US government (presently the Obama administration) to sponsor such a website. But if the government fails to do so, then the task may fall to the world community, especially while there is still a free and open internet to make one's voice heard.

The use of meta-technologies to curve the effects of the technological imperative

The steady expansion of technology is inevitable, but the manner in which it is managed is less settled, since meta-technologies can also arise that set practical and ethical limits on current and prospective technologies. Thus, antivirus and anti-malware software have become a part of most PC users and companies like Symantec and McAfee have made billions in this industry. By analogy, filtering technologies that can help preserve and protect privacy while permitting reasonable applications of surveillance can provide a lucrative opportunity for the commercial sector while serving the public good. Ethics does not have to be inconsistent with the corporate bottom line, although it can be, and often is.

Notes

1 K. A. Taipale, "Foreign Intelligence Surveillance Modernization: Reconciling Signals Intelligence Activity with Targeted Wiretapping," Senate Select Committee on Intelligence Hearing on The Foreign Intelligence Surveillance Modernization Act of 2007, May 1, 2007. Accessed on June 19, 2014 from http://www.fas.org/irp/congress/2007_hr/050107taipale.pdf.

2 Timothy B. Lee, "The new FISA compromise: it's worse than you think," *Ars Technica*, July 8, 2008. Accessed on June 19, 2014 from http://arstechnica.com/tech-policy/2008/07/fisa-compromise/.

3 Anthony Kimery, "EXCLUSIVE: NSA's X-KEYSCORE Does Far More than Just Siphon the Net, But is it Working?" *HSToday.US*, August 5, 2013. Accessed on June 19, 2014 from http://www.hstoday.us/blogs/the-kimery-report/blog/

DOI: 10.1057/9781137408211.0010

exclusive-nsas-x-keyscore-does-far-more-than-just-siphon-the-net-but-is-it-working/f419986393a64eec5bf2630815d3da3e.html.

4 Elliot D. Cohen, *Mass Surveillance and State Control: The Total Information Awareness Project.* New York: Palgrave Macmillan, 2010, pp. 68–9.

5 Deborah Lee James, Profile, Linkedin. Accessed on June 19, 2014 from http://www.linkedin.com/pub/deborah-lee-james/32/607/396.

6 U.S. Code 50 (1978) Section 104(a)(7)(c) http://www.gpo.gov/fdsys/pkg/STATUTE-92/pdf/STATUTE-92-Pg1783.pdf.

DOI: 10.1057/9781137408211.0010

8

Network Surveillance Regulations

Abstract: *This chapter provides Model Rules for Regulating Network Surveillance Policies and Practices. Derived from analyses presented in this book, these Rules provide a draft set of regulations on bulk network surveillance aiming at the protection and promotion of privacy, freedom, and dignity. It consists of a Preamble broaching primary issues of concern such as the clandestine context in which surveillance has been carried out, the overreach of technology at the expense of civil liberties, the lack of meta-technologies to curb this overreach, and the violation of constitutional rights such as freedom of the press and attorney-client privilege. The Rules address these, among other central problems, and address collections, the use of conventional investigative methods, transparency, "new wave" surveillance technologies, national security, and confidential communications.*

Cohen, Elliot D. *Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance.* New York: Palgrave Macmillan, 2014.
DOI: 10.1057/9781137408211.0011.

DOI: 10.1057/9781137408211.0011

A major purpose of this book has been to provide a set of regulations for stopping mass surveillance technologies from undermining privacy; for, without a domain of privacy, where people are free to think and act for themselves, there is no human dignity, and people are relegated to mere objects or things. Accordingly, this chapter presents a concise "code of ethics" directed toward preserving privacy, freedom, and dignity. Beginning with a Preamble that summarizes the problems and challenges raised by mass surveillance, it provides a new beginning in confronting them. As such, following the Preamble is a set of *Model Rules*, a draft proposal, responsive to these problems and challenges. These regulations consist of rules gleaned from the analyses provided throughout this book, and cover major areas of concern addressed in this book: (A) avoiding needless or excess collections, (B) constructive use of conventional methodologies, (C) increasing transparency, (D) constraining next generation technologies, (E) balancing national security against civil liberties, and (F) protection of confidential information.

Model rules for regulating network surveillance

Preamble

Contemporary surveillance technologies have made possible, on a global scale, the mass, warrantless surveillance of both cable and wireless communications. Research, development, and deployment of such technologies have proceeded largely beneath the radar of public awareness, evaluation, and informed consent. This clandestine environment, as well as the development and deployment of the technologies themselves, have been defended by government on the basis of promoting national security, in particular, guarding the homeland against assaults by foreign and homegrown terrorists and other perceived threats. However, little attention has been given by government and the corporate sector to the tendency of mass surveillance technologies to undermine human privacy, freedom, and dignity. Moreover, legal reform to protect these fundamental human values has tended to leave loopholes for continuing and expanding the status quo in acquiring, storing, and analyzing private human communications in cyberspace. Amid the changing face of communications technology (in particular, the emerging age of brain-computer interfaces and technologies that seek to predict future events and actions), the need is greater now than

DOI: 10.1057/9781137408211.0011

ever to stay the negative effects of such technologies on such fundamental human values.

Accordingly, this set of *Model Rules for Regulating Network Surveillance* offers standards that make a rational beginning in balancing the concern for national security against that of human privacy, freedom, and human dignity. These rules have been constructed from the perspective of what a global community of cyberspace users might agree to if afforded a democratic forum for creating such a set of rules. Of course, this is no substitute for an actual world forum but all reform begins with a draft proposal. This set of rules is offered as such a proposal.

The trend by government, in cooperation with the corporate sector, to develop technologies to monitor human communication has not been satisfactorily counterbalanced by meta-technologies that aim at preventing the first-order technologies from devouring basic human rights. Hence, these Rules attempt to effect such a counterbalancing with provisions for incorporating content filters into the practices and policies of network surveillance. Thus, the FIS Court has, in the past, largely accepted claimed technological limitations of network surveillance such as its incapacity to exclude millions of entirely domestic electronic communications in gathering foreign intelligence. Journalists conducting legitimate news gathering activities pursuant to the First Amendment have been monitored. Privileged communications such as between lawyers and their clients pursuant to the Sixth Amendment have also been collected. Meanwhile, the filtering capacity to limit such acquisitions exists, but a set of rules requiring the installment of content-specific filters at appropriate collection locations is lacking. Further, reliance on network surveillance, even when conventional investigative methods are available, places a needless strain on privacy while failing to adequately satisfy national security interests. Needed also are rules for balancing such alternative methods with network surveillance so that the latter does not needlessly intrude on privacy.

