UiO : Faculty of Law
University of Oslo

Under Surveillance

Individual Privacy Rights in the New Era of Secret e-Surveillance

Candidate number: 9005

Submission deadline: 15 May 2014

Number of words: 17,953

Contents

Abbreviations and Acronyms

ARM	Activity, Recognition, and Monitoring
ACLU	American Civil Liberties Union
AUMF	Authorization for Use of Military Force
CALEA	Communications Assistance for Law Enforcement Act (1994)
CCPR	International Covenant on Civil and Political Rights
CIA	Central Intelligence Agency
CNE	Computer Network Exploitation
CAN	Computer Network Attack
CRS	Congressional Research Service
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DoD	Department of Defense
DOJ	Department of Justice
EA	Enterprise Architecture
ECPA	Electronic Communications Privacy Act
EELD	Evidence Extraction and Link Discovery
EFF	Electronic Frontier Foundation
EIC	Elements of the Intelligence Community
EO	Executive Order
EPIC	Electronic Information Privacy Center
EU	European Union
FAA	Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008
FBI	Federal Bureau of Investigation
FIP	Fair Information Practices
FISA	Foreign Intelligence Surveillance Act

FISC	Foreign Intelligence Surveillance Court
FOIA	Freedom of Information Act
FTC	Federal Trade Commission
GPS	Global Positioning System
HRC	Human Rights Committee
IRM	Information Resource Management
IITF	Information Infrastructure Task Force
NGO	Nongovernmental organization
NII	National Information Infrastructure
NCS	National Communications System
NSA	National Security Agency
NSC	National Security Council
NSS	National Security System
NYCLU	New York Civil Liberties Union
OECD	Organization for Economic Co-operation and Development
OMB	Office of Management and Budget
OPCL	Office of Privacy and Civil Liberties
PII	Personal Identifying Information
PRA	Paperwork Reduction Act of 1995
SSNA	Scalable Social Network Analysis
TAO	Tailored Access Operations
TI	Targeted Individuals
TIA	Total Information Awareness
UK	United Kingdom
UN	United Nations
UDHR	Universal Declaration of Human Rights
US	United States of America
USSS	United States SIGINT System
USSID 18	United States Signals Intelligence Directive 18
VCLT	Vienna Convention on the Law of Treaties

VoIP	Voice Over IP
VPN	Virtual Private Networks

INTRODUCTION

SECRET MASS AND TARGETED ELECTRONIC SURVEILLANCE have accelerated viral concerns for privacy rights worldwide. Dragnet surveillance schemes are argued as a necessity for national security. More or less, this has become a standard reasoning used for backing all-encompassing forms of surveillance to combat the "global war on terrorism." Edward Snowden's leaks, however, revealed that not only American citizens, but also "citizens of the world" have been intellectually detained and hooded in darkness by the National Security Agency's (NSA) active surveillance programs into the "private sphere" of personal lives by collecting massive loads of data electronically, and then storing it in databases, long-term.

These stealthy measures supposedly supplement retroactive surveillance to prevent and prosecute criminal acts of terrorism. However, secret e-surveillance disclosures have unmasked some other potentially wider and deeper concerns for humanity and the rights movement guard against. Therefore, this thesis examines the legal debate from multiple perspectives and poses the question – Is the U.S. Federal government, NSA, other elements of the intelligence community, law enforcement officials and private corporations or third-parties violating individual privacy rights inside America and abroad through operating dragnet surveillance schemes?

Americans typically search for privacy protection in the textual scope of interpretations under the *United States Constitution*. Throughout the course of American common-law history, it has been contested that the *right to privacy* is not explicitly stated, however, there are thought to be "zones of privacy" in the *Bill of Rights*. In other words, practical lines have been established by law in order to respect the right to privacy that the government is not legally permitted to pass.

One essential source of applicable US constitutional law that draws a line for privacy is the Fourth Amendment, as it stipulates:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[1]

Additional amendments are linked in this contentious debate as modern technologies evolve. For instance, the legality of using a Global Positioning System (GPS) locator on vehicles,[2] accessing cell phone data at time of arrest,[3] and using thermal-imaging devices to scan a residence,[4] and more. Some contemplate the rise of "administrative regulatory schemes" designed to allegedly protect persons from international terrorism, while also simultaneously encroaching on people's privacy rights, as prescribed by law.

The *Universal Declaration of Human Rights* (UDHR) claims under Article 1 "*All* human beings are born *free* and equal in dignity and rights."[5] Its preamble accentuates that rights are *inalienable*, which in essence, implies that these rights cannot be taken away. This individual sphere for an "inherent dignity, and equal and inalienable rights is considered the foundation for freedom, justice and peace in the world," by which all nations are under a legal obligation "to respect, to protect and to ensure."[6]*Yet still*, a new world of aggressive computerized conditions is being encrypted in cyberspace, silently. And former admirable aspirations to save succeeding generations from the scourge of war are apparently backed by covert operations that militarize the Internet. UDHR Article 12 reinforced verbatim by the *International Covenant of Civil and Political Rights* (CCPR) article 17, states distinctly, "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor or reputation. Everyone has a right to the protection of the law against such interference or attacks.[7]

---

[1] U.S. Constitution, *Fourth Amendment*, http://www.law.cornell.edu/constitution/fourth_amendment
[2] *United States v. Jones*, 132 S. Ct. 945, 565 U.S. (2012).
[3] *Riley v. California*, No. 13-132 S. Ct., U.S. (2014).
[4] *Kyllo v. United States*, 533 U.S. 27, 34, 40 (2001).
[5] UN General Assembly, *Universal Declaration of Human Rights* (UDHR), 10 December 1948, 217 A (III), Article 1.
[6] *See* UNDR, preamble.
[7] UDHR, Article 12; CCPR Article 17.

However, Snowden testifies that *by design* it is no longer in the hands of trustworthy governments or pronounced protections under constitutional rights or international human rights; only encryption offers privacy in the "defense against the dark arts in the digital realm."[8]

In the wake of 11 September 2001, privacy protection laws have been reconsidered as global counterterrorism and counterintelligence measures increasingly intrude and erode the "private sphere." Relevantly noted, the 'concept of privacy' ought to be weighed as a core value, as it can be observed as a fundamental right by which other rights are made possible. Several important cases shall be used to demonstrate how this dynamic concept of privacy comes alive in a courtroom, what value it holds in essence, how it can be manipulated, and finally, why defending it is increasingly vital. This particular interface and mode of interoperability are now perceived as a new legal battle to restore human dignity, online.

It is affirmed that fundamental human rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations or may not be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of these rights and freedoms.[9] 'This thesis argues, however, that broad interpretations of counterterrorism and counterintelligence instruments, as currently practiced/adopted by the US administration, stretch beyond what US and international law allow and what is necessary to counter terrorist activities.' It has been asserted, "there is now a significant gap between what most Americans *think* the law allows and what the government secretly *claims* the law allows."[10] Strikingly, the gap is now expanding worldwide as inescapable uncertainties trigger alarms on the domestic and international level.

---

[8] The Guardian, Edward Snowden Discusses NSA Leaks at SXSW: 'I Would Do It Again, by Jon Swaine and Jemina Kiss, (17 March 2014), available at: https://www.transcend.org/tms/2014/03/edward-snowden-discusses-nsa-leaks-at-sxsw-i-would-do-it-again/

[9] *See* UNDR, Article 30.

[10] The Guardian, Glenn Greenwald, NSA collecting phone records of millions of Verizon customers daily, available at: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

In light of these above challenges, chapter one considers the historical value of American privacy. It studies philosophical, socio-political, ethical and legal origins as enshrined in the *Declaration of Independence*, the *Constitution of the United States* and the *Bill of Rights*. Do earlier customs and cultural heritages expose evidence for privacy as core human value? Where are these historical signposts?

Influenced by scholarly endeavors, narrative analysis and case law, chapter one and two address privacy as a concept and analyzes cases that accentuate positions drawing a line in by which the government should not cross. Enhanced by theories of *ius naturale*, common and constitutional law, in conjunction with theories of interpretation, *sine qua non* principles are considered for "evincing a design" to discern the legitimate form and function for any government in a democratic society, as deemed necessary to maintain a valid "social contract."

Constituents of *privacy* as a legal definition shall also be weighed to enhance clarity and reason its meaning, its role, its function and its value. What does privacy mean? What are essential principles of privacy law? Do these principles change for different actors, as for example, between private corporations and federal agencies? What value does privacy offer to the human individual and society as a whole? Does privacy seem to evolve or de-evolve across time? Is the current law and practice in step with modern information technologies?

Chapter three considers NSA and some divergent allegations stirred by a global war on terror. In a post 9/11 world it examines and discusses the legality of executive authorizations, new legislation, technologies, and surveillance schemes among the intelligence community to combat war in cyberspace, on the homeland, and abroad. What information has been leaked on mass surveillance programs, technological capabilities, capacities and spying activities? Who and what law permits the NSA to collect, analyze, disseminate, stockpile, and possibly use or misuse personal information on foreign persons and more recently, all U.S. citizens? What data are collected? How do various "boots and shoes on the ground" use it? Are various actors violating privacy rights on the US domestic level and perhaps, the international level? What other human rights and freedom might also be impacted?

Chapter four considers the universal human right to privacy. Enriched from various perspectives by associated actors from the United Nations, UN Special Rapporteurs, victims of unwarranted surveillance, and other relevant actors, it contemplates the legality and interconnected concerns of mass communications surveillance for the international human rights regime and its implications for a free and democratic world society.

Based on expert valuations and testimonies across several fields of study, authoritative sources of law, literature review, media studies, and discourse analysis as regards e-surveillance into the "private sphere" whether it be from flipped-on webcams, turned-on audio devices to record private conversations (from personal effects), malware or tracing devices that seemingly "never let you alone," chapter five offers a conclusion. Arguably, is dragnet e-surveillance violating privacy rights?

1 HISTORICAL PERSPECTIVE

> A constitution is a set of fundamental norms about the organization and performance of governmental functions in a community, and the relationship between the government and those who are governed. It shall, in principle for an indefinite period of time, provide a legal frame as well as guiding principles for the political life of a community. It is binding on governmental institutions and the members of the community alike, and it is paramount (or supreme) law in the sense that law of lower rank *must* conform to the constitutional rules.[11]

The US *Constitution* offers no explicit right to privacy. Originalist styles of interpretation call on judges to give words in the constitution the 'original public meaning' held when the constitution or its relevant amendments were enacted into law. As such, Judge Robert H.

[11] Bardo Fassbender, *Ruling the World? Constitutionalism, International Law, and Global Governance*, "Ch 5. Rediscovering a Forgotten Constitution: Notes on the Place of the UN Charter in the International Legal Order", Cambridge University Press, (2009:139). (emphasis added).

Bork held "there is no right to privacy." [12] However, Bork's narrow interpretation has been rigorously dissented since.

In practice, supplementary interpretative theories and case law have broadened Bork's view. As many differences in opinion aim to offer the provisions of the *Bill of Rights* a sense of meaning, form and function. Jefferson assured that if the government failed to guarantee these fundamental rights that it was designed and entrusted to protect, the *Declaration of Independence* affirms, "That to secure these rights, Governments are instituted among Men, deriving their just powers from the *consent of the governed*." [13]

Considering that core of "original public meaning,"Akhil Reed Amar and Les Adams asked, what is the *freedom* that the Founding Fathers were concerned? And rightly so, there are several forms of freedom! Freedom from psychological or physical constraint, such as slavery and imprisonment, freedom from want, freedom to move, freedom to think, freedom to act, freedom to dream, and so on."[14] Patrick Henry understood it is "*political freedom*, the right of citizens to exercise free will in conformity with and under protection of the rule of law."[15]

Yet still, what is required to realize a true sense of political freedom and an independent state of "personal free will?" Is 'privacy' an important element in this legal formula? Does the supreme law of the land designate particular "zones of privacy?"

1.1 The Supreme Law of the Land

The US government has always been a staunch champion of privacy. In securing zones of privacy, the First Amendment stipulates, "Congress shall make *no law* respecting an estab-

[12] Steven G. Calabresi & Lauren Pope, Judge Robert H. Bork and Constitutional Change: *An Essay on Ollman v Evans, 80 U Chi L Rev Dialogue 155.*
[13] U.S. Declaration of Independece (1776)(emphasis added).
[14] Akhil Reed Amar and Les Adam, *The Bill of Rights Primer, A Citizen's Guidebook to the American Bill of Rights*, Skyhorse Publishing, New York, (2013:1).
[15] Ibid., p.2 (emphasis added).

lishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances."[16] In 1972, Justice Douglas held in *Laird v. Tattum*:

> The First Amendment was designed to allow rebellion to remain as our heritage. The Constitution was designed to keep government off the backs of the people. The Bill of Rights was added to keep precincts of belief and expression, of the press, of political and social activities, free from surveillance. The Bill of Rights was designed to keep agents of government and official eavesdroppers away from assemblies of people.[17]

Protecting security of person in the privacy of an *individual's home*, the Third Amendment states, "No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law."[18] The home is traditionally respected as a *zone of privacy*.

To safeguard privacy there are two provisions consistently mentioned. Foremost, the Fourth Amendment protects the right of the people to be secure in their '*persons*, *houses*, *papers*, and *effects*, against unreasonable searches and seizures. This provision protects a right to privacy and freedom from arbitrary invasions."[19] And it also declares zones of privacy as *persons*, *houses*, *papers*, and *effects*.

To avoid arbitrary forms of invasion there is a normative parameter in criminal cases to issue a *warrant* or a "*writ*." A warrant "permits law enforcement personnel to take some action, such as make an arrest, search a location, or seize some piece of property."[20] However, certain "watchwords and catchphrases" rise as the topic of mass and targeted e-surveillance comes into scope.

---

[16] U.S. Constitution, *First Amendment*, available at: http://www.law.cornell.edu/constitution/first_amendment (emphasis added).
[17] Justice William O. Douglas, Dissenting Opinion, (with Justice Thurgood Marshall concurring) in *Laird v. Tattum*, 408 U.S. 1 (1972).
[18] U.S. Constitution, *Third Amendment*, available at: http://www.law.cornell.edu/constitution/third_amendment (emphasis added).
[19] See Fourth Amendment: An Overview, available at: http://www.law.cornell.edu/wex/fourth_amendment
[20] See legal defintion, warant, available at: http://www.law.cornell.edu/wex/warrant (emphasis added).

One catchphrase is a *reasonable expectation of privacy*. This implies, "To invoke protection under the Fourth Amendment against unreasonable searches and seizures, an individual must have a "reasonable expectation of privacy" regarding the location subject to the search or the item seized.[21]

Another is *unreasonable search and seizure.* This implies that, "search and seizure by a law enforcement officer *without* a search warrant and without *probable cause* to believe that *evidence* of a crime is present. This type of search or seizure is unconstitutional under the Fourth Amendment (applied to the states by the Fourteenth Amendment). The *fruit of the poisonous tree* doctrine holds that "evidence gathered with the assistance of illegally obtained information must be excluded from trial."[22]

The other provision oft mentioned to protect the '*privacy of personal information'* is to prevent *self-incrimination* in criminal cases. The Fifth Amendment states, "No person shall be held to answer for a capital, or otherwise infamous crime, … nor shall be compelled in any criminal case to be a witness against himself…."

> 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 recognition of the significance of man's spiritual nature, his feelings, and his intellect.[23]

There is a personal and sacred sense of autonomy and liberty intermeshed with privacy. Justice Harlan once argued that the Fourteenth Amendment forbade the state from engaging in conduct inconsistent with a government based on the concept of ordered liberty. It stipulates under Section 1:

> No state shall make or enforce *any law* which shall abridge the privileges or immunities of citizens of the United States; nor shall any state

---

[21] See legal defintion, reasonable expectation of privacy, available at: http://www.law.cornell.edu/wex/expectation_of_privacy (emphasis added).
[22] See legal defintion, fruit of the posionous tree, available at: http://www.law.cornell.edu/wex/fruit_of_the_poisonous_tree
[23] Justice Brandeis's dissent in *Olmstead v. U. S. (1928).*

> deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.[24]

Justice Marshall recalled, "Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds."[25] Justice Kennedy also stated, "Matters involving the most intimate and personal choices a person may make in a lifetime, choices central to personal dignity and autonomy, are central to the liberty protected by the Fourteenth Amendment...the right to liberty under the 'due process clause' gives them the full right to engage in their conduct without intervention of the government. It is a promise of the constitution that there is a realm of personal liberty which the government may not enter." These protections of the privacies of the human mind offer weight to substantive values upheld by the First Amendment.

