The Future of Privacy in Post-9/11 America

Michelle Louise Atkin

On June 6, 2013, two major newspapers published lead stories on U.S. foreign intelligence surveillance. The headline in the London-based newspaper *The Guardian* read: "NSA Collecting Phone Records of Millions of Verizon Customers Daily," while the headline in *The Washington Post* read: "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program." As additional details of the top-secret telephone and Internet surveillance programs emerged, the Obama administration was quick to both confirm the existence of these programs and to assure the public that the programs, as authorized by the president, were constitutional. In responding to questions from reporters the day after the story broke, President Barack Obama said that he welcomed a public debate on how the country should balance competing privacy and security concerns. He also said that the leaks had done damage to national security by revealing the National Security Agency's (NSA) methods.

A few days later, Edward Snowden, at his own request, had *The Guardian* reveal him to be the person behind the NSA leaks. Snowden, a twenty-nine-year old former technical assistant for the Central Intelligence Agency (CIA) and employee of the defense contractor Booz Allen Hamilton working on an NSA contract, used the media to publicly identify himself as the source, proclaiming: "I have no intention of hiding who I am because I know I have done nothing wrong."[1] Snowden claimed his motivations for releasing such classified information was merely "to inform the public as to that which is done in their name and that which is done against them."[2] In an interview with Glenn Greenwald recorded in Hong Kong, Snowden described his motives this way:

> I think that the public is owed an explanation of the motivations behind the people who make these disclosures that are outside of the

> democratic model. When you are subverting the power of government that's a fundamentally dangerous thing to democracy and if you do that in secret consistently as the government does when it wants to benefit from a secret action that it took. It'll kind of give its officials a mandate to go, "Hey tell the press about this thing and that thing so the public is on our side." But they rarely, if ever, do that when an abuse occurs. That falls to individual citizens but they're typically maligned. It becomes a thing of "These people are against the country. They're against the government," but I'm not.[3]

Snowden's position is that his decision to break the news of the NSA's programs is a matter of principle. In the same interview with Greenwald, he stated that he believes that the government has granted itself power it is not entitled to, and that there is no public oversight. In this sense, one might view Snowden as a kind of conscientious objector who, by his own assessment, believes that what he perceives to be gross violations of the U.S. Constitution excuse him from his responsibility to respect the legal requirements for handling classified information.

The recent revelations by Snowden concerning the NSA's telephone and Internet surveillance programs operating under President Barack Obama, and the legal justification provided to them by the Obama administration, bear a striking resemblance to the December 2005 revelations in the *New York Times* concerning the warrantless surveillance program (later known as the Terrorist Surveillance Program) under President George W. Bush. The arguments advanced by the Bush administration in 2005, and the arguments advanced by the Obama administration in 2013, are palpably utilitarian,[4] with both claiming the greater good (in each case, national security) as the justification for their actions. Likewise, claims that both the Bush and Obama surveillance programs violate the Fourth Amendment protections against unreasonable search and seizure have been largely contractarian[5] in nature, in that they appeal to a rights-based conception of politics in which the government is legally and ethically obligated to respect the fundamental rights as enumerated in the Bill of Rights.

The similarity of the debate in these two cases is not accidental. It points to an underlying theoretical problem that will reemerge any time that measures taken to protect national security come into tension with rights to privacy, due process, and so on. One party will

appeal to a conception of politics based on a utilitarian understanding of ethics, and the other will respond with arguments grounded in a rights-based understanding of ethics. The "debate" will then of necessity be nothing more than a sterile assertion of contrary claims based on contrary philosophies, in which each party tries to score political points and neither is positioned to work constructively toward a solution.

What is needed, then, is a new ethical framework that allows for a constructive dialogue between the parties. Because the underlying problem in the debate is the different philosophical starting points used by each side, that framework has to be one that allows for a principled synthesis of the two philosophical approaches. The objective of this study is to propose one such framework.