Transparency about policies and practice in cyberspace is, as well, an indispensible aspect of protecting privacy and ensuring freedom and human dignity. Yet conflicts of interest between government and telecommunication and news providers characterize the current climate in which mass surveillance is conducted and reported. Telecoms seek to dismantle the neutral architecture of the internet by offering a system of "pay for play" while news organizations owned by these companies censor the story. Government needs to be held accountable for its failure

DOI: 10.1057/9781137408211.0011

to regulate these conflicts through appropriate FCC net neutrality and media ownership rules. Other serious zones of secrecy add to this climate of institutional bias. The FIS Court has made its rulings in secrecy, with no external oversight that would ensure that it does not become a rubber stamp for the government. Establishing a system of oversight that does not itself engender a conflict of interest is still needed. Rules requiring transparency in debating such issues is an inherent part of freedom and democracy. The internet, in its present capacity as a neutral platform, can provide the facility for giving voice to the global community of cyberspace users. Within this free and authentic environment, there can be an honest assessment of the global threat posed by terrorism based on evidence and sound judgment absent the perceived need of any government to resort to mass manipulation, fear mongering, deception, and surveillance without informed consent.

Model Rules

A. Collections shall not include more data than what is useful or authorized for foreign intelligence gathering purposes.
   1. Data shall not be collected or maintained just in case it might become useful at a later time.
   2. Wholly domestic communications (communications wherein the sender and all intended recipients are located in the United States or its territories), and communications from US persons not in the US to recipients in the US, shall not be collected.
   3. If such data is collected accidentally, it shall be immediately deleted. For purposes of the latter, data "accidentally collected" does *not* include data collected with foreknowledge, including the foreseeable collection of wholly domestic communications, even if this data is collected incidental to the collection of foreign intelligence.
   4. Content filters shall be used, which are configured to filter for and automatically delete unauthorized data such as wholly domestic communications (see A.2).
   5. De-identification filters shall be used, which are configured to render sufficiently anonymous the identities of any US person or person residing in the US; whereby a court warrant, based

DOI: 10.1057/9781137408211.0011

on probable cause pursuant to the Fourth Amendment, is required to access the identity of any de-identified person.

6. Unauthorized attempts to access data shall be automatically recorded in an auditable log, which shall be checked periodically by an independent judicial authority (see also C.8).
7. Selection criteria for telephone call metadata searches should be limited to two hops from the target, and should utilize a specific selection term that uniquely describes a person, entity, or account.
8. Collections shall be for foreign intelligence gathering purposes only, and shall not target heads of state, diplomats, foreign corporations or their officials, or other individuals, groups, or organizations wherein such spying is not (empirically) justifiable for national defense purposes.

B. Conventional investigative methods shall guide and restrict the use of network surveillance.

1. The technologies of an electronic surveillance network shall be used only as a last resort where conventional investigative methods are not available, such as the use of informants, undercover operations, interviewing subjects, family member tips, traditional law enforcement methods, and CIA or FBI intelligence.
2. Algorithms such as those used in terrorism pattern matching searches, which produce a high incidence of false positives (e.g. hundreds of thousands), shall be used only in conjunction with conventional investigative methods (see B.1).
3. Technologies such as facial recognition, which have a high percentage of false positives (e.g. 20%) and/or significant biases (e.g. racial biases), shall not be considered actionable intelligence without further confirming evidence (e.g., FBI or CIA evidence).
4. All individuals, groups, or organizations not targeted based on intelligence obtained at least in part from conventional investigations or other equally reliable source shall not be used as strong selectors for searching the surveillance network.

C. Policies and practices of surveillance shall be transparent.

1. The evidentiary basis of a government policy or practice shall be made available to the public.

DOI: 10.1057/9781137408211.0011

2. Any policies or practices, such as a certain use of network surveillance to disrupt terrorist plots, which are not supported by available evidence, shall be discontinued.
3. A global forum for publicly discussing and debating policies and practices of surveillance shall be provided, and taken into account in formulating/implementing/discontinuing such policies and practices.
4. The internet shall remain a free and open platform for democratic dialog, debate, and informed judgment about surveillance policies and practices.
5. Cyberspace shall be conceived as a "global commons," for use by everyone (according to "common carriage"), not as private property.
6. Telecommunication companies that own the internet cables shall either not be permitted to be news and information providers, or their news rooms shall be carefully monitored by an ombudsman, ethics committee, or other independent authority to guard against the conflict of interest.
7. Telecommunication companies shall be forthright and provide full disclosure to their customers about their cooperation with government in conducting bulk surveillance.
8. An independent committee of at least five privacy experts, free of conflict of interest that could impede its judgment, shall oversee and counsel the FIS courts on matters potentially impacting privacy in cyberspace. The Committee shall report to Congress any FIS court decision that, in its collective judgment, violates these *Rules*.

D. Next generation surveillance technologies shall respect basic human rights and treat those subject to them as persons rather than as objects manipulated.

1. Technologies that connect human brains to the internet (BCIs) shall be equipped with content filters that prevent unauthorized collection of private information, or other malicious or harmful assaults on people's privacy (e.g. "downloading" of viruses or other malware into a human brain).
2. Search engines that attempt to predict the future shall not be employed in bulk surveillance networks to incriminate people who have not (yet) committed crimes.

DOI: 10.1057/9781137408211.0011

3. Such "future crimes" technologies shall either not be used at all for intelligence purposes or restricted to gathering information on public websites.

E. "National security" shall not be invoked by government to mislead or intimidate persons into surrendering their civil liberties.