The Ninth Amendment also provides: "The enumeration in the constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."[26]

Justice Douglas supported a broader interpretation that the *Bill of Rights* protects "zones of privacy." Debates have been contentious on "drawing the privacy line," however, it has been historically indicated that certain liberties are "not-for-sale" and are "off-limits" for the government to decide.

Harper believes, "Brandeis's pronouncement remains a prominent and lasting tie in Supreme Court case law between the Fourth Amendment and privacy."[27] Certainly broader interpretations of constitutional law have been evolving since Brandeis dissent in *Olmstead v. U.S.* (1928). Then again, Justice Harlan has convoluted it.

---

[24] U.S. Constitution, *Fourteenth Amendment*, available at: http://www.law.cornell.edu/constitution/amendmentxiv (emphasis added).
[25] *Stanley v. Georgia*, 394 U.S. 557 (1969).
[26] US Constitution, *Ninth Amendement*, available at: http://www.law.cornell.edu/constitution/ninth_amendment
[27] Ibid, Harper, p.1384

1.2 Historical Evidence on Wiretap Surveillance

From the invention of the telegraph in 1837 to the telephone in 1876 wires have been tapped for the latest scoop. As an investigative technique, however, wiretaps were undefined by constitutional law. Eighteenth Amendment enabling legislation called the *National Prohibition Act of 1919, however,* restructured societal conditions and set the course for surveillance history.

With a rise in moonshine came a rise in federal enforcement agents to deal with criminal affairs. Soon followed a rise in applications for warrants to conduct legal searches and seizures and then also a rise in *warrantless wiretapping*. [28] As a general rule, federal law enforcement was prohibited from using wiretaps in the early twentieth century. The Justice Department banned the practice and thereafter, law enforcement officials required a warrant. [29]

In *Weeks v. United States,*[30] the U.S. Supreme Court decided an illegal seizure of items from a private residence constituted a violation of the Fourth Amendment. State agents entered Weeks home and took letters and envelops *without* a warrant to gain material evidence on suspicion of gambling. This evidence was used against him at trial and he was convicted. Unanimously, the Court decided against unreasonable searches and seizures in federal courts, which gave meaning to the Fourth Amendment's application. A physical home intrusion *without a warrant* to confiscate *papers* was deemed *unreasonable*. This set forward an exclusionary rule, prohibiting an admissibility of evidence obtained from an unlawful search and seizure by a federal officer in a federal court; thereafter, *Mapp v. Ohio*[31] extended the Fourth Amendment's protection and application in state courts.

---

[28]Kaplan et. al, The History of Wiretapping, ABA Section of Litigation 2012 Section Annual Conference: The Lessons of the Raj Rajaratnam Trial: Be Careful Who's Listening (April 18-20, 2012:2).
[29] Ibid, Kaplan et al, p.2
[30] *Weeks v. United States* 232 U.S. 383 (1914).
[31] *Mapp v. Ohio*, 367 U.S. 643 (1961).

Week's case drew a line to prevent physical intrusions into a private home by federal enforcement agencies for collecting information and evidence in support of criminal cases. However, *Olmstead v. United States*[32] was the first case to decide a form of surveillance, *warrantless wiretapping.* Once more inspired by the *National Prohibition Act,* federal prohibition agents pursued evidence against an illegal moonshine syndicate. Agents sidestepped the Justice Department's policy and also state law by wiretapping telephone conversations and intercepting messages.[33] Olmstead argued that wiretaps of his private conversations and use of that evidence violated his Fourth and Fifth Amendment rights. Despite this, the argument was rejected, the evidence was admitted and he was convicted.

The US Supreme Court considered that since the government placed wiretaps *in the street* by Olmstead's house, the agents had not *physically* trespassed on his property, and as such, the wiretaps were not a "*search*" under the Fourth Amendment. [34] Although the case "blurred the line" for surveillance activities, it was subsequently overturned by *Katz*, *Berger* and *Jones*. Moreover, wiretaps became a federal criminal offense under the 1934 Communications Act and any evidence collected by these surveillance techniques in admissible in court. [35]

Fourth Amendment protection typically requires that an individual have a *reasonable expectation of privacy.*[36] However, the reasonable expectation of privacy clause is deemed illogical. Harper considers that Justice Harlan's test "in dictum about privacy expectations" is impossible to administer. He said it "creates a one-way ratchet against privacy and Fourth Amendment protection."[37] To solve the dilemma, he adds, Harlan's test should be abandoned and privacy should be treated as a "factual question." Why does Harper believe Justice Harlan created a one-way ratchet? The answer lies within his two-part test.

---

[32] *Olmstead v. United States*, 277 U.S. 438 (1928).
[33] Ibid, Kaplan et al, p.3
[34] Ibid, Kaplan et al, p.3
[35] See Harper, p.1384
[36] See expectation of privacy clause, available at: http://www.law.cornell.edu/wex/expectation_of_privacy
[37] See Harper, p.1382, See id. at 361 (Harlan, J., concurring) (framing the emerging rule as a two- part test requiring a subjective and objective expectation of privacy).

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have *exhibited* an actual (subjective) *expectation of privacy* and, second, that the expectation be one that society is prepared to recognize as "*reasonable*."[38]

Harper explores, "People keep information about themselves private all the time without 'exhibiting' that interest in any perceptible way—indeed, without any *subjective* consideration at all."[39] He adds, "Families obscure their bathing behind the walls of their homes without contemplating that their walls provide them that privacy. One need not consider these things—much less 'exhibit' anything— to have a legitimate, actual interest in them."[40]

In Harlan's first-part test, "If a person has privacy, if the information was *not* generally available, he or she has 'exhibited' an actual (subjective) expectation of privacy." [41] Second, "This question whether society recognizes as *reasonable* the privacy of a given unit of information sounds like an objective test, but it is not. There is *no* objective standard for whether privacy is *reasonable*."[42] He concludes, "Justice Harlan did, alone suggest the *expectation* and *reasonableness* conditions on the Fourth Amendment protection for private information."[43] Adding that this "reasonable expectation of privacy" test does not tether courts to solid conceptual footings." [44]

> Our world is built for ornate combinations of privacy and disclosure that are almost always customary, habitual, or subconscious. They are rarely explicit, "exhibited," or a subject of a conscious "expectation." This does not diminish the importance of privacy or counsel against enforcing the constitutional right that protects it. Constitutional law does not require people to "exhibit" expectations about other constitutionally protected interests.[45]

---

[38] Katz v. United States, 389 U.S. 347 (1967).
[39] Ibid. Harper, p.1387
[40] Ibid. Harper, p.1387
[41] Ibid. Harper, p.1387
[42] Ibid. Harper, p.1387 (emphasis added).
[43] Ibid. Harper, p.1388
[44] Ibid. Harper, p.1388
[45] Ibid. Harper, p.1387

By technological progress "the government has received the ability to invade privacy in more subtle ways; further, there is no reason to think that the rate of such technological advances will slow down. Can it be that the Constitution affords no protection against such invasions of individual security?"[46]

As it stands now, the individual's circumstances as a given (including his or her privacy) asks whether the government has been *reasonable*. It does not ask whether Americans' privacy is reasonable. Current Fourth Amendment doctrine has it backward. It should be reformed.[47]

> As technologies like this press more tightly against the laws of physics, privacy practices and expectations may change, but courts need not guess at these questions, which have societal sweep. In each case, the question whether a person has maintained privacy in particular information is a factual inquiry.[48]

2 PRIVACY E-VALUATION

The protection of individual privacy has conscientiously developed by law together with human societies and modern technologies. As urban societies began to mix and mingle, bedeviling intrusions also came with the scene. It is said that American common law adapted to social, political and economical changes to expand securities for *person* and *property*."[49]

Bratman explains physical violations of the person in the nature of a battery, and for property, corporeal property. As time progressed, persons became protected from a threat of a battery (assault), damage to reputation (slander and libel), and then, property protections

[46] Ibid., Harper, p.1388
[47] Ibid, Harper p.1402
[48] Ibid, Harper, p.1402
[49] Ibid, Bratman p.8

including intangible items such as *products of the mind* such as copyright, trademarks and good will.[50]

Earlier privacy ills stemmed from the activities of gossipmongers "telling private tales," photographers "snapping shots on the fly" and columnists "printing sexy and personal snip-its hot off the press." [51] Moor considers historical cases useful; then again, other lenses to view privacy are philosophically revealing. Especially since "distrusted technology then was not the dreaded computer but the insidious camera" and "a charge that a government, a corporation, or an individual has invaded someone's privacy is regarded as a serious matter."[52]

Privacy is considered multi-dimensional, culturally relevant, and also spiritual in nature. For Brandeis and Warren, a privacy violation was a harm worse than physical injury and the "right to privacy was not something found by squinting at the Constitution but by admitting that cultural values and new technology play a large role in developing new understandings of our rights." [53]

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[54]

Brandeis-Warren upheld, "That courts of law should recognize a cause of action for damages resulting from invasions of the right to privacy, and this cause of action in common law involved the breach of implied contract, trust, or confidence. [55] Although it became clear the right to privacy was an interpretative matter, to define it and defend it, would

---

[50] Ibid, Bratman p.8 (emphasis added).
[51] Ibid, Bratman p.8
[52] James H. Moor, The Ethics of Privacy Protection, p. 71
[53] Ibid, Moor p. 71
[54] Ibid, William and Brandeis (1890).
[55] Ibid, Bratman p.8

prove to be an exceptional challenge, and for others, an unnecessary one. With so many complexities, how is privacy evaluated? To legally administer privacy violations, what does privacy mean?

2.1 What is privacy?

Westin clarifies "Privacy provides individuals and groups in society with a preservation of autonomy, a release from role-playing, a time for self-evaluation and for protected communication."[56] Westin does not limit the concept of surveillance to physical observation, wiretapping, or eavesdropping, he includes *psychological* surveillance (use of *personality testing* and lie detectors as a means of personnel selection) and data surveillance (*central collection of information* on individuals in computer banks).[57]

Others express privacy as a "right to be let alone." It is viewed as a limited access to self, secrecy, control over personal information, personhood, and intimacy.[58] Solove adds, "The conception of privacy as concealing information about the self forms the foundation for what is known as the constitutional right to *information privacy*.[59]

In striving for a modern understanding, Sparkes submits that based on a Socratic heritage, our world culture demands "definitions." Yet "clarity" not definitions is to be valued in Socratic terms, and often times, clarity and precision are confused.[60] Shaping definitions for narrow or technical purposes may be fabricated; yet, to actually believe we've captured the essence in defining whatever-it-is, we're likely deceiving ourselves.[61]

---

[56] Westin, A.F. (1968). Privacy And Freedom, 25 Wash. & Lee L. Rev. 166, p.166, http://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20
[57] Ibid., Westin, p.166
[58] Sabah Al-Fedaghi, The Ethics of Information: What is Valued Most, p. 118
[59] Ibid, Al-Fedaghi, p. 118
[60] A.W. Sparkes, "The right to be let alone: A violation of 'privacy'," Australia.
[61] Ibid, Sparkes

For that reason, Sparkes offers an insightful analytical method. For instance, "Don't try to *define* literature, but give reasons why one bit of writing might be said to be literary and reasons why another might be said not to be, and pay attention to borderline cases and the reasons they are borderline."[62] Perhaps it may be preferable to view privacy not as abstract or culturally relative, but instead aim to clarify "why some situations might be said to be *private* and reasons why another might be said *not to be*, and then, pay attention to borderline cases and reasons for why, they are borderline.

Privacy types to ponder are location privacy, physical privacy, privacy of personal behavior, personal communications, and data and "*information privacy*."[63] Informational privacy entails "the interest an individual has in controlling, or at least significantly influencing the handling of data about themselves."[64] Sabah Al-Fedaghi asserts it involves credit data, medical and government records, and indicating information about identifiable individuals in accessible form." [65] This means "any information concerning a natural person which, because of name, number, symbol, mark, or other identifier, can be used to identify that natural person." [66] Views concerning personal or private information normally equate access to information to promote processes in the identification or de-identification of a person.

Despite attempts to *define privacy* as control of information, undocumented personal information, secrecy, or a right to be let alone, one important consideration is how privacy impacts basic principles and values that justify legal protection. As formerly discussed as "zones of privacy" in the *US Constitution*.

Moor argues the *situation* makes the difference in privacy judgments, not the type of information. *Unauthorized surveillance* by *A* of a *private situation* counts as an invasion of

---

[62] Ibid, Sparkes
[63] Ibid Al-Fedaghi, p. 118
[64] Ibid, Al-Fedaghi, p. 118
[65] Ibid, Al-Fedaghi, p. 118
[66] Ibid, Al-Fedaghi, p. 118

privacy.[67] Conversely, to ensure a balance, it is also important to consider the conception of privacy from another position. Privacy can afford the private sphere to enjoy liberties and autonomy, however, "Separation of the 'concept of privacy' from the 'concept of liberty' is important because we do not want the right to privacy to become a screen to protect truly harmful actions." [68]

> A and B, should have a right to privacy, but their privacy does not give A the freedom to beat B or B the liberty to poison A or A and B the right to torture their children. Distinguishing privacy from particular freedoms allows us to argue for privacy without licensing abuse. A common motivation…is to protect individuals against intrusive laws for *victimless* crimes. [69]

In the contemporary sense, privacy typically equates to control of information. He rightly argues, however, this "theory of control" is insufficient in connection with modern information technologies.

2.2 Privacy in Theory

Many theories are studied to clarify the conception of privacy. It typically considers the "control of personal information" by which privacy is not – lost. However, Moor adds, "if control is construed to mean direct, personal control of information then on the *control theory of privacy* we are giving up privacy whenever we tell anyone anything about ourselves if there is no direct control over what the other person will do with the information." [70] In cyberspace as "personal information about us is stored in computer centers, most persons have no control over how that stored information is used."[71] He claims, if the collected

[67] Ibid, Moor p.78
[68] Ibid, Moor p.74
[69] Ibid, Moor p.74 (emphasis added).
[70] Ibid, Moor p.74-75
[71] Ibid, Moor p.74-75

information is properly used or not used, then privacy is not lost, even if there is a lack of control, on the other hand, if used improperly, it can pose a potential threat. [72]

In effect, this *control theory* for privacy does not seem capable of securing personal information in the digital domain. Therefore, a *restricted access theory* suggests, "Privacy is a matter of the restricted access to persons or information about persons." [73] Moor proposes, "an individual or group has *privacy* in a *situation* if, and *only if*, in that situation the individual or group or information related to the individual or group is protected from *intrusion, observation*, and *surveillance* by others." Al-Fedaghi considers, "Limited access is the condition of being protected from unwanted access by others, either physical access, personal information, or attention" that "entitles one to exclude others from (a) *watching*, (b) *utilizing*, (c) *invading* (intruding upon, or in other ways affecting) his private realm."[74]

Privacy cases in general consider the individual home, personal effects, contents of mind and communications, and personal and professional interrelationships, yet the term "*situation*" by definition is deliberate. It applies to a general range of affairs, which normally attributes privacy.[75] Therefore he adds, "The paradigm example of a *private situation* is a situation in which one is *protected* from the prying eyes of others." [76]

Further logic for considering *restricted access theory* is required. Not every situation by which information is made public is a loss of privacy. Not *all* collection of information constitutes a privacy violation, thus Moor holds, a distinction is necessary between *natural* and *normative* privacy to defend a restricted access theory. [77]

Moor defines "*Naturally* private situations as situations in which people, because of the circumstances of the situation, are naturally protected from intrusion or information-

[72] Ibid, Moor p.74-75
[73] Ibid, Moor p.76-77
[74] Ibid, Al-Fedaghi p. 118
[75] Ibid, Moor p.76-77
[76] Ibid, Moor p.77
[77] Ibid, Moor p.77

gathering by others," whereas in "*normatively* private situations the protection may be natural but is essentially legal or moral." [78] To illustrate the character and distinctive difference for privacy in these *situations*, it loops back to pensive considerations for "what constitutes an intrusion or an invasion.