This article begins with an overview of both the Terrorist Surveillance Program (TSP) under President Bush and the telephone and Internet surveillance programs under President Obama, examining the legal and ethical justifications provided by each administration for their respective programs. Taking into account the utilitarian arguments that have been advanced in support of these programs, and the corresponding rights-based/contractarian arguments advanced by individuals and groups who view these programs as an overreaching of presidential authority, this article advances the view that a more balanced approach is required if there is to be any meaningful discussion on the issue. Achieving a balance in the debate over liberty versus security requires an approach that is proportional. Much of the debate concerning U.S. foreign intelligence surveillance has been framed using utilitarian and contractarian theories as the basis for their arguments. Although such ethical theories are often viewed as incompatible or competing theories, this paper presents an alternative view, one that sees both theories as contributing to an applied ethical framework through the use of a practical proportionality test that can be applied by the courts in their decision making.

Given the legal landscape, with multiple legal challenges being filed in light of the new revelations of the NSA's surveillance programs under the Obama administration, and with new life having been breathed into *Jewel v. NSA*,[6] a legal challenge stemming from the Bush administration's TSP program, such a discussion of legal proportionality is not only important but also timely.

Terrorist Surveillance Program (TSP) under President Bush

The NSA's warrantless surveillance program was authorized by President Bush in October of 2001 through the use of a secret presidential order. News of the program broke on December 16, 2005, in the *New York Times*.[7] The program, which was later called the TSP by the Bush administration, allowed NSA to intercept "communications between individuals on American soil and individuals abroad, without judicial approval."[8] Immediately following the release of the story, President Bush used his weekly radio address on December 17 to publicly admit that he had authorized the program but contended that NSA's actions were "consistent with U.S. law and the Constitution."[9] Rather than responding immediately to the new revelations about warrantless surveillance in his address, Bush used the opportunity to first stress the need for the Senate to reauthorize the soon-to-expire sunset provisions of the PATRIOT Act, emphasizing that America's law enforcement personnel had used this "critical law to prosecute terrorist operatives and supporters and to break up terrorist cells in New York, Oregon, Virginia, California, Texas, and Ohio."[10]

Appealing to the authority vested in him by the Congress through the Joint Authorization for Use of Military Force (AUMF), in combination with his powers as commander in chief, President Bush asserted the claim that he had acted within the bounds of the Constitution and the law. President Bush summed up his address with a short reference to the breaking controversy, stating simply that he had "authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations."[11]

The claim that "only persons with known links to al Qaeda" were the targets of such surveillance was widely contested in the press. What is known is that shortly after 9/11 the president ordered the NSA to secretly wiretap the "international telephone calls and email messages of Americans without obtaining warrants."[12] This secret wiretapping was made possible through a public-private partnership between the NSA and various telecommunications companies.

In breaking the story, the media, according to the president, had endangered Americans by leaking the existence of this program. The

possible chilling effect on free speech was also clear, as President Bush stated:

> As a result, our enemies have learned information they should not have, and the unauthorized disclosure of this effort damages our national security and puts our citizens at risk. Revealing classified information is illegal, alerts our enemies, and endangers our country.[13]

Presidential Power, the TSP, and the Role of the Telecoms

The president's position that he was acting in accordance with the powers given to him in the emergency resolution passed by Congress shortly after 9/11 was not one shared by all lawmakers. As Senator Leahy commented, Democrats and Republicans did not give the president the authority to "go around the FISA law to wiretap Americans illegally." Rather, the authorization in question, according to Leahy, was simply the means necessary to give the President the go ahead to "capture or kill Osama bin Laden and to use the American military to do that. It did not authorize domestic surveillance of American citizens."[14]

The revelations of the TSP's existence quickly gave way to questions concerning whether or not the president had the original authority to implement a program such as the TSP (given FISA's intent—not least of which is to curb executive abuses of such powers). Even on the chance that the president was correct in authorizing such a program, there was still the issue of oversight and where that oversight might belong (i.e., with the Congressional Intelligence Committee or with the Foreign Intelligence Surveillance Court [FISC]).