1. Government shall not exaggerate the seriousness of a national security threat in order to justify changes in law governing bulk surveillance or make claims about the ability of such surveillance technologies to stop terrorist attacks, which cannot be empirically validated.
2. UPSTREAM programs that tap into the "back doors" of foreign telecommunication networks in order to collect masses of useless "intelligence" shall cease and desist or be appropriately regulated pursuant to appropriate law and the provisions of this code.
3. Nations have a right to hold in secret some aspects of their intelligence gathering operations where disclosure would honestly endanger lives and cause irreparable harm to the nation; however this exception shall not be understood to negate the rule of transparency and candor to those subject to bulk surveillance.
4. Media organizations shall acts as watchdogs of government in ensuring that government does not needlessly restrict freedom and democracy in cyberspace in the name of "national security".
5. The people aided by independent news organizations shall act as the Fifth Estate in assuring that corporate, mainstream news organizations meet their First Amendment charge of protecting the free flow of information in cyberspace without censorship.

F. Information legally protected as privileged or confidential shall be acquired by a government agency only if it is acquired pursuant to all applicable legal protections.

1. Prior to acquiring the telephone toll records of a media organization or its journalists, a government agency seeking the records shall disclose, in advance, its intention to acquire the records and negotiate with the media organization the terms of the acquisition.

DOI: 10.1057/9781137408211.0011

2. All electronic communications between attorneys and their clients, or within in any other professional relationship for which privileged communication exists, shall not be acquired by any government agency without a court order or the consent of the client.
3. Content filters shall be added to the surveillance network to assure that privileged electronic communications are not acquired.

The challenge ahead

The Obama administration has begun to address some of the above *Model Rules*, but, as shown in this book, there are many more miles to go before we sleep. The challenges raised by the ever-increasing range of surveillance technology tentacles of the massive network will not go away. As citizens of a world community of cyberspace users, we owe it to ourselves and our descendants to do our best to stop law and policy creep that permits technological advancement to erode our privacy, freedom, and dignity.

There is, clearly, an ongoing tendency of government to collect as much data as possible just in case it needs it. However, more deference needs to be paid to the balancing of the appetite for data and the civil liberties that are being sacrificed as a result. As fellow travelers who spend much of our lives traversing the "global commons" of cyberspace, we need to be as mindful of democracy and freedom there as in navigating through physical space. In this new technological frontier, we cannot afford to accept a dichotomy between cyber and physical space. The cyber world is inexplicably connected to the physical world. Thus, persons wrongfully targeted in cyberspace can loss their freedom and dignity in physical space, as when one is placed on a no-fly list or falsely detained. Further, spying on what one does in cyberspace can be just as degrading as spying on someone in physical space, such as when the NSA intercepts a sexually explicit chat. In plowing the fields of this new frontier, we must, therefore, be equally as mindful of our democratic mission as were our forefathers who came to the new world with ideas of privacy, freedom, and dignity. The future will be as we make it. The time for constructive change is now.

DOI: 10.1057/9781137408211.0011

Bibliography

Ackerman, Spencer and James Ball. "Optic Nerve: Millions of Yahoo webcam images intercepted by GCHQ," *The Guardian*, February 27, 2014. http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo (accessed on August 1, 2014).

American Bar Association (ABA), Model Rules of Professional Conduct. http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html (accessed on August 1, 2014).

Ars Technica. "What the NSA can do with "big data," June 11, 2013. http://arstechnica.com/information-technology/2013/06/what-the-nsa-can-do-with-big-data/ (accessed on August 1, 2014).

AT&T Corporation vs. Portland, US Ct of Appeals for 9th Circuit, No. 99–35609, June 6, 2000. http://www.fcc.gov/ogc/documents/opinions/2000/99–35609.html (accessed on August 1, 2014).

Ball, James. "NSA collects millions of text messages daily in 'untargeted' global sweep," *The Guardian*, January 16, 2014. http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep (accessed on August 1, 2014).

Bamford, James. *The Shadow Factory: The NSA from 9/11 to the Eavesdropping on America.* New York: Anchor Books, 2009.

BBC. "China employs two million microblog monitors state media say," October 2013. http://www.bbc.com/news/world-asia-china-24396957 (accessed on August 1, 2014).

DOI: 10.1057/9781137408211.0012

Bergen, Peter David Sterman, Emily Schneider, and Baily Cahall. "Do NSA's Bulk Surveillance Programs Stop Terrorists?" New America Foundation, January 2014. http://www.newamerica.net/sites/newamerica.net/files/policydocs/Bergen_NAF_NSA%20Surveillance_1_0_0.pdf (accessed on August 1, 2014).

Bewert. "All about NSA's and AT&T's Big Brother Machine, the Narus 6400," *Daily Kos*, April 7, 2006. http://www.dailykos.com/story/2006/04/08/200431/-All-About-NSA-s-and-AT-T-s-Big-Brother-Machine-the-Narus-6400 (accessed on August 1, 2014).

Bilton, Nick. "Disruptions: Brain Computer Interfaces Inch Closer to Mainstream," *New York Times*, April 28, 2013. http://bits.blogs.nytimes.com/2013/04/28/disruptions-no-words-no-gestures-just-your-brain-as-a-control-pad/?_php=true&_type=blogs&_r=0 (accessed on August 1, 2014).

Bloom, Jonathan. "Department Of Justice Issues Revised News Media Subpoena Policies," *Corporate Counsel*, October 2, 2013. http://www.metrocorpcounsel.com/articles/24621/department-justice-issues-revised-news-media-subpoena-policies (accessed on August 1, 2014).

Boadle, Anthony. "U.S. spied on presidents of Brazil, Mexico – Report," *Reuters*, September 2, 2013. http://in.reuters.com/article/2013/09/02/usa-security-brazil-mexico-surveillance-idINDEE98108U20130902 (accessed on August 1, 2014).

Bok, Sissela. *Lying: Moral Choice in Public and Private Life*, New York: Vintage Books, 1999.

Bowman, Christine. "Did the NYT Help Bush Win the 2004 Election by Sitting on the Illegal NSA Wiretapping Story at the Request of Jane Harman?" *Buzzflash*, April 30, 2009. http://www.truth-out.org/buzzflash/commentary/did-the-nyt-help-bush-win-the-2004-election-by-sitting-on-the-illegal-nsa-wiretapping-story-at-the-request-of-jane-harman/7135-did-the-nyt-help-bush-win-the-2004-election-by-sitting-on-the-illegal-nsa-wiretapping-story-at-the-request-of-jane-harman (accessed on August 1, 2014).