Moor explains, one "*naturally private situation*" is a family hiking alone in the woods, there is no one else around and the forest naturally protects them from observation by others. If girl scouts suddenly appear in the woods on the trail in front of this family, they lose their *natural privacy*, the girl scouts intrude and observe them, however, they are doing nothing wrong as they have every right to be there. A loss of natural privacy is not automatically an invasion of privacy. [79]

In contrast, the protection of "*normatively private situations*" may be natural but is fundamentally legal or moral as "some people (the outsiders) are morally or legally forbidden from intruding or gathering information about others (the insiders) who are allowed in the situation." [80] To consider that very same scenario, he resumes, "If a family is enjoying a videotape in their home, they are in a *normatively private*, as well as a naturally private, situation. If girl scouts come to a window of their house and the girl scouts secretly peer through the window to watch this family, *privacy* will be lost. Because in this situation, there is normative protection, the family has a right to complain as the girl scouts are *outsiders* to the situation, and they have violated the right to privacy." [81]

As stated previously, it is normally agreed that control of information is an important aspect of privacy. What constitutes privacy in a normative context is culturally relative to be assessed on rational and moral considerations on a case-by-case basis. In deciding a proper balance, Moor agrees, on the one hand, the elements of liberty, personal development, and

---

[78] Ibid, Moor p.77
[79] Ibid, Moor p.77
[80] Ibid, Moor p.77
[81] Ibid, Moor p.77

control of information is a sphere of concern. Yet on the other, social and political institutions may become less effective which in turn may also be detrimental to individuals. [82]

The *situation* makes the difference, according to Moor. As an added example, "Suppose A confesses personal information to a priest B. Though A has no control over what B will do with the information, confessions are regarded in this culture as a *private situation*. The loss of control does not entail any loss of privacy. Clearly, if the confessional moment had been recorded clandestinely by someone else, then there would have been an *invasion of a private situation* and a corresponding *loss of privacy*." [83]

Drawing a line between an intrusion and an invasion, *restricted access theory* deems an intrusion as a *privacy violation* only *if* it "interrupts a private situation." For example, an intrusion on a public street is not an invasion of privacy. [84] However, "unauthorized manipulations of computer databases by using personal computers and modems are intrusions into private situations, and therefore, these are *invasions of privacy*." [85]

Cyberspace is consistently re-molding new environments and living conditions, for better and worse. Reasonable questions stem from an extraordinary overreach by secretive governmental authorities and secret agreements in a post-Snowden world, alongside a rising public interest to restore an acceptable system of legitimate checks and balances.

Moor believes *restricted access theory* "suggests the right questions for keeping *technology* in check." [86] To respect, to protect and to ensure a right to privacy, he stimulates basic questions to ask involving technological advancement. One might ask, "What kinds of restrictions should be put on the *access to individuals* and *information about them* in order to

[82] Ibid, Moor p.77
[83] Ibid, Moor p.78 (emphasis mine).
[84] Ibid, Moor p.78 (emphasis mine).
[85] Ibid, Moor p.79
[86] Ibid, Moor p.80 (emphasis mine).

protect privacy? What kinds of "restricted-situations or zones of privacy" will give us better lives?" [87]

By avoiding ambiguities that may arise in aiming to "define the essence of what privacy is," Moor believes one ought to shift away from asking abstract questions about the personal control of information or undocumented personal information, and instead ask – whether and how *specific situations* should have *restricted access*. [88] To protect personal information while also embracing Justice Douglas's concept of zones of privacy one illustrative example is library records. Moor explains:

> As library circulation records become more computerized, the resulting circulation databases ought to be regarded as zones of privacy. The issue is not whether a borrower should have control of his or her lending record in the database, but whether there is restricted access to the data so that borrowers feel the freedom to read what they please without scrutiny from the FBI or other outside organizations. One of the features of computers is that circulation records can be even more restricted than the traditional paper records. In a typical situation using computerized circulation records, a librarian need not have access to information about who has borrowed a particular item in the past. Computer technology can protect zones of privacy as well as invade them. [89]

2.3 Justification for Privacy Rights

The justification for *privacy rights* has adopted several approaches. An illustrious classic, the "right to be let alone" is cited frequently to capture an essence of *privacy*. Douglas agrees, "The right of privacy extends to the right to be let alone in one's belief and in one's conscience as well as in one's home." [90] In general, this seems reasonable. However, the right to be let alone could create very strange laws and strange morals.[91] Sparkes believes the right to be left alone suggests a social morality that seems irresponsible and neurotically

---

[87] Ibid, Moor p.80
[88] Ibid, Moor p.80
[89] Ibid, Moor p.80
[90] Ibid, p.252 (see fn.2)
[91] Ibid, Sparkes, p.253

agoraphobic.[92] Brandeis concept to be "let alone" no longer suffices to define the privacy concept in today's digital environment where personal information can be transported and distributed around the world in a flash.[93]

Sparkes adds, rights are matters of non-interference or include non-interference, and in formulating a right to privacy to determine its application, "the right to be let alone in a legal sense gets us absolutely nowhere."[94] A philosophical line of traction for this thought is:

> If you are drowning and I ignore your cries for help, I am letting you alone, but I am thereby respecting your privacy. If I shoot you, I am not letting you alone, but I am not thereby invading your privacy. If I hide in a bush to watch what goes on in your bedroom, I am acting with intent to invade your privacy, but with also intent to let you alone (if I don't let you alone my snooping project will be frustrated). [95]

In articulating a proper justification for the *right to privacy*, several *instrumental* values hold significance. Charles Fried asserts that privacy is necessary for love and friendship; James Rachaels advocates privacy is necessary to create diverse social relationships; Deborah Johnson claims that privacy increases a sense of personal autonomy. Moor upholds, "All of these are certainly plausible *justifications for privacy*, for *private situations* do foster diverse kinds of relationships and autonomous decision making." [96]

Not only are instrumental values available for privacy protection, but also privacy may offer strong *intrinsic* value. Brilliantly seeded, Moor paints a vivid picture to portray a deeper sense and justification for the protection of privacy rights, as an intrinsic value.

> Consider someone who has his entire life under surveillance by others. These others do not interfere with his life and he doesn't know that the surveillance is taking place. In effect, *all private situations* for this person are invaded, but his life is no different with regard to

---

[92] Ibid, Sparkes, p.253
[93] Jerry Berman and Paula Bruening. "Is Privacy Still Possible in the Twenty-first Century?" Center for Democracy and Technology, September (2007).
[94] Ibid, Sparkes p.253
[95] Ibid, Sparkes p.254
[96] Ibid, Moor p.80

> making decisions and having diverse relationships than it would have been without the surveillance. The only thing different about his life *under surveillance* is that he has *no privacy*. This person seems morally wronged by the invasion of his privacy though no special harm comes to him other than the invasion of his privacy. This thought experiment suggests that privacy has an intrinsic justification as well as an instrumental one.

Linking *privacy rights* as an *intrinsic* value is appropriate in the new era of secret e-surveillance. By design, artificial environments gradually impose a digital world upon humanity that has the power to capture virtually every aspect of the human individual, oftentimes, without their personal knowledge or consent. Drawing a line to prevent an unwelcome intrusion by outsiders into the *private situations* of human lives is a basic principle to secure human dignity and therefore, an essential foundation to respect universal human rights.

2.4 Privacy Principles

> In the infosphere, information exists about the proprietor: his/her thoughts, his/her body, and his/her relationships with other persons. Privacy and information are entangled in PII. Personal identifiable information is more "valuable" than non-PII because of its privacy aspect. It has an *intrinsic* value because it is "a human matter," just as privacy is a human trait. [97]

Computer Professionals for Social Responsibility claim, "Our personal information has become a commodity, it is used to predict behavior both for national security and for marketing and other purposes."[98] Since 1973, *Records, Computers, and the Rights of Citizens* introduced guidelines on Fair Information Practices (FIP).

The *Code of Fair Information Practices* offers five basic principles in respect for *record keeping systems*: (1) must be no personal data record-keeping systems whose very exist-

[97] Ibid, Al-Fedaghi p.122 (emphasis added).
[98] Ibid, Al-Fedaghi p.119

ence is *secret*; (2) must be a way for a person to find out what information about the person is in a record and how it is used; (3) must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's *consent*; (4) must be a way for a person to *correct* or *amend* a record of identifiable information about the person; (5) *Any* organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their *intended use* and must take precautions *to prevent misuses of the data.*

The Federal Trade Commission (FTC) Act aimed to protect consumers from unfair or deceptive practices in and affecting commerce. FTC's report entitled *Consumer Privacy on the Global Information Infrastructure* offer five principles based on international data protection standards: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.

The FTC, U.S. Department of Commerce and other federal agencies have often endorsed FIPs. Congress also includes FIP style protections in numerous laws.[99] However, regarding a federal "system of records," Federal agencies are directed to follow the *Privacy Act of 1974* and the Office of Management and Budget (OMB) guidance, not FTC's fair information principles. [100]

In 1999, OMB Director Jacob J. Lew held federal agencies must protect an individual's right to privacy when they collect personal information and supported *Principles for*

[99] Privacy Act of 1974; Family Educational Rights and Privacy Act of 1974; Right to Financial Privacy Act of 1978; Cable Communications Policy Act of 1984; Electronic Communications Privacy Act of 1986; Employee Polygraph Protection Act of 1988; Video Privacy Protection Act of 1988; Telephone Consumer Protection Act of 1991; Driver's Privacy Protection Act of 1994; Health Insurance Portability and Accountability Act of 1996; Children's Online Privacy Protection Act of 1998; Gramm- Leach-Bliley Act of 1999; CAN-SPAM Act of 2003; and Fair and Accurate Credit Transaction Act of 2003.

[100] Director Jacob J. Lew, M-99-18, "Memorandum for the Heads of Executive Departments and Agencies, Executive of the Office of the President, Office Management and Budget, (2 June 1999).

Providing and Using Personal Information published by the Information Infrastructure Task Force (IITF) on June 6, 1995.[101]

IITF Privacy Working Group issued draft *Principles for Providing and Using Personal Information* on May 4, 1994. In the *Privacy Guidelines for the National Information Infrastructure* (NII) a draft privacy code was discussed. However, the Electronic Privacy Information Center (EPIC) claims it is "weaker than the current codes and leaves large gaps in NII privacy policy in areas such as encryption, informed consent, unique identifiers, and enforcement."[102] Despite this, the US government expressed its commitment for the perpetual development of the NII.

The Privacy Working Group proposed the *Information Privacy Principle*, by which "individuals are entitled to a reasonable expectation of information privacy."[103] *Information integrity principles*, addressed whereas NII relies upon information integrity, it is the responsibility of all participants to ensure that integrity and participants should to the extent reasonable, "ensure that information is secure using whatever means are appropriate." [104]

The *Collection Principle* proposes, "Before individuals make a decision to provide personal information, they need to know how it is intended to be used, how it will be protected, and what will happen if they provide or withhold the information." [105] Information should "tell the individual why they are collecting the information, what they expect it will be used for, what steps they will take to protect its confidentiality and integrity, the consequences of providing or withholding information, and any rights of redress."[106]

---

[101] Ibid,, M-99-18
[102] See Electronic Privacy Information Center, Report 94-1, Privacy Guidelines for the National Information Infrastructure, A Review of the Proposed Principle of the Privacy Working Group, available at: http://epic.org/privacy/internet/EPIC_NII_privacy.txt
[103] Ibid, Report 94-1
[104] Ibid, Report 94-1
[105] Ibid, Report 94-1
[106] Ibid, Report 94-1

Section III addressed *Principles for Information Users*. It lists: (a) *acquisition and use principles,* whereas users of personal information should: (i) assess the impact on personal privacy of current or planned activities before obtaining or using personal information; (ii) obtain and keep only information that could reasonably be expected to support current or planned activities and use the information only for those or compatible purposes; (iii) assure personal information is as accurate, timely, complete and relevant as necessary for the intended use." [107] It also states a *protection principle*, by which "users of personal information must take reasonable steps to prevent the information they have from being disclosed or altered improperly, and therefore use appropriate managerial and technical controls to protect the confidentiality and integrity of personal information." [108]

The *Education Principle* states "the full effect of the NII on both data use and personal privacy is not readily apparent, and individuals may not recognize how their lives can be affected by networked information."[109] For that reason, information users should: "(1) educate themselves, their employees, and the public about how personal information is obtained, sent, stored and protected, and how these activities affect others; (2) ensure that information is accurate, timely, complete, and relevant for the purpose for which it is given." [110]

Fairness Principles were also included as "information is used to make decisions that affect individuals, those decisions should be fair." [111] As such, information users should, as appropriate: "(1) provide individuals a reasonable means to obtain, review, and correct their own information; (2) inform individuals about any final actions taken against them and provide individuals with means to redress harm resulting from improper use of personal information; (3) allow individuals to limit the use of their personal information if the

[107] Ibid, Report 94-1
[108] Ibid, Report 94-1
[109] Ibid, Report 94-1
[110] Ibid, Report 94-1
[111] Ibid, Report 94-1

intended use is incompatible with the original purpose for which it was collected, unless that use is authorized by law." [112]

Awareness Principles include that "*w*hile information collectors have a responsibility to tell individuals why they want information about them, individuals also have a responsibility to understand the consequences of providing personal information to others." [113] Therefore, individuals should obtain adequate and relevant information about: (1) planned primary and secondary uses of the information; (2) any efforts that will be made to protect the confidentiality and integrity of the information; (3) consequences for the individual of providing or withholding information; and (4) any rights of redress the individual has if harmed by improper use of the information." [114]

Based on first impressions from this Working Group session, Honorable David Flaherty claimed, "Surveillance, carried out for whatever presumed benevolent purpose, has the potential to hinder our liberty and erode democracy." [115] Significant gaps, back doors and privacy concerns remain.

EPIC claims, "the use of cryptography, collection of transactional data, use of unique identifiers, sale of personal records, and creation of on-line mailing lists are not addressed in the proposed code." [116] The Clipper proposal was also controversial for the working group, however, the White House decided to move forward. Privacy advocates refer to FIPs based on "the basic principle that organizations that collect and use personal information have a responsibility to the person about whom the information refers."[117]

In sum, NII proposed principles are contrary to FIPs and in general, and to the structure of privacy law in the United States, which places responsibilities squarely on organizations to

[112] Ibid, Report 94-1
[113] Ibid, Report 94-1
[114] Ibid, Report 94-1
[115] Ibid, Report 94-1
[116] Ibid, Report 94-1
[117] Ibid, Report 94-1

protect personal information.[118] It is argued that these NII privacy principles weaken the FIPs *notice* provision making it more difficult for users to know fully the privacy implications of new network services, and it is silent on issues as to what constitutes *consent*, therefore, eliminating current safeguards for data subjects. It requires only that "information collectors" inform individuals why information is collected, how it will be used, protected, and consequences for withholding. However, it does not include the responsibility to collect information only necessary for a transaction. [119] With reference to *redress*, there is "no recognition of a legal right to be compensated for harm." [120]

To improve the privacy code, EPIC argues that NII principles should include these amendments: (1) privacy implications of new network services should be made fully known to the public; (2) set out clear rights for individuals whose personal information is collected; (3) sale of personal data should require informed consent, possibly even financial compensation; and (4) enforcement of the principles will require legal rights.[121]

Other NII recommendations include privacy protection methods for the confidentiality of electronic communications, explicit provisions for privacy concerns must be recognized, proper use and regulation of telecommunications services, telecom personal data collection should be limited to the extent necessary for providing service and should not disclose information without the explicit consent of service users. In terms of security policies, it should be developed to protect network communications and establish mechanisms to ensure the observance of these principles.[122] The right to remain anonymous and use encryption was listed to advance this area of concern.[123]

It seems a conflict of interest for privacy principles remain at this time. The White House indicated support for the FBI's Digital Telephony Proposal, while on the other hand, 80%

[118] Ibid, Report 94-1
[119] Ibid, Report 94-1
[120] Ibid, Report 94-1
[121] Ibid, Report 94-1
[122] Ibid, Report 94-1
[123] Ibid, Report 94-1

of the American public opposed the Clipper Chip. [124] This proposal would provide that "The chip would contain a "back door" that would allow a third party to decrypt the user's messages. The special chip would be used in phones, cell phones, email, and other electronic transmissions."[125]

To achieve a political or profitable end, person(s) can access all of a person's "contacts and contents" and gain virtually complete insight into every facet of an individual's private world, literally access, everything about you.