Whether the president had acted in accordance with the law is subject to debate, but even if he had acted within proper bounds, questions concerning the role of the telecom companies within the program and their potential legal liability remained. Clearly, the program could not have existed without their cooperation; however, their ability to refuse to participate, as well as the scope of the presidential order in question, was not fully understood at the outset. As Jon D. Michaels notes:

> First, the intelligence agencies depend greatly on private actors for information gathering. Second, the Executive is institutionally predisposed to act decisively and unilaterally during times of crisis, even if

> that means bypassing legal restrictions, skirting congressional and judicial oversight, and encroaching on civil liberties. Third, to the extent corporations currently are (or can be made to be) willing partners, the Executive may choose to conduct intelligence policy through informal collaborations, notwithstanding the legal, political, and structural collateral harms these inscrutable bargains may generate.[15]

A month after the president had defended his authorization of the TSP, on January 17, 2006, the American Civil Liberties Union (ACLU) on behalf of a diverse group of prominent journalists, scholars, attorneys, and national nonprofit organizations filed a lawsuit against the NSA arguing the TSP was unconstitutional.[16] The ACLU lawsuit alleged:

1. the NSA program violates the First and Fourth Amendments of the United States Constitution. The program authorizes the NSA to intercept the private communications of people who the government has no reason believe have committed or are planning to commit any crime, without first obtaining a warrant or any prior judicial approval, and
2. the program violates the constitutional principle of separation of powers, because it was authorized by President Bush in excess of his Executive authority and contrary to limits imposed by Congress.[17]

The ACLU lawsuit was followed two weeks later by the Electronic Frontier Foundation (EFF) class action lawsuit against telecom giant AT&T, on January 31, 2006.[18] The EFF lawsuit alleged that AT&T violated the Stored Communications Act, Title II of the Electronic Communications Privacy Act (ECPA); the Wiretap Act, Title I of the ECPA; and the Pen Register Statute, Title III of the ECPA.[19]

With papers such as *USA Today* reporting that AT&T, Sprint, and MCI were all participating in the program of warrantless surveillance, the number of possible partners within the TSP appeared to be growing. The spring of 2006 gave way to increasingly negative press reports and mounting public concern over the scope of the program. *Newsweek* reported that the NSA had apparently revealed the names of more than ten thousand U.S. citizens that it had monitored.[20] In addition, the scope of the participation by the telecom companies in the TSP made further headlines on May 11, 2006, when *USA Today* reported that NSA had constructed a "massive database of Americans' phone calls."[21] The call records of perhaps tens of millions of Americans, the paper alleged, had been provided to NSA using data provided by AT&T, Verizon, and BellSouth. The collection of these

call records, according to reporter Seymour Hersh, initially began with the tracking of chains of phone numbers connected to phones that had called high-risk regions.[22] According to Hersh's reporting, programmed computers were used to:

> map the connections between telephone numbers in the United States and suspect numbers abroad, sometimes focussing on a geographic area, rather than on a specific person—for example, a region of Pakistan. Such calls often triggered a process, known as "chaining," in which subsequent calls to and from the American number were monitored and linked.[23]

As the telephone chains grew longer, more and more American calls were being swept into the monitoring. With more and more telecoms being implicated, several were quick to proclaim their noninvolvement with the TSP. Companies such as Qwest, although never named in the original press reports, announced publicly that it had not participated in the program (it later became known that its lawyers were more than skeptical about any potential legal liability that compliance would bring and advised the company not to participate).[24] This was soon followed by pronouncements from BellSouth and Verizon that they were never involved in the program—forcing *USA Today* to amend its original claim that these companies had participated in the program.[25] That being said, AT&T neither confirmed nor denied assisting the NSA—with the media and legal storm around that company's involvement continuing as new revelations about its involvement in the NSA program were coming out in the press.[26]

Piecing together details of the program through documents and interviews with Mark Klein, the whistleblower at the center of the EFF class action suit, it appeared that AT&T had provided NSA with access to phone and Internet traffic passing through its San Francisco switching center, which it could then sift using data mining software.[27] Combining this information with the administration's account of the program, it would seem that the TSP's main operation was one of interception, data mining, and human search of intercepted messages. Once a communication was intercepted, it could then be filtered through computer data mining techniques, and eventually, if there was reason to believe that the communication was of interest, it could be passed through a human filter.[28]