Braingate. http://www.braingate.com/ (accessed on August 1, 2014).

Cauley, Leslie. "NSA has massive database of Americans' phone calls," *USA Today*, May 11, 2006. http://usatoday30.usatoday.com/news/washington/2006–05-10-nsa_x.htm (accessed on August 1, 2014).

Chevron U.S.A., Inc. v. Natural Resources Defense Council, Inc., 467 U.S. 837, decided June 25, 1984. http://www.law.cornell.edu/supct/html/historics/USSC_CR_0467_0837_ZS.html (accessed on August 1, 2014).

DOI: 10.1057/9781137408211.0012

Choicepoint. "ChoicePoint AutoTrackXP®, and ChoicePoint Online." *ChoicePoint,* 2003. http://web.archive.org/web/20031218085618/www.choicepoint.com/business/public/cbi_1.html (accessed on August 1, 2014).

Clapper, James. "Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage," September 8, 2013. http://icontherecord.tumblr.com/post/60712026846/statement-by-director-of-national-intelligence (accessed on August 1, 2014).

Clifford, W. K. *The Ethics of Belief.* Amherst, NY: Prometheus Books, 1999.

CNN. "Bush defends NSA spying program," January 1, 2006. http://www.cnn.com/2006/POLITICS/01/01/nsa.spying/ (accessed on August 1, 2014).

Cohen, Elliot D. "Digging Deeper: Politico-Corporate Media Manipulation, Critical Thinking, and Democracy," *Project Censored* 2014, November 13, 2013. http://www.projectcensored.org/digging-deeper-politico-corporate-media-manipulation-critical-thinking-democracy/ (accessed on August 1, 2014).

——. "Help Stop Destruction of the Free Internet Now," *Truthdig*, December 26, 2010. http://www.truthdig.com/report/item/help_stop_destruction_of_the_free_internet_now_20101226# (accessed on August 1, 2014).

——. Mass *Surveillance and State Control: The Total Information Awareness Project.* New York: Palgrave Macmillan, 2010.

——. Neural Network Data Filtering and Monitoring Systems and Methods, US8516568B2, August 20, 2013.

——. *News Incorporated: Corporate Media Ownership and Its Threat to Democracy.* Amherst, NY: Prometheus Books, 2005. (accessed on August 1, 2014).

——. Offensive message interceptor for computers, US 5796948 A, August 18, 1998. http://www.google.com/patents/US5796948 (accessed on August 1, 2014).

——. "Web of Deceit: How Internet Freedom Got the Federal Ax, and Why Corporate News Censored the Story," *Buzzflash.com*, July 18, 2005. http://billtotten.blogspot.com/2011/01/web-of-deceit.html (accessed on August 1, 2014).

Cohen, Jeff. "Snowden Coverage: If U.S. Mass Media Were State-Controlled, Would They Look Any Different?" *Huffington Post*, June

DOI: 10.1057/9781137408211.0012

26, 2013. http://www.huffingtonpost.com/jeff-cohen/snowden-media-coverage_b_3503971.html (accessed on August 1, 2014).
Defense Advanced Research Projects Agency. "DARPA-BAA-09–55: Persistent Stare Exploitation and Analysis System (PerSEAS)." *FedBizOpps*, September 18, 2009. https://www.fbo.gov/index?s=opportunity&mode=form&id=f0144cfa4fb1ebbd4ac95f43a3a24540&tab=core&_cview=0 (accessed on August 1, 2014).
Dharmendra Modha. "IBM Seeks to Build the Computer of the Future Based on Insights from the Brain"(Video). YouTube. http://www.youtube.com/watch?v=1yoNOa-yjr8&feature=player_embedded (accessed on August 1, 2014).
Emotiv. http://emotiv.com/ (accessed on August 1, 2014).
Falconer, Bruce. "Defense Research Agency Seeks to Create Supersoldiers." *National Journal*, November 10, 2003. http://www.ratical.org/ratville/CAH/superSoldier.html (accessed on August 1, 2014).
Fantastico. "NSA Documents Show United States Spied Brazilian Oil Giant," August 9, 2013. http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html (accessed on August 1, 2014).
Federal Bureau of Investigation. *Next Generation Identification: System Requirements Document,* Version 4.4, October 1, 2010, p. 244 http://epic.org/foia/fbi/ngi/NGI-System-Requiremets.pdf (accessed on August 1, 2014).
Feldman, Josh. "Former MSNBC Producer Skewers Hosts For Pro-Obama Bias: 'Official Network of The Obama White House,'" *Mediaite*, July 8, 2013. http://www.mediaite.com/tv/former-msnbc-producer-skewers-hosts-for-pro-obama-bias-official-network-of-the-obama-white-house/ (accessed on August 1, 2014).
Fletcher, Owen. "China Orders Google to Suspend Foreign Site Searches," *PC World,* June 19, 2009. http://www.pcworld.com/businesscenter/article/166996/china_orders_google_to_suspend_foreign_site_searches.html?tk=rel_news (accessed on August 1, 2014).
Foreign Intelligence Surveillance Act Amendments Act of 2008, HR 6304 (2008). https://www.govtrack.us/congress/bills/110/hr6304/text (accessed on August 1, 2014).
Foreign Intelligence Surveillance Act Amendments Act Reauthorization Act of 2012, HR 5949 (2012). http://www.fas.org/sgp/crs/intel/R42725.pdf (accessed on August 1, 2014).

DOI: 10.1057/9781137408211.0012

Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95–511, 92 Stat. 1783 (1978). http://www.statewatch.org/news/2014/apr/usa-fisa-1978.pdf (accessed on August 1, 2014).

Foreign Intelligence Sureveillance Court, U.S. Memorandum Opinion, April 22, 2011, note 14. https://ia601003.us.archive.org/1/items/775440-fisc-opinion-unconstitutional-surveillance-0/775440-fisc-opinion-unconstitutional-surveillance-0.pdf (accessed on August 1, 2014).

Foreign Intelligence Surveillance Court, U.S. Amended Memorandum Opinion, October, 2011, note 7. https://www.aclu.org/files/assets/br13–09-primary-order.pdf (accessed on August 1, 2014).