> Consider the act of possessing PII that is not one's own, against the proprietor's will, whose consent is not unreasonably withheld. What is wrong with such an act is not the possession of information, hardly valued in itself as an anonymized piece of information, but the possession of information with a particular quality—namely, that of being not the proprietary information of the possessor. Thus, possession of PII—against the proprietor's will—amounts, morally, to theft, where what is wrong is not acting on the stolen thing, but taking the thing that is not one's own. [126]

3 DRAGNET SURVEILLANCE: CHARTING THE CYBER-LINE BETWEEN NATIONAL SECURITY INTEREST AND INDIVIDUAL PRIVACY RIGHTS

> The United States is an increasingly digital nation where the strength and vitality of our economy, infrastructure, public safety, and national security have been built on the foundation of cyberspace. Despite all of our efforts, our global digital infrastructure, based largely upon the Internet, is not secure or resilient enough today and future purposes. Effectively protecting cyberspace requires strong vision and leadership and will require changes in policy, technology, education, and perhaps law. [127]

---

[124] Ibid, Report 94-1
[125] See http://cs.stanford.edu/people/eroberts/cs201/projects/global-networks/nations/USA/Clipper.html
[126] Ibid, Al-Fedaghi p. 122 (emphasis added).
[127] Ensuring a Secure Global Digital Information and Communications Infrastructure, http://www.whitehouse.gov/issues/homeland-security

IN A REPLICATED DOMAIN called cyberspace people's private lives seem no longer *private*. As personal information travels *swiftly* across the superhighway known as the Internet, telltale contents can be transported in a flash. But then again, who has it, accesses it, controls it, uses it, and has a privileged power to copy it, retain it, retrieve it, manipulate it, or possibly abuse it, presents a contemporary challenge for human rights – everywhere in the world.

NSA's trailblazing scandal has casted a hypersensitive iCloud over individual privacy rights. Experts are debating for a "rights revolution" to reaffirm faith in basic human rights and ultimately, the preservation for freedom, human dignity and personal autonomy by calling forward a *Universal Bill of Human Rights for the Internet*.[128]

As this contested debate continues, an advanced search also continues to distinguish the line between national security interests and individual privacy rights. In light thereof, where is the cyber-line for the US government, the intelligence community, law enforcement authorities and private corporations subcontracted by the government agencies?

3.1 Enterprise Architecture

The Enterprise Architecture (EA)[129] is geared for interoperability, application portability, and scalability of electronic applications across networks of heterogeneous hardware, software, and telecommunications platforms.[130] The handling of *personal information* is stated to be consistent with government-wide and agency policies, however, there may be some additional considerations regarding the individual right to privacy. [131]

---

[128] *The Charter of Human Rights and Principle for the Internet*, avaibale at: http://igmena.org/userfiles/files/IRP_booklet.pdf
[129] Ibid, Circular No. A-130
[130] Ibid, Circular No. A-130
[131] Ibid., Circular No. A-130 (8, viii)

OMB Circular No. A-130[132] offers general policies concerning privacy guidelines applicable to "information activities of all agencies of the executive branch of the Federal government."[133] *Information technology* is defined as "the hardware and software operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information on behalf of the Federal government to accomplish a Federal function, regardless of the technology involved, whether computers, telecommunications, or others."[134] This includes automatic data processing equipment,[135] however it states, "For the purposes of this Circular, automatic data processing and telecommunications activities "related to certain critical *national security* missions," are *excluded*.[136]

As this Circular provides administrative executive directives regarding privacy laws, it seems a significant exclusion. For this involves the telecommunications and information systems operated by the Department of Defense (DoD), which defines a *national security system* (NSS)[137] as "any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency by which the function, operation, or use (i) involves intelligence activities; (ii) involves cryptologic activities related to national security; (iii) involves command and control of military forces; (iv) involves equipment that is an integral part of a weapon or weapons system; (v) is critical to the direct fulfillment of military or intelligence missions; or is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy."[138] This seems to create a potential gap between what is typically considered a *system of records*

---

[132] Circular No. A-130 provides uniform government-wide information resources management policies as required by the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35.
[133] Circular No. A-130 rescinds: OMB Memoranda M-96-20, "Implementation of the Information Technology Management Reform Act of 1996;" M-97-02, "Funding Information Systems Investments;" M-97-09, "Interagency Support for Information Technology;" M-97-15, "Local Telecommunications Services Policy;" M-97-16, "Information Technology Architectures," available at, http://www.whitehouse.gov/omb/circulars_a130_a130trans4#1
[134] Circular No.A-130, (6,p).
[135] See Section 111(a)(2) of the Federal Property and Administrative Services Act of 1949.
[136] See 44 U.S.C. 3502(2) and 10 U.S.C. 2315. (emphasis added).
[137] See 44 U.S.C. § 3542.
[138] 44 U.S. Code § 3542 – Definitions, (2, a, i-ii), available at: http://www.law.cornell.edu/uscode/text/44/3542

that all Federal agencies are required to comply with the *Privacy Act of 1974* and other statues, and the *national security system*, which appears to fall outside that scope of application.

For example, the NSS is *exempt* from the requirement of the OMB Director evaluating the information resources management practices of executive agencies with respect to performance and the results of the investments in information technology and it is *exempt* from any enforcement of accountability."[139]

For national security, classified information should be handled in accordance with the appropriate national security directives and national security emergency preparedness activities under *Executive Order (EO) No. 12472*. [140] Policy objectives stated under *EO 12472* refer to the *National Security Decision Directive* (NSDD) *97*.[141] It stipulates, "The nation's domestic and international telecommunications resources, including commercial, private, and government-owned services and facilities are essential in support of U.S. national security policy and strategy." [142] This includes "specific automated information processing resources which are embedded in, or support, the telecommunications facilities and systems and their associated databases." [143] It is unclear how privacy matters are handled under the NSS, as this remains classified information.

3.1.1 Technological Means and Methods of Mass and Targeted e-Surveillance

NSA's surveillance enterprise "Owning the Net" startled the Internet community by its alarming roster of codenames to virtually tap "*private situations*" worldwide. Headquar-

[139] See 40 U.S. Code § 11303 - Performance-based and results-based management
[140] An order of the President of the United States or the Chief Executive of a state that has the force of law and that is published in a manner permitting regular public access.
[141] National Security Telecommunications Policy (NSC-NSDD-97), avaiable at: http://www.fas.org/irp/offdocs/nsdd/nsdd-097.htm
[142] Ibid, (NSC-NSDD-97), (access file, p.1)
[143] Ibid, (NSC-NSDD-97), (access file, p.2)

tered in Fort Meade, Maryland, it also involves other intelligence agencies and operational bases located in the United Kingdom (UK), Japan, and many other locations.

NSA's top-secret program Stellar Wind is disputed to be so controversial that in 2004 it nearly caused top Justice Department officials to resign in protest.[144] Depicted as bottomless databases, it allegedly has ample technological muscle to hold all the *contents* of e-mails, Google searches, cellphone calls, and personal data details. By use of satellites, undersea cables, microwave links, cell phones, e-mail and other computer links, the data centers act as a virtual Data Cloud[145] and imposes a serious threat to individual privacy.

Stanford University confirms metadata is sensitive even in a small population and over a short time window.[146] Metadata surveillance discloses highly sensitive personal information, including medical issues, financial history, and marijuana cultivation. Using phone metadata, researchers found sensitive information about people's daily lives, including: neurological and heart conditions, gun ownership, marijuana cultivation, abortion, and participation in Alcoholics Anonymous. This study directly contradicts the repeated assurance by President Obama that NSA "is not looking at people's names, and they're not looking at content."[147]

Another important privacy concern is malware. Computer Network Exploitation (CNE) tactics operated through a special department referred as NSA Tailored Access Operations (TAO) "allegedly infected more than 50,000 computer networks worldwide with malicious software designed to steal sensitive information."[148] Malware implants referred to as "digi-

---

[144] *See* http://www.nytimes.com/2012/08/23/opinion/the-national-security-agencys-domestic-spying-program.html?_r=0

[145] *See* http://www.democracynow.org

[146] Transcend, Researchers Confirm: When NSA Watches Your Metadata, It Is Watching You, 17 March 2014, available at: https://www.transcend.org/tms/2014/03/researchers-confirm-when-nsa-watches-your-metadata-it-is-watching-you/

[147] Ibid, Transcend

[148] NRC, NSA infected 50,000 computer networks with malicious software, 23 November 2013, available at: http://www.nrc.nl/nieuws/2013/11/23/nsa-infected-50000-computer-networks-with-malicious-software/

tal sleeper cells" can be remotely controlled and remain active in targeted countries without being detected for years.[149]

Other technological means and methods that hold a capacity to intrude on the privacy rights include a program code-named CAPTIVATEDAUDIENCE that targets a computer's microphone to record conversations near the device.[150] A computer's webcam can be covertly hi-jacked to snap photographs by a program called GUMFISH. [151] Internet browsing can be recorded and username and passwords to access websites and e-mail accounts can be collected by FOGGYBOTTOM.[152] GROK logs user's keystrokes.[153] SALVAGERABBIT can extract data whenever a portable flash drive is connected to the system. [154] In addition, privacy-enhancing encryption tools can be circumvented to prohibit anonymous Internet browsing or scramble e-mails contents sent across the network.[155] HAMMERCHANT and HAMMERSTEIN can also intercept and perform exploitation attacks against user data transmitted via Virtual Private Networks (VPN). Skype and other Voice Over IP (VoIP) software can track whenever a person makes a call and reveal usernames and capture audio recordings over the Internet. [156] QUANTUMHAND allegedly exploits targeted computers as users access what is entrusted to be a "personal" Facebook account. Users are deceived by a false link and redirected to NSA-TAO FOXACID server, not Facebook's server in order to infect a target's computer and exfiltrate files from a hard drive." [157] NSA has significantly expanded its traditional signals intelligence operations to intercept electronic communications worldwide by infiltrating targeted computers or network devices directly.[158]

---

[149] Ibid, NRC, 23 November 2013
[150] The Intercept, Ryan Gallagher and Glen Greenwald, How the NSA Plans to Infect Millions of Computers with Malware, 17 March 2014, available at: https://www.transcend.org/tms/2014/03/how-the-nsa-plans-to-infect-millions-of-computers-with-malware/
[151] Ibid, Intercept, 17 March 2014
[152] Ibid, Intercept, 17 March 2014
[153] Ibid, Intercept, 17 March 2014
[154] Ibid, Intercept, 17 March 2014
[155] Ibid, Intercept, 17 March 2014
[156] Ibid, Intercept, 17 March 2014
[157] https://www.transcend.org/tms/2014/03/compare-the-nsas-facebook-malware-denial-to-its-own-secret-documents/
[158] Ibid, Intercept, 17 March 2014

These hostile activities create a "digital divide" for privacy rights and impact other fundamental rights. CCPR Article 19 states, "Everyone shall have the right to hold opinions without *interference*… this right shall include 'freedom to seek, receive and impart information' and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." [159] Mass and targeted surveillance operations spawn a "virtual interference" on end user's ability to access and receive information.

President Obama affirmed that "signals intelligence shall be collected exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions, and not for any other purposes." [160] Despite the legal justification arguing for mass e-surveillance is to defend against *international terrorism*,[161] it has also consisted of targeting the G-8 and G-20 summits, and also the climate change summit.

National security interests have shifted to the awfully vague "valid foreign intelligence purposes" as the line of justifiable activities has debatably been crossed.[162] Snowden claims, " Every country believes its 'foreign intelligence purposes' are 'valid,' but that does not make it so." He asks, are all these "activities necessary, proportionate, and an unquestionable matter of national security?" [163]

US intelligence heads claim that mass e-surveillance for defending national security has prevented 54 terrorist attacks. However, "Two independent White House reviews with access to classified evidence on which this claim was founded concluded it was untrue, as did

---

[159] ICCPR Article 19, avaiable at: http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
[160] Ibid, Intercept, 17 March 2014

[161] 50 U.S. Code § 1801 – Definitions, (c),(1-3), (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State; (2) appear to be intended— (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnapping; and (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.
[162] Transcend, Edward Snowden's Written Testimony to the European Parliament, 10 March 2014, available at: http://www.transcend.org/tms/2014/03/edward-snowdens-written-testimony-to-the-european-parliament/
[163] Ibid, Transcend 10 March 2014

a Federal Court."[164] The White House's Privacy and Civil Liberties Oversight Board determined "the mass surveillance program investigated was not only ineffective, but found it had never stopped a single imminent terrorist attack and it had no basis in law. [165]

3.1.2 Legal Debates: Federal Level

Traced to the cutting-edge laboratory of the Defense Advanced Research Projects Agency (DARPA), a clandestine vision was designed to place everyday actions "public and private" under the looking glass, and the Bush Administration pushed for a long-debated total information awareness (TIA) program that has the capacity to "handle financial information, stock transactions, business deals, foreign military and diplomatic secrets, legal documents, and confidential personal communications."[166]

By 2002, the largest data-surveillance system constructed was in the hands of John Poindexter, formerly "convicted of five felony counts of lying to Congress, destroying official documents, and obstructing congressional investigations." [167] Part of this TIA schema, was the Evidence Extraction and Link Discovery program (EELD) armed with *highly intrusive* techniques for obtaining pertinent information on links between people, organizations, places, and things from masses of available data, and then, connecting these bits of information into patterns that can be evaluated and analyzed to establish patterns and distinctions between legitimate and suspicious behavior. [168]

---

[164] Ibid, Transcend 10 March 2014
[165] Ibid, Transcend 10 March 2014
[166] Wired Magazine, James Bamford, The NSA Is Building the Country's Biggest Spy Center (Watch What You Say) (15 March 2012) 7:24 pm, available at: http://www.wired.com/2012/03/ff_nsadatacenter/
[167] James Bamford, "The Shadow Factory," The Ultra-Secret NSA from 9/11 to the Eavesdropping on America, First Anchor Books Edition, United States of America, (2009:102).
[168] Ibid, Bamford p.103.

Offering an entirely new lens to view freedom of movement, this invasive governance package incorporates Scalable Social Network Analysis (SSNA) that analyzes daily activities, such as telephone calls, ATM withdrawals, and meetings to distinguish terrorist cells from ordinary groups; as well as Activity, Recognition, and Monitoring (ARM) to develop "computerized cameras capable of watching, recording, and learning how people act and behave – to capture human activities in surveillance environments." [169]

This collective vision and design in secret by a few men for *all*, made a new mark for conducting government surveillance. Through the eyes of one privacy advocate, William Safire, a totally different world was observed:

> Every purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every Web site you visit and e-mail you send or receive, every academic grade you receive, every bank deposit you make, every trip you book and every event you attend – all these transactions and communications will go into what the department of Defense describes as "a virtual, centralized grand database." [170]

Scrapped once by Congress in concern for individual privacy rights, this TIA controversial data-mining operation slithered only deeper into the underworld. In time, however, it unwillingly resurfaced by unauthorized media disclosures and top-secret releases of information by former NSA contactor, Edward Snowden. "Everybody's a target; everybody with communication is a target." [171]

As multi-national industrial-complex expansions rose to protect *national security*, a series of decisions were placed in the hands of the executive branch, military department, elements of the intelligence community (EIC)[172] and a global information sharing enterprise.