District Court judge Anna Diggs Taylor's decision on August 17, 2006, in the case of *ACLU v. NSA*[29] made it clear that the president

did not have the power to authorize the NSA's domestic spying program under either the Iraq War resolution or the Constitution. In her ruling she states:

> It was never the intent of the Framers to give the President such unfettered control, particularly where his actions blatantly disregard the parameters clearly enumerated in the Bill of Rights.[30]

Taylor stayed her ruling pending appeal.[31] In October 2006, a three-judge panel of the Sixth U.S. Circuit Appeals Court ruled that the NSA's TSP program could continue through the appeal process.[32] As the *ACLU v. NSA* case was working its way through the courts in 2006 to 2007, Attorney General Gonzales attempted to assure the public that there was sufficient legal oversight in place and that there was a unified legal opinion among Department of Justice and administration officials that the program itself was constitutional.[33] Still the court of public opinion did not seem convinced—and in a surprising reversal, the attorney general announced on January 17, 2007, that "any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court."[34]

The fate of the appeal in the *ACLU v. NSA* case marked the change in the legal tide, with the case being overturned on appeal in July 2007. The Appeals Court did not address any of the legality issues surrounding the program, but rather only the issue of whether the plaintiffs lacked standing.[35] In order to prove that they had legal standing, the plaintiffs would have had to demonstrate that their rights had actually been infringed, and given the secret nature of the program, finding the evidence to prove such violation would have been close to if not impossible. The end result, a 2–1 ruling, found the plaintiffs lacking such standing, and therefore the case was overturned.[36] With a change in the legal tide there was a corresponding shift in the political tide. With the original ruling now struck down, the question of the constitutionality of the program was rendered moot (at least for the moment). The only issue that remained to be dealt with was the class action lawsuits against the telecoms—the providers of the very data required to run the TSP—as well as the need to protect the administration and its agencies and departments against any further lawsuits in the event that any future plaintiffs could prove their legal standing in court.

Addressing the Remaining Legal Concerns

Several legal questions remained, not least of which was whether authorization of the program was within the president's powers. Even if it were, the constitutional questions as to whether NSA's data collection methods were in violation of Fourth Amendment rights also had to be taken into account. In his book, *In the Common Defense: National Security Law for Perilous Times*, military judge James E. Baker sets out a number of legal arguments facing the president and his legal advisors in response to both sides of the argument for and against presidential authority in authorizing the TSP. In presenting arguments for the program, Baker looks at the constitutional framework that established the president's powers as commander in chief. The courts have recognized that this power is not subject to legislative interference when acting in this capacity. In times of war, it is well agreed upon that "the president has no higher constitutional responsibility than to protect the United States from attack."[37]

Taking into account the fact that Congress cannot legislatively interfere with the president's wartime powers, FISA would in this sense be acting unconstitutionally if it impeded the president's ability to carry out his constitutional duties as commander in chief. Baker best sums up these arguments as follows:

> Based on the president's broad constitutional authority in the area of national security, including his authority to collect the intelligence necessary to effectively execute those duties, the president may lawfully authorize the TSP. This argument is enhanced to the extent the president determines the FISA requirements are impractical in application and prevent the president from undertaking his core security functions.[38]

In presenting arguments against the president's authority, Baker examines the constitutional framework as laid out by the Fourth Amendment, which provides a guarantee against unreasonable searches and seizures. As a matter of law, FISA requires that judicial approval for a warrant be obtained in order to conduct electronic surveillance within the United States. To argue that FISA would be unconstitutional in impeding the president's ability to conduct warrantless surveillance would ignore the fact that the statute allows him to conduct such surveillance in periods of declared war and in periods of emergency, when obtaining such a warrant may not be

possible given the time constraints involved. In those cases the warrant can be applied for after the fact. Baker sums up his arguments against as follows:

> Absent a compelling demonstration that the surveillance falls outside the FISA's parameters . . . presidential authorization of warrantless surveillance at best places the president at a low ebb of his authority. The better view, in light of the specificity of the statute, and the long-standing acquiescence of the executive in the Act's constitutionality, is that FISA did not leave the president at a low ebb in exercising residual inherent authority, but extinguished that authority.[39]