Gallagher, Sean. "Building a panopticon: The evolution of the NSA's XKeyscore," *Ars Technica*, August 9, 2013. http://arstechnica.com/information-technology/2013/08/building-a-panopticon-the-evolution-of-the-nsas-xkeyscore/ (accessed on August 1, 2014).

——. "Quantum of pwnness: How NSA and GCHQ hacked OPEC and others," Arstechnica, November 12, 2013. http://arstechnica.com/information-technology/2013/11/quantum-of-pwnness-how-nsa-and-gchq-hacked-opec-and-others/ (accessed on August 1, 2014).

Gaudin, Sharon. "Intel: Chips in brains will control computers by 2020," *Computerworld*, November 19, 2009. http://www.computerworld.com/s/article/9141180/Intel_Chips_in_brains_will_control_computers_by_2020 (accessed on August 1, 2014).

Gellman, Barton and Ashkan Soltani. "NSA collects millions of e-mail address books globally," *Washington Post*, October 14, 2013.http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9–11e3–80c6–7e6dd8d22d8f_story.html (accessed on August 1, 2014).

——. "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say," *Washington Post*, October 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 (accessed on August 1, 2014).

——. "NSA tracking cellphone locations worldwide, Snowden documents show," December 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 (accessed on August 1, 2014).

DOI: 10.1057/9781137408211.0012

Gellman, Barton and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program," *Washington 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 (accessed on August 1, 2014).

Genachowski, Julius. "Preserving a Free and Open Internet: A Platform for Innovation, Opportunity, and Prosperity." *The Brookings Institution*, Washington DC, September 21, 2009. http://openinternet.gov/read-speech.html (accessed on August 1, 2014).

Givens, G. and, J. R. Beveridge, B. A. Draper, and D. Bolme. "A Statistical Assessment of Subject Factors in the PCA Recognition of Human Faces," Proceedings of the 2003 Conference on Computer Vision and Pattern Recognition Workshop, 8 (2003), p. 7.

Glanz, James and Andrew W. Lehren, "N.S.A. Spied on Allies, Aid Groups and Businesses," *New York Times*, December 20, 2013. http://www.nytimes.com/2013/12/21/world/nsa-dragnet-included-allies-aid-groups-and-business-elite.html?_r=0 (accessed on August 1, 2014).

Glanz, James, Jeff Larson, and Andrew W. Lehren. "Spy Agencies Tap Data Streaming From Phone Apps," *New York Times*, January 27, 2014. http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html?_r=0 (accessed on August 1, 2014).

Gorman, Siobhan and Evan Perez. "U.S. Collects Vast Data Trove," *Wall Street Journal*, June 7, 2013. http://online.wsj.com/news/articles/SB10001424127887324299104578529112289298922

Gorman, Siobhan and Jennifer Valentino-Devries. "New Details Show Broader NSA Surveillance Reach," *Wall Street Journal,* August 20, 2013. http://online.wsj.com/news/articles/SB10001424127887324108204579022874091732470 (accessed on August 1, 2014).

Gosztola, Kevin. "Supreme Court Declines to Hear Case That Would Have Challenged NSA Warrantless Surveillance of Lawyers," *The Dissenter*, March 4, 2014. http://dissenter.firedoglake.com/2014/03/04/supreme-court-declines-to-hear-case-that-would-have-challenged-nsa-surveillance-of-lawyers/ (accessed on August 1, 2014).

Greenwald, Glenn. "The Administration's pattern of deceit re: eavesdropping," *Unclaimed Territory*, January 31, 2006. http://glenngreenwald.blogspot.com/2006/01/administrations-pattern-of-deceit-re.html (accessed on August 1, 2014).

DOI: 10.1057/9781137408211.0012

——. "*Guardian* Reporter, Blasts Media, MSBNC Over Edward Snowden Stories," *Huffington Post*, June 16, 2013. http://www.huffingtonpost.com/2013/07/16/glen-greenwald-media-edward-snowden-stories_n_3600016.html (accessed on August 1, 2014).
——. "How the NSA Tampers with US-Made Internet Routers," *The Guardian*, May 12, 2014. http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden (accessed on August 1, 2014).
——. "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 (accessed on August 1, 2014).
——. "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 (accessed on August 1, 2014).
Groenfeldt, Tom. "Recorded Future – Big Data From The Internet Sees Into The Future," *Forbes*, November 29, 2011. http://www.forbes.com/sites/tomgroenfeldt/2011/11/29/recorded-future-big-data-from-the-internet-sees-into-the-future/2/ (accessed on August 1, 2014).
Harrell, L. Scott. "Locating Mobile Phones through Pinging and Triangulation," *Pursuit*, July 1, 2008. http://pursuitmag.com/locating-mobile-phones-through-pinging-and-triangulation/ (accessed on August 1, 2014).
Harris, Andrew. "Spy Agency Sought US Call Records Before 9–11, Lawyers say," *Bloomberg*, June 30, 2006. http://www.bloomberg.com/apps/news?pid=newsarchive&sid=abIVocO64zJE (accessed on August 1, 2014).
Harris, Shane. "TIA Lives on." *National Journal*, February 23, 2006. http://shaneharris.com/magazinestories/tia-lives-on/ (accessed on August 1, 2014).
——. *The Watchers: The Rise of America's Surveillance State*, Penguin Books, 2010.
Inspectors General of the Department of Defense, Office of, Department of Justice, et al., "Unclassified Report on the President's Surveillance Program," July 10, 2009. https://www.fas.org/irp/eprint/psp.pdf (accessed on August 1, 2014).
Isikoff, Michael. "NSA program stopped no terror attacks, says White House panel member," *NBC News*, December 20, 2013. http://

DOI: 10.1057/9781137408211.0012

investigations.nbcnews.com/_news/2013/12/20/21975158-nsa-program-stopped-no-terror-attacks-says-white-house-panel-member?lite (accessed on August 1, 2014).

James, William. "The Dilemma of Determinism," *The Will to Believe and Other Essays.* London: Longman, Green, & Co., 1912, pp. 161–162. http://www.gutenberg.org/files/26659/26659-h/26659-h.htm#P145 (accessed on August 1, 2014).