---

[169] Ibid, Bamford p.103.
[170] Ibid, Bamford p.104.
[171] Ibid, Wired Magazine, 15 March 2012
[172] The Central Intelligence Agency (CIA); The National Security Agency (NSA); The Defense Intelligence Agency (DIA); The Offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs; The Bureau of Intelligence and Research of the Department of State; The intelligence elements of the Army, Navy, Air Force and Marine

Dispersed among *all* tiered-levels of government and clandestine governmental partnerships, it also required decisions by private corporations and other non-state actors. Still, several subscribe that a need to sacrifice human liberty for national security was not necessary.

Quite the reverse, it is confidently argued that a top-secret intelligence program known as Thin Thread had adequate technological capabilities and capacities for conducting e-surveillance ops in accordance with the law. It ensured privacy protection by strict encryption standards and intercepted communications within and between foreign countries *without* violating the Fourth Amendment and the Foreign Intelligence Surveillance Act of 1978 (FISA).

Thin Thread intended to "isolate and trap key conversations and messages while discarding the rest, unheard and unread." [173] It also employed an "automated auditing system to ensure analyst were not abusing the system and "peeking" at the contents." [174] NSA Whistleblower, William Binney stated while referring to worldwide Internet communications under the new system, Trailblazer, that "The NSA could not collect and smartly select from the large volume of data traversing the Internet for the nuggets of needed information about "Entities of Interest" or "Communities of Interest," while protecting the privacy of U.S. persons."[175] On the other hand, Thin Thread encrypted data (protecting privacy of U.S. citizens) until a *warrant* could be obtained from the Foreign Intelligence Surveillance Court (FISC).[176]

As a leading expert in considering the profound technological changes inspired by 11 September 2001, he argued:

Corps, the Federal Bureau of Investigation (FBI), the Department of the Treasury, and the Department of Energy; The staff elements of the Office of the Director of Central Intelligence, available at: http://cryptome.org/dod5240-1-r.htm

[173] Ibid, Bamford p.45.

[174] Ibid, Bamford p.45.

[175] Jewel et al vs National Security Agency, http://info.publicintelligence.net/NSA-WilliamBinneyDeclaration.pdf (p.2 line 2-3)

[176] Ibid, *Jewel et al vs National Security Agency*, (p.2 line 12-16)

> There was never a need for such as system. If Hayden had simply done as his job allowed and traced the calls and e-mail back from the Yemen ops center and obtained a FISA warrant for the California phone numbers and e-mail addresses, he would have discovered who, what, and where they were back in the spring of 2000. And then by monitoring their domestic communications, the FBI could have discovered the other members of the group.[177]

Yet, there seems to be a stark difference from the people's "right to know" what the government is doing with their personal information as compared to the professed "need to know"[178] by the DoD. Although *The Freedom of Information Act* (FOIA) is "the law that keeps citizens in the know about their government," and authorizes citizens "the right to access information from the federal government," this is not the case for classified information. The White House permits "agencies to release information requested under FOIA wherever doing so is compatible with the law and good policy."[179]

Regarding the NSA and EIC, the *U.S. Constitution*, *National Security Act 1947*, *War Powers Resolution*, *Authorization to Use Military Force* (AUMF), *Foreign Intelligence Surveillance act (FISA)*, *Title III of the Omnibus Crime control Act of 1968* (Wiretap Act) and other U.S. statutory criminal laws are seriously contested.[180] Several cases are also leveraged to argue for and against the deployment of dragnet surveillance schemes.

> Accurate and timely information about the capabilities, intentions and activities of foreign powers, organizations, or persons and their agents is essential to informed decision making in the areas of national defense and foreign relations. Collection of such information is a priority objective and will be pursued in a vigorous, innovative and responsible manner that is consistent with the Constitution and

---

[177] Ibid, Bamford p.122.
[178] http://cryptome.org/dod5240-1-r.htm (B, D (1).
[179] http://www.whitehouse.gov/21stcenturygov/tools/foia
[180] 18 U.S.C. §§ 2510-22, as amended by the Electronic Communications Privacy Act (ECPA)(Pub. L. 99-508; 10/21/86), the Communications Assistance to Law Enforcement Act (CALEA)(Pub. L. 103-414; 10/24/94), Antiterrorism and Effective Death Penalty Act of 1996 ("Antiterrorism Act") (Pub. L. 104-132; 4/24/96), USA PATRIOT Act (Pub. L. 107-56; 10/26/01), USA PATRIOT Additional Reauthorization Amendments Act of 2006 (Pub. L. 109-178; (3/9/06), FISA (Foreign Intelligence Surveillance Act) Amendments Act of 2008 (Pub. L.110-261; 7/10/2008), FISA Sunsets Extension Act (Pub. L. 112-3; 2/25/11) PATRIOT Sunsets Extension Act of 2011 (Pub. L. 112-14; 5/26/11).

> applicable law and respectful of the principles upon which the United States was founded.[181]

14 September 2001, President George W. Bush declared a *national emergency* in response to the attacks on the World Trade Center, the Pentagon and in New York. Based on the perceived continuous and immediate threats under *Proc. No. 7463. Declaration of National Emergency by Reason of Certain Terrorist Attacks*, President Barack Obama extended this national emergency to protect national security.[182]

Former NSA private contractor and whistleblower, Edward Snowden claims that his authorization for conducting e-surveillance[183] in support of *foreign intelligence* and *counter-intelligence* ops came under *Executive Order 12333*[184] and the *FISA Amendments Act* (FAA) *of 2008* § 702.

EO 12333 stipulates the administrative guidelines for *all* the EIC. On 31 July 2008, *Further Amendments to EO 12333 United States Intelligence Activities* was signed by former President George W. Bush authorizing for a progressive integration among the intelligence community for collaboration and information exchange to protect against international terrorism and other dangerous crimes. In addition, it presented a legal divide whereas many still question the assumed authorities of the US executive branch, NSA, other intelligence elements and law enforcement agencies, and progressively, private corporations, as *war-*

---

[181] Federal register, Executive Order 12333--United States intelligence activities, Source: The provisions of Executive Order 12333 of Dec. 4, 1981, appear at 46 FR 59941, 3 CFR, 1981 Comp., p. 200, unless otherwise noted, available at: http://www.archives.gov/federal-register/codification/executive-order/12333.html

[182] Notice of President of the United States, dated Sept. 11, 2012, 77 F.R. 56517,; Notice of President of the United States, dated Sept. 9, 2011, 76 F.R. 56633; Notice of President of the United States, dated Sept. 10, 2010, 75 F.R. 55661; Notice of President of the United States, dated Sept. 10, 2009, 74 F.R. 46883; Notice of President of the United States, dated Aug. 28, 2008, 73 F.R. 51211; Notice of President of the United States, dated Sept. 12, 2007, 72 F.R. 52465; Notice of President of the United States, dated Sept. 5, 2006, 71 F.R. 52733; Notice of President of the United States, dated Sept. 8, 2005, 70 F.R. 54229; Notice of President of the United States, dated Sept. 10, 2004, 69 F.R. 55313; Notice of President of the United States, dated Sept. 10, 2003, 68 F.R. 53665; Notice of President of the United States, dated Sept. 12, 2002, 67 F.R. 58317, available at: http://www.law.cornell.edu/uscode/text/50/1621

[183] Electronic surveillance is the acquisition of a non-public communication by electronic means 'without the consent of a person' who is a party to an electronic communication or, in the case of a non-electronic communication, 'without the consent of a person who is visibly present at the place of communication,' but not including the use of radio direction-finding equipment solely to determine the location of a transmitter.

[184] 46 Federal Register 59,941 (December 4, 1981), as amended by E.O. 13284, 68 Federal Register 4,075 (January 23, 2003); E.O. 13355, 69 Federal Register 53,593 (August 27, 2004); and E.O. 13470, 73 Federal Register 45,325 (July 30, 2008).

rantless wiretapping arguably runs counter to the civil and political guarantees, as provided by the *U.S. Constitution*.

> The government has a *solemn obligation*, and shall continue in the conduct of *intelligence activities* under this order, to protect fully the legal rights of all United States persons, including *freedoms, civil liberties*, and *privacy rights* guaranteed by Federal law.[185]

EO 12333 section 2.4 states, the EIC "shall use the *least intrusive* collection techniques feasible within the United States or directed against United States persons abroad"…*and* are *not* permitted to use "electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices *unless* in accordance with procedures established by the head of the Intelligence Community element concerned or the department head containing such element and approved by the *Attorney General*." [186]

Under Section 2.5, as amended, the Attorney General is delegated "the power to approve the use of *any* technique for intelligence purposes within the United States or against a U.S. person abroad of any technique for which a *warrant* would be required if undertaken for law enforcement purposes, provided that such techniques shall not be undertaken unless the Attorney General has determined in each case that there is *probable cause* to believe that the technique is directed against a *foreign power* or an *agent of a foreign power*.

As defined under FISA, electronic surveillance shall be conducted in accordance with that Act, as well as this Order.[187] The procedures shall "protect constitutional and other legal rights and limit use of such information to lawful governmental purposes."[188] And adds, under section 2.8 that "Nothing in this Order shall be construed to authorize any activity in violation of the Constitution or statutes of the United States." [189]

---

[185] Ibid., http://www.techlawjournal.com/topstories/2008/20080731.asp (emphasis mine).
[186] Ibid, EO 12333, 2.4
[187] Federal Register, Executive Order 12333--United States intelligence activities, note: Source: The provisions of Executive Order 12333 of Dec. 4, 1981, appear at 46 FR 59941, 3 CFR, 1981 Comp., p. 200, unless otherwise noted.
[188] Ibid., http://www.techlawjournal.com/topstories/2008/20080731.asp
[189] Ibid, EO 12333, 2.8

Congressional Research Service (CRS) upholds, FISA "provides a statutory framework by which government agencies may, when gathering foreign intelligence information, obtain authorization to conduct wiretapping,[190] physical searches,[191] utilize pen registers and trap and trace devices,[192] or access to specified business records and other tangible things."[193] CRS reports the "authorization for such activities is typically obtained via a court order from the Foreign Intelligence Surveillance Court (FISC), a specialized court created by FISA to act as a neutral judicial decision maker in the context of activities authorized by the statute."[194] References to FISA, and *Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA)*, are also linked to the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (USA PATRIOT Act).

However, EO 12333 and anti-terrorism laws are proclaimed as patently vague. Enabling legislation that also affords permission for conducting e-surveillance is substantively vague as regards data acquisition and communication surveillance. Despite these shortcomings, President Obama signed H.R. 5949, the *Foreign Intelligence Surveillance Act Amendments Act Reauthorization Act of 2012* extending Title VII of FISA until December 31, 2017.

Yet these laws impose some contradicting and incompatible overlaps for privacy protection. As for example, the *Electronic Communications Privacy Act* (ECPA) defines general prohibitions for e-surveillance in law enforcement investigations. Prohibitions include the interception of wire, oral, or electronic communications (wiretapping),[195] access to the *con-*

---

[190] 50 U.S.C. §§1801-1808.
[191] 50 U.S.C. §§1822-1826.
[192] 50 U.S.C. §§1841-1846. Pen registers capture the numbers dialed on a telephone line; trap and trace devices identify the originating number of a call on a particular telephone line. See 18 U.S.C. §3127(3)-(4) (2008).
[193] 50 U.S.C. §§1861-1862 (2008).
[194] Congressional Research Service, Edward C. Liu, *Reauthorization of the FISA Amendments Act* (8 April 2013), available at: http://www.fas.org/sgp/crs/intel/R42725.pdf
[195] *See* 18 U.S.C. §§2510-2522.

tent of stored electronic communications and communications transaction records,[196] and use of trap and trace devices and pen registers.[197]

Collection of *foreign intelligence* might fall within the scope of prohibitions under ECPA unless however, "the activity in question falls within the definition of e-surveillance under FISA then it may be conducted, *if* the government complies with FISA procedures" and "*if* the activity in question is not e-surveillance, as defined in FISA, but involves the acquisition of foreign intelligence information from international or foreign communications, then it is not subject to ECPA."[198] Comparing conflicts of interest, CRS adds, that the interception of a domestic telephone is generally prohibited by ECPA, however, it may be authorized under FISA. [199]

Prior to FISA amendments, the US government had authorization in the United States to monitor private electronic communications between the United States and a foreign country if: (1) the government's purpose was, in significant part, to obtain foreign intelligence information (which includes information concerning a 'foreign power' or 'territory' related to national defense or security or the conduct of ... foreign affairs; (2) the target of the government surveillance was 'a foreign power or an agent of a foreign power;' and (3) the government used surveillance procedures designed to '*minimize* the acquisition and retention, and prohibit the dissemination, of 'any private information' acquired about Americans.[200]

In addition, the government required the FISC's approval by submitting an application describing: (1) each "specific target;" (2) the "nature of the information sought;" and (3) the "type of communications or activities to be subjected to the surveillance." [201] Probable

---

[196] *See* 18 U.S.C. §§2701-2712.
[197] *See* 18 U.S.C. §§3121-3127.
[198] CRS, Edward C. Liu, Reauthorization of the FISA Amendments Act, Congressional Research Service, 7-5700, www.crs.gov, R42725 (8 April 2013:2-3), available at: http://www.fas.org/sgp/crs/intel/R42725.pdf
[199] Ibid, CRS p. 3
[200] Ibid, *Clapper v. Amnesty International USA*, (See also FISA §§ 1801(e), (h), 1804(a)).
[201] Ibid, *Clapper v. Amnesty International USA* (See also FISA § 1804(a)).

cause was also required to demonstrate each specific target was "a foreign power or an agent of a foreign power." [202] Instance-specific procedures had to be described and used "to *minimize* intrusions upon Americans' privacy (compliance with which the court subsequently could assess)." [203]

Exclusive means by which e-surveillance and interception of communications may be conducted is specified under 50 U.S. Code § 1812. It requires that "Only an *express statutory authorization* for e-surveillance or the interception of domestic wire, oral, or electronic communications, other than as an amendment to this chapter or chapters 119, 121, or 206 of title 18 shall constitute an additional exclusive means for the purpose of subsection."[204]

Therefore, the core argument at the Federal level seems to rest on the assessments and interpretations as to *if* executive authorizations for dragnet surveillance schemes are in compliance with an *expressly* authorized statute.

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act) expressly prohibits unauthorized, and nonconsensual interceptions of a wire, oral, or electronic communication by government agencies and private parties. It also provides statutory procedures for obtaining a *warrant* to allow wiretaps by government officials, and regulate disclosure and use of lawful intercepted communications by investigative and law enforcement officers.[205]

The w*arrantless wiretapping* program, conversely, traces back to the FISA amendments (FAA). FAA expanded authorizations for federal officials and private companies to wiretap for foreign intelligence purposes abroad and also *within* the United States. Title VII added procedures to acquire foreign intelligence information such as "targeting non-U.S. persons

---

[202] Ibid, *Clapper v. Amnesty International USA*, (See also FISA §§ 1804(a), 1805(a)).
[203] Ibid, *Clapper v. Amnesty International USA*, (See FISA §§ 1804(a), 1805(d)(3). (emphasis added).
[204] See 50 U.S. Code § 1812 - Statement of exclusive means by which electronic surveillance and interception of certain communications may be conducted.
[205] *Title III of the Omnibus Crime Control and Safe Streets Act of 1968*, (Pub. L. 90-351; 6/19/68).

abroad *without* individualized court orders,[206] new requirements to obtain an individualized court order when targeting U.S. persons abroad,[207] new procedures to obtain court orders authorizing the targeting of U.S. persons abroad for e-surveillance, acquisition of stored communications and other means for acquiring foreign intelligence information."[208]

The amendments eliminated requirements that the government describe to the court each specific target and identify each facility that surveillance would be directed at, therefore, permitting surveillance on a programmatic level and not necessarily on an individual basis; it eliminated a requirement that a target be a foreign power or an agent of a foreign power; and it also reduced the court's authority to insist on and supervise instance-specific privacy-intrusion minimization procedures.[209]

In relation to an "*expressly authorized statue*" that permits dragnet surveillance, Swire argues "there is no *third* statue" and Congress spoke clearly under 18 U.S.C. § 2511(2)(f),[210] plainly describing that Title III and FISA "shall be the *exclusive means* by which e-surveillance ... and the interception of domestic wire and oral communications may be conducted."[211] The *Authorization to Use Military Force* (AUMF) as an act of Congress may have provided the additional statutory basis for NSA, except however; the AUMF did *not* authorize wiretaps. Therefore, without a *statutory basis* it is considered as a federal crime by 50 U.S.C. § 1809.[212]

50 U.S.C. § 1809 expressly states that e-surveillance is a *criminal offense* and a prohibited activity. A person is guilty (including federal officials in the course of duty) *if* the person

---

[206] 50 U.S.C. §1881a.
[207] 50 U.S.C. §1881c(a)(2).
[208] 50 U.S.C. §§1881b, 1881c.
[209] Ibid, *Clapper v. Amnesty International USA*, (See also FISA § § 1881a(g).
[210] Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted.
[211] See http://www.peterswire.net/nsa_full_faq.htm
[212] Ibid, Swire

intentionally: (a) engages in e-surveillance under color of law *except as authorized by statute*; or (b) discloses or uses information obtained under color of law by e-surveillance, knowing or having reason to know that the information was obtained through e-surveillance *not authorized by statute*.[213]

E-surveillance conducted by law enforcement or investigative officers during the course of official duties can be a legitimate defense *if* "the e-surveillance was *authorized by* and conducted pursuant to a search *warrant* or *court order* of a court of competent jurisdiction."[214]

The Administration asserted, "The President has vast authority to order intelligence surveillance *without* warrants of *foreign powers* or their *agents.*"[215] The Justice Department filing with the Foreign Intelligence Surveillance Court of Review in 2002 indicated, "Congress cannot by statute extinguish that constitutional authority."[216] Then again, does Congress hold a measure of power to counter such a strong claim?