Jonas, Jeff and Jim Harper. "Effective Counterterrorism and the Limited Role of Predictive Data Mining," *Policy Analysis*, Cato Institute, No. 584, December 11, 2006. http://www.cato.org/sites/cato.org/files/pubs/pdf/pa584.pdf (accessed on August 1, 2014).

Kang, Cecilia. "Court rules for Comcast over FCC in 'net neutrality' case," *Washington Post*, April 7, 2010. http://www.washingtonpost.com/wpdyn/content/article/2010/04/06/AR2010040600742.html (accessed on August 1, 2014).

Kant, Immanuel. *Fundamental Principles of the Metaphysics of Morals*, 1785. Accessed on June 18, 2014 from http://www.gutenberg.org/ebooks/5682 (accessed on August 1, 2014).

——. *Perpetual Peace: A Philosophical Essay*, London: Swan Sonnenscheine, 1903. https://archive.org/details/perpetualpeaceaookantgoog (accessed on August 1, 2014).

Kravets, David. "Obama Sides with Bush in Spy Case." *Wired*, January 22, 2009. http://www.wired.com/threatlevel/2009/01/obama-sides-wit/ (accessed on August 1, 2014)

Kennedy, Pagan. "The Cyborg in Us All," *New York Times*, September 14, 2011. http://www.nytimes.com/2011/09/18/magazine/the-cyborg-in-us-all.html?pagewanted=all (accessed on August 1, 2014).

Kimery, Anthony. "EXCLUSIVE: NSA's X-KEYSCORE Does Far More than Just Siphon the 'Net, But is it Working?" HSToday.US, August 5, 2013. http://www.hstoday.us/blogs/the-kimery-report/blog/exclusive-nsas-x-keyscore-does-far-more-than-just-siphon-the-net-but-is-it-working/f419986393a64eec5bf2630815d3da3e.html (accessed on August 1, 2014).

Klein, Mark. Declaration of in Support Of Plaintiffs, Motion for Preliminary Injunction, *Hepting v. AT&T*, North District of California, June 8, 2006. https://www.eff.org/node/55051 (accessed on August 1, 2014).

——. "Domestic Surveillance and AT&T" (Video), *CSPAN*, November 2007. http://www.c-span.org/video/?201508–6/domestic-surveillance-att (accessed on August 1, 2014).

DOI: 10.1057/9781137408211.0012

——. *Wiring Up the Big Brother Machine… And Fighting It*, BookSurge Publishing, July 7, 2009.

Lee, Timothy B. "The new FISA compromise: it's worse than you think," *Ars Technica*, July 8, 2008. http://arstechnica.com/tech-policy/2008/07/fisa-compromise/ (accessed on August 1, 2014).

Lim, Choon Guan et al, "A Brain-Computer Interface Based Attention Training Program for Treating Attention Deficit Hyperactivity Disorder," *PLOS One*, October 24, 2012. http://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0046692 (accessed on August 1, 2014).

Machines Like Us. "IBM's global brain." October 30, 2008. http://machineslikeus.com/news/ibms-global-brain (accessed on August 1, 2014).

Markoff, John. "Chief Takes Over New Agency to Thwart Attacks on U.S.," *New York Times,* February 13, 2002. http://www.ratical.org/ratville/JFK/JohnJudge/linkscopy/PoindyToIAO.html (accessed on August 1, 2014).

Markoff , John and James Goreman, "Obama to Unveil Initiative to Map the Human Brain," *New York Times*, April 2, 2013. http://www.nytimes.com/2013/04/02/science/obama-to-unveil-initiative-to-map-the-human-brain.html (accessed on August 1, 2014).

Masnick, Mike. "How The NSA Pulls Off Man-In-The-Middle Attacks: With Help From The Telcos," *Techdirt*, October 4, 2013. http://www.techdirt.com/articles/20131004/10522324753/how-nsa-pulls-off-man-in-the-middle-attacks-with-help-telcos.shtml (accessed on August 1, 2014).

Mayes, Eric. "Google Partners with NSA, CIA on Intelligence Database." *Raw Story*, March 31, 2008. http://rawstory.com/news/2008/CIA_creates_miniGoogle_0331.html (accessed on August 1, 2014).

Mazzetti. Mark and Carl Hulse. "Inquiry by C.I.A. Affirms Spying on Senate Panel," *New York Times*, July 31, 2014. http://www.nytimes.com/2014/08/01/world/senate-intelligence-commitee-cia-interrogation-report.html?_r=0 (accessed on August 1, 2014).

Mello Jr, John P. "FCC Publishes Net Neutrality Rules," *PC World*, September 23, 2011. http://www.pcworld.com/article/240505/fcc_publishes_net_neutrality_rules.html (accessed on August 1, 2014).

Mick, Jason. "Tax and Spy: How the NSA Can Hack Any American, Stores Data 15 Years," *Daily Tech*, December 31, 2013. http://www.dailytech.com/Tax+and+Spy+How+the+NSA+Can+Hack+Any+American+Stores+Data+15+Years/article34010.htm (accessed on August 1, 2014).

DOI: 10.1057/9781137408211.0012

Mill, John Stuart. *On Liberty.* New York: The Walter Scott Publishing Co., Ltd., 1989, p. 20. http://www.gutenberg.org/files/34901/34901-h/34901-h.htm (accessed on August 1, 2014).

Moskvitch, Katia. "Real-life Jedi: Pushing the limits of mind control," BBC, October 10, 2011. http://www.bbc.co.uk/news/mobile/technology-15200386 (accessed on August 1, 2014).

Nakashima, Ellen. "FBI Prepares Vast Database of Biometrics." *Washington Post*, Saturday, December 22, 2007.

——. "Lockheed Secures Contract to Expand Biometric Database." *Washington Post*, Wednesday, February 13, 2008.

NARUS. NARUS nSYSTEM. http://narus.com/images/pdf/Narus_nSYSTEM_brochure.pdf (accessed on August 1, 2014).

National Cable & Telecommunications Assn. v. Brand X Internet Services (04–277) 545 U.S. 967 (2005) 345 F.3d 1120, reversed and remanded. http://www.law.cornell.edu/supct/html/04-277.ZS.html.

National Security Agency. Accounts Receivable Check (ARC) entry for Recorded Futures, August 4, 2010. http://www.scribd.com/doc/53042529/NSA-s-ARC-Entry-For-Recorded-Future.