Article I states "All legislative powers herein granted shall be vested in a *Congress* of the United States, which shall consist of a Senate and House of Representatives."[217] This seems to imply that Congress has the statutory authority to regulate domestic wiretaps by federal agencies.

CRS reports, "The President may sometimes have the effective power to take unilateral action in the absence of any action on the part of the Congress to indicate its will, but this should not be taken to mean that the President possesses the inherent authority to exercise full authority in a particular field without Congress's ability to encroach."[218]

---

[213] See 50 U.S.C. § 1809 (a,b)
[214] 50 U.S.C. § 1809 (b).
[215] USAToday, Bush acknowledges approving eavesdropping, Posted 12/16/2005 6:27 PM, available at: http://usatoday30.usatoday.com/news/washington/2005-12-15-bush-spying_x.htm?csp=24
[216] Ibid, USAToday, 16 December 2005
[217] United States Constituion, Article 1.1
[218] Congresional Research Service, Presidential Authoirty to Conduct Warrantless Electronic Surveillance to Gather Foregin Inteligence Information, CRS-6, (5 Januray 2006) available at: http://epic.org/privacy/terrorism/fisa/crs_analysis.pdf

Concerning *EO 12333*, Rep. Pete Hoekstra (R-MI) a ranking Republican on the House Intelligence Committee affirmed, "The president is within his authorities to sign an executive order, but his administration is wrong to suggest that Congress was in any way involved or consulted.[219] The text of this order was *not* provided to the intelligence committee until 30 minutes before the committee was briefed and after it had been released on the Web. He adds, concerning "the impact that this order will have on America's intelligence community, and this committee's responsibility to oversee intelligence activities, this cannot be seen as anything other than an attempt to undercut *congressional oversight*."[220]

In consideration of congressional oversight for the NSA dragnet surveillance program, Administrative briefings were conducted with a "very limited group of Congressional leaders referred to as the Gang of Eight." [221] The group was strictly prohibited from "talking even with their lawyers about the legality of the program or actions Congress could take in response."[222] CRS suggested, "If NSA's surveillance program were considered an intelligence collection program, limiting congressional notification of the NSA program to the Gang of Eight, which some Members who were briefed about the program contend, would appear to be *inconsistent with the law*, which requires that the 'congressional intelligence committees be kept fully and currently informed of *all* intelligence activities,'[223] other than those involving covert actions."[224]

Handwritten, sealed and secured at the Senate Intelligence Committee dated on 17 July 2003, Senator Jay Rockefeller detailed several concerns in his disproval letter that stresses profound oversight issues on technology, surveillance, security, as well as the direction of the Administration.[225] In that letter, he explicitly referenced Poindexter's TIA program.

---

[219] Ibid,
[220] Ibid, (emphasis added).
[221] Ibid, Swire
[222] Ibid, Swire
[223] Sec. 501 [50 U.S.C. 413 (a)(1) and Sec. 502 [50 U.S.C. 413a] (a) (1).
[224] CRS Memorandum, Statutory Procedures Under Which Congress Is To Be Informed of U.S. Intelligence Activities, Including Covert Actions (18 January 2006).
[225] United States Senate, letter from Senator Jay Rockefeller, Senate Intelligence Committee, 17 July 2013, available at: http://www.fas.org/irp/news/2005/12/rock121905.pdf

Serious concerns were evidently being considered, however, these were withheld without proper channels to search for answers to critical questions.

Ronald Dworkin et al. resumes, "Congress did *not* implicitly authorize the NSA domestic spying program in the AUMF, and in fact *expressly prohibited* it in FISA."[226] CRS deduced that "It appears unlikely that a court would hold that Congress has expressly or implicitly authorized the NSA e-surveillance operations." [227] And keenly emphasized, "Attorney General Alberto Gonzales admitted that the administration did not seek to amend FISA to *authorize* the NSA spying program because it was advised that Congress would *reject* such an amendment. The administration *cannot* argue on one hand that Congress authorized the NSA program in the AUMF, and at the same time, it did *not* ask Congress for such authorization because it feared Congress would say no." [228]

Interpreting this needed separation of powers, three categorical distinctions provide the legal analysis based on Justice Jackson's concurring opinion. It has been subsequently adopted by the US Supreme Court as a key legal doctrine, stating:

> First, where the Congress has supported Presidential power, then the courts give great deference to that shared decision. Second, where Congress has stayed silent, there is a "twilight zone" where the courts are uncertain about the Presidential claim to power. Third, where Congress has acted contrary to the President's claim of power, then the President's power is at "its lowest ebb." [229]

Even *if*, the sole Presidential authority and NSA's main defense hinges on the AUMF, the text provides:

> That the President is authorized to use *all necessary and appropriate force* against those nations, organizations, or persons he determines planned, authorized, committed, or harbored such organizations or

---

[226] The New York Review of Books, Ronald Dworkin et al., On NSA Spying: A Letter to Congress (February 9, 2006 Issue), available at: http://www.nybooks.com/articles/archives/2006/feb/09/on-nsa-spying-a-letter-to-congress/
[227] Ibid, CRS Memorandum
[228] Ibid, Dworkin et. al
[229] See *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 635-38 (1952).

> persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations, or persons.[230]

Firstly Swire argues, this text does *not* explicitly mention or authorize wiretaps. Second, Congress did not intend for the AUMF to authorize *warrantless* wiretaps against United States persons inside the U.S. [231] And construing NSA's warrantless wiretap program as part of "*all necessary and appropriate force*," CRS issued a memorandum maintaining that "the President authorized the NSA to collect signals intelligence from communications involving U.S. persons within the United States, *without* obtaining a warrant or court order, raises numerous question."[232]A broad interpretation of "*all necessary and appropriate force*" escalates fervent concerns for the assumed powers under AUMF.

Swire emphasizes the AUMF authorizes *appropriate force* and that "the appropriate action is to comply with the law."[233] Likewise it is not 'appropriate' to violate the 'exclusive means' for conducting wiretaps in the United States, when FISA creates an effective mechanism to conduct surveillance on persons with known links to terrorists. [234] Obscuring the rules of clearly defined statues can lead to a spectrum of potential abuses and adversely impact other fundamental rights and freedom.

As for example, *Hamdi*[235] was indefinitely detained without due process of law. Nor was he granted access to an attorney or a trial as guaranteed under the Fourth and Fifth Amendment. In the name of *national security*, the government stripped his basic rights by simply stating that the Executive Branch had the right during wartime, to declare people who fight against the United States as "enemy combatants" and thus, restrict their access to the court system. This is a startling claim as fundamental rights are not privileges they are entitlements.

---

[230] S.J.Res. 23 (107th): *Authorization for Use of Military Force* 107th Congress, 2001–2002. Text as of Sep 18, 2001 (Passed Congress/Enrolled Bill).
[231] Ibid, Swire
[232] Ibid, CRS Memorandum
[233] Ibid, Swire
[234] Ibid, Swire
[235] *Hamdi v. Rumsfeld* 542 U.S. 507 (2004), see http://www.oyez.org/cases/2000-2009/2003/2003_03_6696

Fourth Circuit Court of Appeals reversed the decision; as it deemed the separation of powers require federal courts to practice restraint during wartime because "the executive and legislative branches are organized to supervise the conduct of overseas conflict in a way that the judiciary simply is not."[236] Rights afforded citizens of the United States are upheld as a cornerstone of the Constitution and necessary to prevent any one branch of government from obtaining a majority of power and control. [237] *Hamdi v. Rumsfeld* is argued to be a ringing example that exhibits a need to decipher and balance separation of powers, by proclaimed national security interests that encroach upon constitutional rights.[238]

Regarding the scope of dragnet e-surveillance, Attorney General Alberto Gonzales laid some of its parameters, advising reporters that it involves "intercepts of *contents* of communications where one party to the communication is outside the United States" and the government has "a *reasonable basis* to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda." [239] It is obvious as to why this raises questions. Firstly, the interception of *contents* is a serious privacy rights concern. Secondly, the cutback from having *probable cause* to merely declaring a "reasonable basis" considerably reduces the normative standard protected by the Fourth Amendment.

Additionally, Attorney General Gonzales statement implies that only terrorist and associates are targets in dragnet surveillance schemes. But is it only terrorist and associates? Snooping activities apparently also target and impact the lives of journalist, spouses, Red Cross workers and business people.[240] NSA linguist John Berry said, "The thing is you can't listen to Americans, and I was very careful that we never did because, one it's *illegal*. Two, I realized that we were in a kind of electronic minefield…you're sucking in someone

---

[236] *Ibid, Hamdi v. Rumsfeld* 542 U.S. 507 (2004).
[237] Ibid, *Hamdi v. Rumsfeld* 542 U.S. 507 (2004).
[238] Ibid, *Hamdi v. Rumsfeld* 542 U.S. 507 (2004).
[239] Ibid, CRS Memorandum
[240] Ibid, Bamford p.12.

you don't know until you listen to it, and yet the decision was made to continue listening, recording, and storing the conversations." [241]

Kinne adds, "Basically all rules were thrown out the window and they would use any excuse to justify a waiver to spy on Americans…we could have blocked the humanitarian aid organizations and all those other ones, but they said we had to monitor them just in case they ever talked about – because they eyes were on the ground – just in case they ever talked about seeing weapons of mass destruction anywhere and gave a location. Or in case they lost their phone and some random terrorist picked it up and started using it…and for those two reasons, we could listen to *all* the NGOs, humanitarian aid organizations, and frigging journalists in the area – and continue to even after they were identified and we knew who they were and that they weren't terrorists or terrorist affiliated… so that was the excuse they gave." [242]

United States Signals Intelligence Directive 18 (USSID 18) "prescribes policies and procedures, and assigns responsibilities to ensure that the missions and functions of the United States SIGINT System (USSS) are conducted in a manner that safeguards the constitutional rights and privacy of U.S. persons."[243] However, when David Murfee Faulk asked, Sir, these people are Americans – are there USSID 18 questions here? No, just transcribe them, that's an order, transcribe everything."[244]

USSID 18 also offers privacy measures granted to the Five Eyes, yet it is claimed "they could report on the substance of the call but not identify them as individuals."[245] Obviously not a member, but an ally, under code-name *GE Chancellor Merkel*, the German Chancel-

[241] Ibid, Bamford p131.
[242] Ibid, Bamford p131.
[243] United States Signal Intelligence Directive (USSID) 18, Limitations and Procedures in Signals Intelligence Operations of the USSS (U).
[244] Ibid, Bamford p131.
[245] Ibid, Bamford p132.

lor accused the US of a grave breach of trust upon learning that her mobile phone has been on NSA's target list since 2002. [246]

Since then, France and Germany have engaged in bilateral talks with the United States to discuss the issue of the eavesdropping, and pressed for a "no spying" agreement with Washington. [247] These activities led to a draft resolution before the UN General Assembly submitted by Germany and Brazil urging the 193 nations to "to take measures to put an end to violations of these rights and to create the conditions to prevent such violations, including relevant national legislation complies with their obligations under international human rights law."[248]

In defending NSA's activities occurring since 11 September 2001, the Department of Justice (DOJ) claims that the constitutional authority listed under Article II, and by the AUMF as the *express statutory authority* grants "the President has the authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States and in War Powers Resolution."[249] DOJ claims conducting warrantless surveillance is permissible for national security purposes "if the President of the United States or his chief legal officer, the Attorney General has considered the requirements of national security and authorized electronic surveillance as *reasonable*."[250] If this is accepted as a legal basis, it significantly widens the lens for considerations in the protection of constitutional rights and the international human right to privacy.

At its core, DOJ argues that communication intelligence (COMINT) and signals intelligence (SIGINT) is a fundamental part of waging war. Leveraging the *Hamdi* case, DOJ put forth that since COMINT is "a fundamental incident waging war, the AUMF *clearly and*

---

[246] See http://www.transcend.org/tms/2014/02/germany-france-to-mastermind-european-data-network-bypassing-us/
[247] See http://www.transcend.org/tms/2014/02/germany-france-to-mastermind-european-data-network-bypassing-us/
[248] See http://rt.com/news/un-draft-resolution-surveillance-110/
[249] U.S. Department of Justice, Office of Legal Affairs, *DoJ letter on Legal Authority on NSA Surveillance*, (22 December 2005), available at: https://www.fas.org/irp/agency/doj/fisa/doj122205.pdf (see also 50 U.S.C. §1541).
[250] Ibid, DoJ (p.2)

unmistakably authorizes such activities directed at the communication of our enemies." [251] Others strongly argue that Article II powers do not override the powers granted to the courts under Article III. Attorney General Alberto Gonzales stated on 19 December 2005:

> In terms of legal authorities, the Foreign Intelligence Surveillance Act provides -- requires a court order before engaging in this kind of surveillance that I've just discussed and the President announced on Saturday, unless there is somehow -- there is -- unless otherwise authorized by statute or by Congress. That's what the law requires. Our position is, is that the authorization to use force, which was passed by the Congress in the days following September 11th, constitutes that other authorization, that other statute by Congress, to engage in this kind of signals intelligence.[252]

Dworkin et al. counter argues, "DOJ's argument rests on an unstated general "implication" from the AUMF that directly contradicts *express* and *specific* language in FISA. Specific and "carefully drawn" statutes prevail over general statutes where there is a conflict." [253] Moreover, "There is no reason even to consider construing the AUMF to have implicitly overturned the carefully designed regulatory regime that FISA establishes. FISA does not prohibit foreign intelligence surveillance, but merely imposes reasonable regulation to protect legitimate privacy rights." [254]

FISA also dictates that "notwithstanding any other law, the President, through the Attorney General, may authorize e-surveillance *without* a court order … to acquire foreign intelligence information *for a period not to exceed fifteen calendar days following a declaration of war by the Congress*,"[255] and instead, the President acted unilaterally and secretly in contravention of FISA's terms. [256] FISA details rules of the road for dealing with wiretaps *without* a warrant in wartime, and it sets strict limitations. Noting this deficiency, it has

---

[251] Ibid, DoJ (p.3)
[252] See http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051219-1.html
[253] Ibid, Dworkin et al., ,See also *Morales v. TWA*, Inc., 504 U.S. 374, 384-85 (1992) (quoting International Paper Co. v. Ouelette, 479 U.S. 481, 494 (1987).
[254] Ibid, Dworkin et al.,
[255] 50 U.S.C. § 1811 (emphasis added).
[256] Ibid, Dworkin et al.,

been emphasized, "The DOJ letter remarkably does not even *mention* FISA's fifteen-day war provision, which directly refutes the President's asserted "implied" authority." [257]