——. *Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information pursuant to Section 702 of the Foreign Intelligence Surveillance Act as Amended*, October 31, 2011. https://www.aclu.org/files/assets/minimization_procedures_used_by_nsa_in_connection_with_fisa_sect_702.pdf (accessed on August 1, 2014).

——. "Slides about NSA's Upstream collection," Top Level Telecommunications, January 17, 2014. http://electrospaces.blogspot.com/2014/01/slides-about-nsas-UPSTREAM-collection.html (accessed on August 1, 2014).

——. "(U) Converged Analysis of Smartphone Devices: Identification/Processing/Tasking - All in a day's work [Slides]," May 2010. https://www.documentcloud.org/documents/1009660-nsa.html (accessed on August 1, 2014).

——. XKEYSCORE Slide, February 25, 2008. http://www.documentcloud.org/documents/743244-xkeyscore-slidedeck.html (accessed on August 1, 2014).

Neil Jr., "Spy Agency Taps into Undersea Cable," *ZDNet*, May 23, 2001. http://www.zdnet.com/news/spy-agency-taps-into-undersea-cable/115877 (accessed on August 1, 2014).

Neurosky. http://neurosky.com/ (accessed on August 1, 2014).

DOI: 10.1057/9781137408211.0012

New Statesman. "Somebody's Listening," August 12, 1988. http://cryptome.org/jya/echelon-dc.htm#echelon (accessed on August 1, 2014).

Nicolelis, Miguel A. L. et al. *Closed loop brain machine interface*, US7, 209, 788, April 24, 2007.

Obama, Barrack. "Speech on NSA reforms," *Washington Post*, January 17, 2014. http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3–9556-4a4bf7bcbd84_story.html (accessed on August 1, 2014).

——, Transcript of Remarks on NSA Controversy, *Wall Street Journal*, June 7, 2013. http://blogs.wsj.com/washwire/2013/06/07/transcript-what-obama-said-on-nsa-controversy/ (accessed on August 1, 2014).

Olmstead v. United States. 277 U.S. 438 (1928) 48 S. Ct. 564, Brandeis, J., Dissenting.

Orenstein, David. "People with paralysis control robotic arms using brain-computer interface," Brown University, May 16, 2012. http://news.brown.edu/pressreleases/2012/05/braingate2 (accessed on August 1, 2014).

Orwell, George. *1984*. London: Secker and Warburg, 1949. http://www.msxnet.org/orwell/print/1984.pdf (accessed on August 1, 2014).

Parenti, Michael. "Monopoly, Media, and Manipulation." In Elliot D. Cohen, ed., *News Incorporated: Corporate Media Ownership and Its Threat to Democracy*. Amherst, NY: Prometheus Books, 2005.

Parent, W. A. "Privacy, Morality, and the Law." In Elliot D. Cohen, ed., *Philosophical Issues in Journalism*. New York: Oxford University Press, 1992.

Peterson, Andrea. "How we know the NSA had access to internal Google and Yahoo cloud data," *Washington Post*, November 4, 2013. Retrieved on June 17, 2014 from http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/ (accessed on August 1, 2014).

Pew Research Center for the People and the Press. "Amid Criticism, Support for Media's 'Watchdog' Role Stands Out," August 8, 2013. http://www.people-press.org/2013/08/08/amid-criticism-support-for-medias-watchdog-role-stands-out/ (accessed on August 1, 2014).

——. "Internet Overtakes Newspapers as News Outlet," December 23, 2008. http://people-press.org/report/479/internet-overtakes-newspapers-as-news-source (accessed on August 1, 2014).

Phillips, Peter. "News Bias in the Associated Press." *Common Dreams*, July 22, 2006. http://www.commondreams.org/views06/0722–21.htm.

DOI: 10.1057/9781137408211.0012

Poeter, Damon. "*Guardian, Washington Post* Get Pulitzers for NSA Reporting," PC, April 14, 2014. http://www.pcmag.com/article2/0,2817,2456559,00.asp (accessed on August 1, 2014).

Poindexter, John and Robert Popp. "Countering Terrorism through Information and Privacy Protection Technologies," *Security and Privacy*, November/December 2006 (vol. 4 no. 6), pp. 18–27.

Poitras, Laura, Marcel Rosenbach and Holger Stark. " 'Follow the Money': NSA Monitors Financial World," *Spiegel International*, September 16, 2013. http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430–2.html (accessed on August 1, 2014).

PressTV. "Germans rally to condemn silence on US spy schemes," June 19, 2014. http://www.presstv.com/detail/2013/08/01/316708/germans-slam-silence-on-us-spy-schemes/ (accessed on August 1, 2014).

Project Censored. Independent Media Sources.http://www.projectcensored.org/independent-periodicals-webzines/ (accessed on August 1, 2014).

Project for the New American Century. *Rebuilding America's Defenses*, September 2000. http://www.informationclearinghouse.info/pdf/RebuildingAmericasDefenses.pdf (accessed on August 1, 2014).

——. "Statement of Principles,"1997. http://cf.linnbenton.edu/artcom/social_science/clarkd/upload/PNAC---statement%20of%20principles.pdf (accessed on August 1, 2014).

Protect America Act of 2007, S. 1927, 110th Cong. (2007). https://www.govtrack.us/congress/bills/110/s1927/text (accessed on August 1, 2014).

Pruitt, Gary B., President & CEO, Associated Press. Letter to Attorney General Eric Holder, May 13, 2013. http://www.ap.org/Images/Letter-to-Eric-Holder_tcm28–12896.pdf (accessed on August 1, 2014).

Reardon, Marguerite. "Appeals court strikes down FCC's Net neutrality rules," *Cnet*, January 14, 2014. http://www.cnet.com/news/appeals-court-strikes-down-fccs-net-neutrality-rules/ (accessed on August 1, 2014).

Recorded Futures. https://www.recordedfuture.com/ (accessed on August 1, 2014).

Reuters. "Proposed New FBI Rules Draw Civil Liberties Worries." *Reuters*, Friday, September 12, 2009. http://www.reuters.com/article/idUSN1247176820080912.

Risen, James and Eric Lichtblau. "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005. http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=print&_r=0 (accessed on August 1, 2014).