> One of the crucial features of a constitutional democracy is that it is always open to the President—or anyone else—to seek to change the law. But it is also beyond dispute that, in such a democracy, the President cannot simply violate criminal laws behind closed doors because he deems them obsolete or impracticable.[258]

Former General Counsel of the Central Intelligence Agency, Jeffrey H. Smith concludes, "It is not credible that the 2001 authorization to use force provides authority for the President to ignore the requirements of FISA." [259] Department of Defense (DoD) senior official, Morton Halperin adds, "the congressional resolution authorizing the use of military force after 9/11 did not amend FISA."[260] Senator Daschle also reported that the administration sought to add the words "in the United States" to the AUMF after the words "appropriate force." However, Senator Daschle and the Senate refused. No such grant of power to conduct dragnet surveillance in the United States was intended by the AUMF, "The Bush administration now argues those powers were inherently contained in the resolution adopted by Congress -- but at the time, the administration clearly felt they weren't or it wouldn't have tried to insert the additional language."[261]

> There is absolutely nothing in the clear language of that resolution or in its legislative history suggesting that it was intended to override specific federal laws governing electronic surveillance. If Bush succeeds in establishing this as a precedent, he will have accomplished a breathtaking expansion of unilateral Executive power that could be easily applied to virtually any other area of *domestic activity* as long as a link to *national security* is asserted.[262]

---

[257] Ibid, Dworkin et al.,
[258] Marty Lederman, Center for Democracy and Technology, (January 9, 2006).
[259] Ibid, Swire
[260] Ibid, Swire
[261] Ibid, Swire
[262] Center for American Progress, Legal FAQs on NSA Wiretaps, available at: http://www.americanprogress.org/kf/NSA_WIRETAPS.PDF

In sum, the U.S. Supreme Court has never permitted all-inclusive powers to invade the right to privacy of Americans on domestic soil without individualized suspicion or judicial oversight. Yet still, the NSA surveillance program approves wiretapping in the United States without *either* safeguards required by the Fourth Amendment —individualized probable cause and a warrant or other order issued by a judge or magistrate. [263] Regarding the *only* instance for "national security wiretaps," the Court held that the Fourth Amendment prohibits domestic security wiretaps without those safeguards. [264]

Wiretaps are considered "searches" under Fourth Amendment.[265] In the Supreme Court's latest ruling on national security tap, it had been decided in the Keith Case that in accordance with the Fourth Amendment a judicial warrant is required.[266] According to Swire, "The case specifically did not rule on the issue of wiretaps directed at foreign intelligence targets."[267] In addition, in considering the "reasonable test" as most are not privy to the details involving the NSA program, he adds, "a thorough investigation of the facts, likely by Congressional staff, will be crucial to an assessment of the constitutional reasonableness of the government's actions." [268] Special needs may sometimes excuse the warrant and individualized suspicion requirements only where those requirements are impracticable and the intrusion on privacy *minimal*. However, wiretaps are *not* a minimal intrusion on privacy, yet are deemed as a highly intrusive act.

This new era of warrantless wiretapping has imposed a "chilling effect" on the world community in a multitude of ways. Instead securing a world based on the former Four Fundamental freedoms, it has stimulated a culture of fear and insecurity. For some, attorneys, human rights workers, whistleblowers, media organizations, and more, the basic freedom of speech and belief everywhere in the world is falling silent. Persons have already begun

---

[263] Ibid, Dworking et al. (See also *Katz v. United States*, 389 U.S. 347 (1967).
[264] Ibid, Dworkin et al, (See also *United States v. United States District Court*, 407 U.S. 297 (1972).
[265] Ibid, *Katz v. United States*; *Berger v. New York*
[266] Keith Case. 407 U.S. 297.
[267] Ibid, Swire.
[268] Ibid, Swire.

adjusting forms of communication and suffering "costly and burdensome measures" to protect the confidentiality of sensitive communications.[269]

It also has imposed additional hurdles in court. Despite psychological forms of harm due to profound uncertainties of being considered targeted individuals or perhaps associated with them; the threat of future injury was deemed insufficient in *Clapper v. Amnesty International.* On 26 February 2013 the United States Supreme Court dismissed the suit because plaintiffs did not suffer a sufficient concrete injury to have legal standing to challenge Title VII. Therefore, the Court did not decide the merits of the Fourth Amendment question in this case.[270]

3.1.3 The Private Sector

Access to communications data from third party service providers is a valuable technique for State surveillance. [271] Some private sector companies have facilitated mass e-surveillance activities of their clients. Substantial and costly investments have also been taken to modify the global network infrastructure in order to obtain massive data repositories, enabling access and allowing technological intrusions and various collection techniques on individual communications in a programmable fashion.[272]

From implementing measures that compromise privacy, security and anonymity of communication service, and in promoting interception capabilities for State surveillance numerous "back doors" are being identified. [273]This failure to integrate privacy-enhancing technologies or to implement less protective measures by lowering encryption standards, La Rue argues the private sector has been "complicit in developing technologies that enable

[269] *Clapper v. Amnesty International USA*, 132 S. Ct. 2431(2013)., at 1146
[270] *Clapper v. Amnesty International USA*, 132 S. Ct. 2431(2013).
[271] A/HRC/23/40 (p.20).
[272] A/HRC/23/40 (p.20)
[273] A/HRC/23/40 (p.22).

mass or invasive surveillance in contravention of existing legal standards."[274] Virtually unregulated, he adds, States have failed to keep pace with technological and political developments." [275]

High protection standards and protection of human rights should be a top priority for the private sector. La Rue remarks, "Access to communications data held by domestic corporate actors should only be sought in circumstances where other available less invasive techniques have been exhausted." [276] Despite this, under the Communications Assistance for Law Enforcement Act of 1994 (CALEA), telephone companies were required to design systems in a manner that would enable law enforcement to eavesdrop as needed. [277] In 2013, the Justice Department also noted that the Domestic Communications Center would facilitate the sharing of expertise among federal, state, and local law enforcement agencies and telephone companies looking to "centralize electronic surveillance." [278]

The private sector and government partnership not only tap communications by technology, but also by demand. The Justice Department Office of the Inspector General reportedly criticized this practice and cited abuses of the USA PATRIOT Act, emphasizing for example "data collection is authorized by legislation" signed by the Bush and Obama administration, and AT&T, Verizon and BellSouth delivered millions of telephone records to NSA. [279]

The scope of NSA's surveillance program is classified. However, former officials and telecom workers have indicated that the program extends beyond monitoring those individuals with suspect links to terrorism. [280] This adds consideration for the *legitimate aim* of the e-surveillance program.

---

[274] A/HRC/23/40 (p.20)
[275] A/HRC/23/40 (p.20)
[276] A/HRC/23/40 (p.22)
[277] Heidi Boghosian, "Spying on Democracy: Government Surveillance, Corporate Power, and Public Resistance," Open Media Series, City Light Books, San Francisco (2013:31).
[278] Ibid, Boghosian,p. 31.
[279] Ibid, Boghosian,p. 89.
[280] Ibid, Boghosian,p. 90.

Mark Klein provided documentation revealing a fiber-optic splitter at the AT&T facility located at 611 Folsom Street in San Francisco that "makes copies of all e-mails, Web browsing, and other Internet traffic to and from AT&T customers, and provides copies to NSA." [281] Heidi Boghosian argues that private corporations are enticed by lucrative government contracts keeping an eye on the profit motive, as customer information privacy is routinely and readily handed over without legal justification. [282]

In May 2012, for example, Twitter went to court and defended against the prosecutor's efforts to access several months worth of Malcom Harris' tweets. [283] Being one of the seven hundred protestors arrested on the Brooklyn Bridge on 1 October 2011 in an "Occupy movement" prosecutors wanted to investigate the *contents* of the tweets, IP addresses, e-mails and other information to learn if he was aware that police told demonstrators not to march across the bridge. [284] The Electronic Frontier Foundation (EFF), the American Civil Liberties Union (ACLU), the New York Civil Liberties Union (NYCLU) and Public Citizen urged a New York City judge to reconsider his decision authorizing a broad subpoena to Twitter and argued it "seriously threatens First Amendment rights and privacy of everyone on the Internet."[285]

The court ruled, "Harris didn't have legal standing to challenge it because the information—including all of his tweets —belonged to Twitter." [286] The government was allowed to get the content of communication—tweets—with a subpoena, "not a search warrant as required by the Fourth Amendment and the Stored Communications Act." [287] Twitter provided Harris' tweets to the Manhattan Criminal Court to avoid being held in contempt, but vowed to continue fighting to keep them out of prosecutions hands. [288]

30 June 2012, the judge denied Twitter's challenge to the subpoena. Twitter plans to ap-

---

[281] Ibid, Boghosian,p. 90.
[282] Ibid, Boghosian,p. 90.
[283] Ibid, Boghosian,p. 91.
[284] Ibid, Boghosian,p. 91.
[285] *Harris vs. New York*, available at: https://www.eff.org/cases/new-york-v-harris
[286] *Harris vs. New York*, available at: https://www.eff.org/cases/new-york-v-harris
[287] *Harris vs. New York*, available at: https://www.eff.org/cases/new-york-v-harris
[288] Ibid, Boghosian,p. 91.

peal. [289] This case illustrates a massive overreach on access and use of personal communications by law enforcement agencies during constitutionally protected activities. These are not "terrorist activities" but a legitimate civil movement of political dissent.

In the ongoing battle for rights, another case viewed the use of the Internet and the First Amendment differently. A group called Bash Back, a queer activist network challenged anti-gay polices of Mount Hope Baptist Church in Lansing, Michigan.[290] Mount Hope and the Alliance Defense Fund sued Bash Back and fifteen activists to uncover protester's identities that had disrupted a 2008 Sunday service. [291] Riseup.net was the only service provider that challenged the subpoenas and was successful. Federal judge, Richard A. Jones ruled that Riseup did not have to turn over the records by finding that "the Users' First Amendment right to speak anonymously online outweighs Mount Hope's right to discovery." [292]

To advance human rights and deter the commercialization of surveillance technologies, it is argued, "attention must be given to research, development, trade, export and use of these technologies considering their ability to facilitate systematic human rights violations." [293] These surveillance technologies are often sold to countries, which impose a serious risk to violate human rights, more specifically, human rights defenders, journalists or other vulnerable groups.[294]

Aggregation of information regarding relationships, locations, identities, and activities allow States to track an individual's movements across a wide-range of areas. There is also a noted lack of independent authorization and formal oversight in the access to data communications. [295] This raises strong concerns in terms of individual or group privacy and the potential abuse for discrimination.

---

[289] *Harris vs. New York*, available at: https://www.eff.org/cases/new-york-v-harris
[290] Ibid, Boghosian,p. 92.
[291] Ibid, Boghosian,p. 92.
[292] Ibid, Boghosian,p. 92.
[293] A/HRC/23/40 (p.22).
[294] A/HRC/23/40 (p.20)
[295] A/HRC/23/40 (p.16).

4 UNIVERSAL HUMAN RIGHT FOR PRIVACY

> Who are the authorities mandated to promote the surveillance of individuals? What is the final destiny of the massive amounts of the stored information on our communications? These questions urgently need to be studied in all countries to ensure a better protection of the rights to privacy and the right to freedom of expression.[296]

The United States of America ratified the *International Covenant on Civil and Political Rights* (CCPR*)* on 8 June 1992. The Vienna Convention on the Law of Treaties (VCLT) requires States to give effect to obligations under the Covenant in good faith.[297] CCPR is applicable to all branches of government (executive, legislative and judicial), and other public or governmental authorities; it "shall extend to all parts of federal states without any limitations or exceptions." [298]

Human Rights Committee (HRC) claims, "Failure to comply with this obligation cannot be justified by reference to political, social, cultural or economic considerations within the State."[299] Therefore, States are bound by international law to make changes to domestic laws and practices as are necessary to ensure their conformity with the Covenant. [300] As modern technologies evolve it is fundamental that awareness is ever present and that the laws must strive to keep pace in ascertaining the benefits and risks they may impose on human societies. Concerning the new modalities of surveillance technologies, UN Special Rapporteur Frank La Rue reported that it is necessary "to revise national laws regulating these practices in line with human rights standards."[301]

---

[296] UN Special Rapporteur, Frank La Rue, State communication surveillance undermines freedom of expression, warns UN expert, GENEVA (4 June 2013), http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=13400&LangID=E
[297] United Nations, Vienna Convention on the Law of Treaties, 23 May 1969, United Nations, Treaty Series, vol. 1155, p. 331, available at: http://www.refworld.org/docid/3ae6b3a10.html [accessed 5 May 2014].
[298] General Comment No. 31 [80], The Nature of the General Legal Obligation, Imposed on States Parties to the Covenant, Adopted on 29 March 2004 (2187th meeting). CCPR/C/21/Rev.1/Add. 13 26 May 2004.
[299] HRC, General Comment 31, 2004.
[300] HRC, General Comment 31, 2004.
[301] A/HRC/23/40

CCPR states from the outset, "the ideal of *free* human beings enjoying civil and political freedom and freedom from fear and want can only be achieved if conditions are created whereby everyone may enjoy his civil and political rights, as well as his economic, social and cultural rights."[302] As a general rule, the basic right of the human person is an *erga omnes* obligation.[303] In meeting compliance with *United Nations Charter*, all States Parties must promote universal respect for, and observance of, human rights and fundamental freedoms.[304] VCLT Article 27 also provides that the States Parties "may not invoke the provisions of its internal law as justification for its failure to perform a treaty." [305]

> States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights. In no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right. [306]

CCPR Article 17 states, "No one shall be subjected to *arbitrary*[307] or *unlawful* [308] interference with his *privacy*, *family*, *home* or *correspondence*, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[309] HRC affirms this right is required "to be guaranteed against *all* such interferences and attacks whether they emanate from State authorities or from natural or legal persons."[310] As a positive obligation "the privacy-related guarantees of article 17 must be protected by law." [311]

States are required to adopt legislative and other measures to give effect to a prohibition against interferences and attacks and for the protection of this right for individuals in their

---

[302] ICCPR
[303] HRC, General Comment 31, 2004.
[304] United Nations Charter (1945).
[305] HRC, General Comment 31, 2004.
[306] HRC, General Comment 31, 2004.
[307] Arbitrary interference can also extend to interference provided for under the law. The introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances. (3)
[308] Unlawful means that no interference can take place except in cases envisaged by the law. Interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant. (3)
[309] CCPR, Art. 17
[310] HRC General Comment 16, 1988.
[311] HRC, General Comment 31, 2004.

territory and subject to their jurisdiction. To uphold positive and negative obligations a State must also ensure Covenant rights against violations by its agents and acts committed by private persons or entities. [312] Measures are required to prevent a recurrence of a violation of the Covenant and due diligence applied to prevent, punish, investigate or redress the harm caused by private persons or entities.[313]

As a drawback, HRC reports, "necessary attention is *not* being given to information concerning the manner in which respect for this right is guaranteed by legislative, administrative or judicial authorities, and in general, by the competent organs established in the State."