DOI: 10.1057/9781137408211.0012

Risen, James and Laura Poitras, "Spying by N.S.A. Ally Entangled U.S. Law Firm," *New York Times*, February 15, 2014. http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html?_r=3.

Rudolph, Alan. "Brain Machine Interfaces." DARPA. http://www.infowars.com/print/ps/brain_machine_darpa.htm (accessed on August 1, 2014).

SAIC. "Data Mining & Data Warehousing." SAIC, 2006. http://web.archive.org/web/20060209120733/www.saic.com/datamining/data-analysis.html (accessed on August 1, 2014).

Savage, Sam and Howard Wainer. "Until Proven Guilty: False Positives and the War on Terror: Bayesian Analysis." *Visual Revelations*. http://www-stat.wharton.upenn.edu/~hwainer/Readings/Wainer%20Savage.pdf (accessed on August 1, 2014).

Science Daily. "Seeing through Walls Engineers Develop Technology to See Through Walls." July 1, 2007. http://site.uspystore.com/blog3/2010/06/25/seeing-through-walls-engineers-develop-technology-to-see-through-walls/ (accessed on August 1, 2014).

Seals, Tara. "Net Neutrality Watch: The FCC Reconsiders Toll Road Deals," *TMCNet*, May 13, 2014. http://zone.tmcnet.com/topics/articles/378549-net-neutrality-watch-fcc-reconsiders-toll-road-deals.htm (accessed on August 1, 2014).

Snowden, Edward. Interview with Hubert Seipel, *NDR News*, January 26, 2014. http://www.commondreams.org/headline/2014/01/27–1 (accessed on August 1, 2014).

Society for Professional Journalism. *Code of Ethics*, http://www.spj.org/pdf/ethicscode.pdf (accessed on August 1, 2014).

Spiegel International. "Inside TAO: Documents Reveal Top NSA Hacking Unit," December 29, 2013. http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969–3.html (accessed on August 1, 2014).

Stanley, Jay and Barry Steinhardt. "Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society." American Civil Liberties Union, January http://www.aclu.org/FilesPDFs/aclu_report_bigger_monster_weaker_chains.pdf (accessed on August 1, 2014).

Svenssen, Peter. "Comcast Blocks Some Internet Traffic." *MSNBC*, October 19, 2007. http://www.msnbc.msn.com/id/21376597/ (accessed on August 1, 2014).

DOI: 10.1057/9781137408211.0012

Taipale, K. A. "Foreign Intelligence Surveillance Modernization: Reconciling Signals Intelligence Activity with Targeted Wiretapping," Senate Select Committee on Intelligence Hearing on The Foreign Intelligence Surveillance Modernization Act of 2007, May 1, 2007. http://www.fas.org/irp/congress/2007_hr/050107taipale.pdf (accessed on August 1, 2014).

Tavernise, Sabrina, Eric Schmitt, and Rick Gladstone. "Jetliner Explodes Over Ukraine; Struck by Missile, Officials Say," *New York Times*, July 17, 2014. http://www.nytimes.com/2014/07/18/world/europe/malaysian-airlines-plane-ukraine.html

Top Level Telecommunications. "BOUNDLESSINFORMANT only shows metadata," October 22, 2013. http://electrospaces.blogspot.com/2013/10/boundlessinformant-only-shows-metadata.html (accessed on August 1, 2014).

Tapper, Jake. "Obama's FISA Shift." *ABC News*, July 9, 2008. http://blogs.abcnews.com/politicalpunch/2008/07/obamas-fisa-shi.html (accessed on August 1, 2014).

Temple-Raston, Dina. "FISA Court Appears To Be Rubber Stamp For Government Requests," *NPR*, June 13, 2013. http://www.npr.org/2013/06/13/191226106/fisa-court-appears-to-be-rubberstamp-for-government-requests (accessed on August 1, 2014).

Truve, Staffan. "Recorded Futures: A White Paper on Temporal Analytics." https://www.recordedfuture.com/assets/RF-White-Paper.pdf (accessed on August 1, 2014).

U.S.A. Freedom Act, HR 3361, 113th Cong., 2d Session (2014). http://www.gpo.gov/fdsys/pkg/BILLS-113hr3361eh/pdf/BILLS-113hr3361eh.pdf (accessed on August 1, 2014).

U.S. Patriot Act, HR 3162, 107th Cong. (2001). http://www.law.cornell.edu/uscode/text/50/1861 (accessed on August 1, 2014).

Wall Street Journal. "Clash on the Great Firewall," January 14, 2010. http://online.wsj.com/article/SB10001424052748704586504574655232889222954.html (accessed on August 1, 2014).

Washington Post. "How the NSA's MUSCULAR program collects too much data from Yahoo and Google," October 30, 2013. http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/#document/p2/a129323 (accessed on August 1, 2014).

——. "NSA slides explain the PRISM data-collection program," June 6, 2013. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (accessed on August 1, 2014).

DOI: 10.1057/9781137408211.0012

——. "The NSA's problem? Too much data," October 15, 2013. http://apps.washingtonpost.com/g/page/world/the-nsas-overcollection-problem/517/ (accessed on August 1, 2014).

——. "One month, hundreds of millions of records collected," November 4, 2013. http://apps.washingtonpost.com/g/page/world/one-month-hundreds-of-millions-of-records-collected/554/ (accessed on August 1, 2014).

White House Office of Science and Technology Policy. "Obama Administration Proposes Doubling Support for the BRAIN Initiative," March 2014. http://www.whitehouse.gov/sites/default/files/microsites/ostp/FY%202015%20BRAIN.pdf (accessed on August 1, 2014).

Wired, "Wiretap Whistleblower's Account," April 2006. http://www.wired.com/science/discoveries/news/2006/04/70621 (accessed on August 1, 2014).

Zetter, Kim. "Is the NSA spying on U.S. Internet traffic?" *Salon*, June 21, 2006. http://www.salon.com/2006/06/21/att_nsa/ (accessed on August 1, 2014).

DOI: 10.1057/9781137408211.0012

Index

DOI: 10.1057/9781137408211.0013

DOI: 10.1057/9781137408211.0013

DOI: 10.1057/9781137408211.0013

DOI: 10.1057/9781137408211.0013