> Concerns about national security and criminal activity may justify the exceptional use of communications surveillance…Nevertheless, national laws regulating what constitutes the necessary, legitimate and proportional State involvement in communications surveillance are often inadequate or simply do not exist. [314]

Cyberspace enables a prospective portal to virtually *all* aspects of the human individual. Never before has there been such a vast capability to access the most intimate domain of another's private sanctities of life, real-time. On one hand, innovations in technology have "enabled greater connectivity, facilitated the global flow of information and ideas, and increased the opportunities for economic growth and societal change." [315] Whereas on the other, it has provided new opportunities for State surveillance and intervention into individuals' private lives, by interception capabilities to permit State surveillance, rendering modern telephone networks remotely accessible and controllable."[316]

La Rue maintains, "communications data or metadata, includes personal information on individuals, their location and online activities, and logs and related information about the e-mails and messages they send or receive." [317] Largely unregulated in terms of disclosure,

---

[312] HRC, General Comment 31, 2004.
[313] HRC, General Comment 31, 2004.
[314] Ibid, La Rue (4 June 2013).
[315] Ibid, La Rue 4 June 2013.
[316] Ibid, La Rue 4 June 2013.
[317] Ibid, La Rue 4 June 2013.

he adds, "Communications data are storable, accessible and searchable." [318] When it becomes aggregated and analyzed, data can be both highly revealing and invasive. [319]

> Compliance with article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read. Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be *prohibited.* [320]

HRC appraised the United States' implementation of the CCPR on 13 Mar 2014. New York Times reported, "the U.S. sought to shield itself from criticism, claiming that the rights treaty imposes no human rights obligations on American military and intelligence forces when they operate abroad, rejecting an interpretation by the United Nations and the top State Department lawyer during President Obama's first term." [321] The United States held that its interpretation of the covenant applies only to individuals both within its territory and within its jurisdiction, stating that this is the most consistent with the covenant's language and negotiating history." [322]

Martin Scheinin, former UN special rapporteur on human rights and counter-terrorism, claimed "the surveillance constituted an unlawful or arbitrary interference with privacy or correspondence."[323] Aiming to secure privacy rights online in a similar fashion as that offline, Brazil and Germany proposed the "Right to Privacy in the Digital Age" at the UN General Assembly on 7 March 2013. The draft resolution recognizes "illegal surveillance of communications, their interception and the illegal collection of personal data consti-

---

[318] Ibid, La Rue 4 June 2013.
[319] Ibid, La Rue 4 June 2013.
[320] Ibid, General Comment 16 1988
[321] See https://www.transcend.org/tms/2014/03/us-to-un-we-can-disregard-intl-human-rights-treaty/
[322] See https://www.transcend.org/tms/2014/03/us-to-un-we-can-disregard-intl-human-rights-treaty/
[323] The Guardian, Dominic Rushe, UN advances surveillance resolution reaffirming 'human right to privacy.'Tuesday (26 November 2013 15.00 EST), available at: http://www.theguardian.com/world/2013/nov/26/un-surveillance-resolution-human-right-privacy

tute a highly intrusive act that violates the right to privacy and freedom of expression and may threaten the foundations of a democratic society."[324]

Striving to end mass e-surveillance worldwide, the United Nations High Commissioner for Human Rights (UNCHR) was requested to submit an interim report regarding the right to privacy in a domestic and extraterritorial surveillance of communications context. [325] As matters of communications interception, personal data collection, and mass surveillance raised significant concerns, the UNGA was invited to share its views in a movement to identify and clarify principles, standards, and best practices to address security concerns "in a manner consistent with States' obligations under international human rights law, with full respect for human rights, and in particular with respect to surveillance of digital communications and the use of other intelligence technologies that may violate the human right to privacy and freedom of expression and of opinion." [326]

EFF considers this opportunity as momentous to address advancing technologies over the past twenty-five years, declaring that if adopted, "it will be the first General Assembly resolution on the right to privacy since 1988."[327] Professor of law at Lewis & Clark Law School, Tung Yin, believes that the resolution would bring additional attention to Snowden's issues, but it would not likely have a real impact on the NSA's activities 'except at the margins.'[328]

In a resilient movement to guard against mass e-surveillance, the EFF, Privacy International, Human Rights Watch, Access, APC, Article 19 and a coalition of 290 NGOs issued "the *International Principles on the Application of Human Rights to Communications Surveil-*

---

[324] United Nations General Assembly, A/C.3/68/L.45, Brazil and Germany Draft resolution, *The Right to Privacy in the Digital Age*: (1 November 2013).
[325] Ibid, A/C.3/68/L.45, p.3
[326] Ibid, A/C.3/68/L.45, p.3
[327] EFF, Katitza Rodriguez, Brazil and Germany Proposed UN Resolution Against Mass Surveillance: (12 November 2013), available at: https://www.eff.org/deeplinks/2013/11/brazil-and-germany-propose-un-resolution-condemning-global-threat-mass
[328] The Guardian, Dominic Rushe, UN advances surveillance resolution reaffirming 'human right to privacy.'Tuesday (26 November 2013 15.00 EST), available at: http://www.theguardian.com/world/2013/nov/26/un-surveillance-resolution-human-right-privacy

lance, as a set of principles that "provide States with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights." [329]

At this particular stage of development, it seems clear that the US offers its citizen's greater protection than foreigners from NSA operations, and the Five Eyes argued that "that the legal right to privacy was an internal matter for states alone."[330] Nevertheless, human rights organizations stated that indiscriminate surveillance is never consistent with the right to privacy.[331]

On the international level, it remains a bit unclear as to the direction this may lead, as GA resolutions are non-binding; all the same, positive steps are being taken in the right direction in order to respect and protect the individual right to privacy.

> If even the US is willing to knowingly violate the rights of billions of innocents — and I say billions without exaggeration — for nothing more substantial than a "potential" intelligence advantage that has never materialized, what are other governments going to do? Whether we like it or not, the international norms of tomorrow are being constructed today, right now, by the work of bodies like this committee. If liberal states decide that the convenience of spies is more valuable than the rights of their citizens, the inevitable result will be states that are both less liberal and less safe. [332]

5 CONCLUSION

Mass and targeted electronic surveillance patterns have emerged across time based on the identification of dangerous criminal activities and the important role that federal agencies and law enforcement serve to protect society from harm. Enabling legislation to combat violent crimes has also lead to forms of surveillance and information sharing practices that

---

[329] Demand an End to Mass Surveillance, available at: https://necessaryandproportionate.org/take-action/EFA
[330] See http://www.theguardian.com/world/2013/nov/26/un-surveillance-resolution-human-right-privacy
[331] Human Rights Watch, UN: Reject Mass Surveillance, General Assembly Should Pass Strong Resolution on the Right to Privacy in the Digital Age (21 November 2013), available at http://www.hrw.org/news/2013/11/21/un-reject-mass-surveillance
[332] http://www.transcend.org/tms/2014/03/edward-snowdens-written-testimony-to-the-european-parliament/

have infringed upon constitutionally protected rights, and thereafter, have been explicitly regulated by law. Elements of the intelligence community and law enforcement officials are required to use the least intrusive collection techniques feasible. Wiretaps are highly intrusive acts of surveillance and constitute a search under the Fourth Amendment, which therefore, require individualized probable cause and a judicial warrant or court order. As a matter of precedent, the US Supreme Court has never permitted all-encompassing powers to invade the right to privacy of Americans without the safeguards as expressly provided in the Fourth Amendment. Title III and FISA provide the only statutory basis and exclusive means by which electronic surveillance may be conducted. Lacking an additional statutory basis, electronic surveillance is a federal criminal offense and prohibited activity. Article II Presidential powers do not override the powers of that granted to the legislative branch as defined under Article I, nor of those powers of Article III to the courts. The AUMF did not expressly authorize the use of wiretaps and Congress did not intend or authorize the NSA domestic warrantless wiretapping program against US citizens. Secret and warrantless electronic surveillance prompted by the global war on terrorism appears to lack a clear statutory basis and official authorization by Congress. And therefore, undermines and poses a threat to the individual right to privacy not only for American citizens, but also world-wide.

Privacy is a fundamental human right. It offers human individuals and society both instrumental and intrinsic values that serve as an essential basis to a preserve a sense of autonomy and human dignity. These fundamental principles and core values justify legal protection. On both the domestic and international level, measures to protect individuals from arbitrary and unlawful interference with his privacy, family, home or correspondence are required, regardless if these surveillance activities are being conducted by the State or private persons or entities. Unauthorized surveillance into normatively private situations of an individual constitutes a privacy violation and persons should be protected from intrusive laws that erode fundamental human rights and freedom. The broad interpretations of counterterrorism and counterintelligence instruments as presently adopted and practiced by the

US administration seem to surpass what US constitutional law and international law allow to counter terrorist activities.

6 LIST OF REFERENCES

Books and Articles

Akhil Reed Amar and Les Adams, "The Bill of Rights Primer, A Citizen's Guidebook to the American Bill of Rights," Skyhorse Publishing, New York, (2013).

Alan F. Westin, "Privacy And Freedom," 25 Wash. & Lee L. Rev. 166, (1968).

A.W. Sparkes, "The Right to Be Let Alone: A Violation of Privacy.

Bardo Fassbender, Ruling the World? Constitutionalism, International Law, and Global Governance, "Ch 5. Rediscovering a Forgotten Constitution: Notes on the Place of the UN Charter in the International Legal Order", Cambridge University Press, (2009:139).

Congressional Research Service, Edward C. Liu, "Reauthorization of the FISA Amendments Act" (8 April 2013).

Congresional Research Service, "Presidential Authoirty to Conduct Warrantless Electronic Surveillance to Gather Foregin Inteligence Information," CRS-6. (5 Januray 2006)

CRS Memorandum, "Statutory Procedures Under Which Congress Is To Be Informed of U.S. Intelligence Activities, Including Covert Actions" (18 January 2006).

Ronald Dworkin et al. , On NSA Spying: A Letter to Congress," The New York Review of Books, (February 9, 2006 Issue).

EFF, Katitza Rodriguez, "Brazil and Germany Proposed UN Resolution Against Mass Surveillance." (12 November 2013).

Heidi Boghosian, "Spying on Democracy: Government Surveillance, Corporate Power, and Public Resistance," Open Media Series, City Light Books, San Francisco (2013).

Human Rights Watch, "UN: Reject Mass Surveillance, General Assembly Should Pass Strong Resolution on the Right to Privacy in the Digital Age." (21 November 2013).

James Bamford, “The Shadow Factory,” The Ultra-Secret NSA from 9/11 to the Eaves-dropping on America, First Anchor Books Edition, United States of America, (2009).

James H. Moor, “The Ethics of Privacy Protection,” Library Trends, 39 (1 and 2), Summer/Fall 1990: 69-82.

Jerry Berman and Paula Bruening, “Is Privacy Still Possible in the Twenty-first Century?” Center for Democracy and Technology, September (2007).

Jim Harper, “Reforming Fourth Amendment Privacy Doctrine,” American University Law Review, Vol. 57:138. (2008).

Kaplan et. al, “The History of Wiretapping, ABA Section of Litigation 2012 Section Annual Conference:” The Lessons of the Raj Rajaratnam Trial: Be Careful Who’s Listening (April 18-20, 2012:2).

Marty Lederman,Center for Democracy and Technology, (January 9, 2006).

Richard Beeman, “The Penguin Guide to the United States Constitution”, Penguin Books, United States, (2010).

Sabah Al-Fedaghi, The Ethics of Information: What is Valued Most

Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review, 4 (5), (1890): 193-220.

Steven G. Calabresi & Lauren Pope, Judge Robert H. Bork and Constitutional Change: *An Essay on Ollman v Evans, 80 U Chi L Rev Dialogue 155.*

The Guardian, Dominic Rushe, “UN advances surveillance resolution reaffirming 'human right to privacy.” Tuesday (26 November 2013 15.00 EST),

UN Special Rapporteur, Frank La Rue, “State communication surveillance undermines freedom of expression,” warns UN expert, GENEVA (4 June 2013),

Westin, A.F. (1968). “Privacy And Freedom,” 25 Wash. & Lee L. Rev. 166, p.166,

7 Table of Instruments

CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, Adopted at the Thirty-second Session of the Human Rights Committee, on 8 April 1988.

General Comment No. 31 [80], The Nature of the General Legal Obligation Imposed on States Parties to the Covenant, Adopted on 29 March 2004 (2187th meeting).

CENTRAL INTELLIGENCE AGENCY ACT OF 1949 (Chapter 227; 63 Stat. 208; approved June 20, 1949)[As Amended Through P.L. 112–87, Enacted January 3, 2012]

Clinger-Cohen Act of 1996

Communications Assistance to Law Enforcement Act (CALEA),(Public Law 103-414; 10/24/94).

Declaration of Independence (1776).

Director Jacob J. Lew, M-99-18, "Memorandum for the Heads of Executive Departments and Agencies, Executive of the Office of the President, Office Management and Budget, (2 June 1999).

Homeland Security Act of 2002, Public Law 107-295 (Homeland Security Act),

Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22.

Electronic Privacy Information Center, Report 94-1, Privacy Guidelines for the National Information Infrastructure, A Review of the Proposed Principle of the Privacy Working Group

Executive Order 12333, "United States Intelligence Activities," December 4, 1981.

Executive Order 13470 of July 30, 2008, Further Amendments to Executive Order 12333, United States Intelligence Activities.

Foreign Intelligence Surveillance Act of 1978 (Public Law 95-511)need date

Foreign Intelligence Surveillance Act of 2008 (Pub. Law 110-261; 7/10/2008).

Foreign Intelligence Surveillance Act Sunsets Extension Act (Pub. L. 112-3; 2/25/11).

GAO/AIMD-00-296R Federal Agencies' Fair Information Practices

Gramm-Leach Bliley/Financial Modernization Act of 1999

H.R. 5949, the Foreign Intelligence Surveillance Act Amendments Act Reauthorization Act of 2012.

Paperwork Reduction Act of 1995.

Privacy Act of 1974.

S.J.Res. 23 (107th): *Authorization for Use of Military Force* 107th Congress, 2001–2002. Text as of Sep 18, 2001 (Passed Congress/Enrolled Bill).

Terrorism Prevention Act of 2004 (Public Law 108–458)

Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act).

United Nations, "Charter of the United Nations," 24 October 1945, 1 UNTS XVI.

United Nations, "Convention for the Suppression of Unlawful Seizure of Aircraft," 16 December 1970, UN Treaty Series 1973.

United Nations, Statute of the International Court of Justice, 18 April 1946.

United Nations General Assembly, "International Covenant on Civil and Political Rights" (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).

United Nations General Assembly, "International Covenant on Economic, Social and Cultural Rights," 16 December 1966, United Nations, Treaty Series, vol. 993.

United Nations General Assembly, A/C.3/68/L.45, Brazil and Germany Draft resolution, The Right to Privacy in the Digital Age: (1 November 2013).

United Nations General Assembly, "Universal Declaration of Human Rights," 10 December 1948, 217 A (III).

United Nations, General Comment No. 31 [80], The Nature of the General Legal Obligation, Imposed on States Parties to the Covenant, Adopted on 29 March 2004 (2187th meeting). CCPR/C/21/Rev.1/Add. 13 26 May 2004.

United Nations, of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/23/40, Report: (17 April 2013).

United Nations, Vienna Convention on the Law of Treaties, 23 May 1969, United Nations, Treaty Series, vol. 1155.

U.S. Department of Justice, Office of Legal Affairs, “DoJ letter on Legal Authority on NSA Surveillance,” (22 December 2005).

United States Senate, letter from Senator Jay Rockefeller, Senate Intelligence Committee, 17 July 2013.

United States Signal Intelligence Directive (USSID) 18, Limitations and Procedures in Signals Intelligence Operations of the USSS (U).

United States Constitution

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) of 2001.

USA PATRIOT Additional Reauthorization Amendments Act of 2006 (Pub. L. 109-178; (3/9/06).

USA PATRIOT Sunsets Extension Act of 2011 (Pub. L. 112-14; 5/26/11).

8 Table of Cases

Stanley v. Georgia, 394 U.S 557 (1969).

State v. Berger, 285 N.W.2d 533 (N.D. 1979).

United States v. Jones, 132 S. Ct. 945, 565 U.S. (2012).

Weeks v. United States, 232 U.S. 383 (1914).

Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635-38 (1952).

Key online resources

http://www.archives.gov/federal-register/codification/executive-order/12333.html

http://www.americanprogress.org/kf/NSA_WIRETAPS.PDF

http://cryptome.org/nsa-ussid18-80.htm

http://www.democracynow.org/

https://www.fas.org/irp/agency/doj/fisa/doj122205.pdf

http://www.fas.org/irp/news/2005/12/rock121905.pdf

http://www.fas.org/irp/offdocs/nsdd/nsdd-097.htm

http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051219-1.html

http://www.law.cornell.edu/lii/get_the_law

http://www.peterswire.net/nsa_full_faq.htm

http://www.theguardian.com/world/2013/nov/26/un-surveillance-resolution-human-right-privacy

http://www.whitehouse.gov/issues/homeland-security