In examining these arguments, it is clear that there are merits on both sides, if the president is truly acting within his capacity as commander in chief. Assuming that he is acting within this capacity, the arguments on the side of the president seem strongest if FISA is actually impeding his ability to carry out those duties. What is not clear, though, is why FISA would actually be doing so. If it is possible to obtain such warrants without prior judicial approval, assuming that these can be easily gotten retroactively, then the argument for presidential authority begins to weaken. Of more concern, then, becomes the Fourth Amendment argument:

> The issue of whether the TSP violates the Fourth Amendment entails a reasonableness analysis that strikes a balance between governmental and individual interests.[40]

In examining this issue, Richard Henry Seamon presents the original three-part test as laid out by Justice Jackson in *Youngstown Sheet and Tube Co. v. Sawyer*. In this case, President Truman tried, albeit unsuccessfully, to take over the steel mills in order to ensure that they would produce enough steel for the Korean War effort. In this instance the Court rejected the president's commander-in-chief arguments on the grounds that although the president is commander in chief he is not commander of the country. That test puts in place a framework that, according to Justice Jackson, "reflects the interdependence of the President and Congress in certain matters, including war."[41] The test lays out three scenarios that rank presidential power against that of Congress in descending order of legitimacy, and it works as follows:

1. President acts with express or implied authority from Congress.
   - This is presidential power at its maximum.

2. President acts with neither congressional approval nor denial.
   - President must rely upon his own independent powers.
3. President acts in defiance of congressional orders.
   - This is presidential power at its "lowest ebb."[42]

By Seamon's analysis, the application of the same test in *Youngstown* to the TSP provides an interesting juxtaposition. As Seamon states:

> Justice Jackson's framework makes it important to determine whether the TSP is authorized by—or is instead inconsistent with—the express or implied will of Congress. The President argues that the TSP was authorized at its inception by the AUMF, but this argument lacks merit. Without the AUMF to support it, the TSP violates FISA and so presents Justice Jackson's third situation. Accordingly, the surveillance can fall within the President's power, despite violating FISA, only to the extent that Congress is constitutionally "disabled" from curbing the President's power.[43]

Although the Court in *Youngstown* did not find President Truman's actions to fall within the scope of the president's commander-in-chief powers, as such actions were not authorized by any statute or any extrastatutory power under the Constitution,[44] let us assume for argument's sake that this did not apply in the TSP case. Even if this were a genuine situation whereby wartime power applies, the question of the Fourth Amendment still requires consideration, since it would only seem sensible that whatever course of action the president took, his advisors should be advocating measures that would impair those rights as minimally as possible.

NSA's Bulk Telephone Metadata Collection and PRISM Programs under President Barack Obama

Similar in scope to the revelations regarding the TSP, recent news of the government's collection of millions of Verizon customers' telephone records, as well as its access to data held by nine of the nation's largest Internet service providers via the NSA's PRISM program, has been the subject of heated debate concerning the nature and extent of surveillance activities under the Obama administration. News of these NSA surveillance programs broke in both *The Guardian*[45] and the *Washington Post*[46] on June 6, 2013. *The Guardian* in its headline

story broke the news that the Foreign Intelligence Surveillance Court (FISC) had ordered Verizon, one of America's largest telecom providers, to provide on an "ongoing, daily basis" the NSA information on all telephone calls in its systems, both within the United States and between the United States and other countries.[47] The top-secret order (now known to have been leaked by Edward Snowden, a former technical contractor for the NSA) dated April 25, 2013, specified that the company comply with the order for a three-month period ending July 19, 2013.[48] As *The Guardian* article noted:

> The document shows for the first time that under the Obama administration the communication records of millions of US citizens are being collected indiscriminately and in bulk—regardless of whether they are suspected of any wrongdoing.[49]

The *Washington Post* simultaneously published in its lead story the claim that the NSA was tapping into the central servers of nine leading U.S. Internet companies (Microsoft, Yahoo!, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple) in order to extract "audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets."[50] However, "unlike the collection of those call records, this surveillance can include the content of communications and not just the metadata."[51]

According to the *New York Times*, all of the companies cited claimed they had no knowledge of a government program providing officials with access to its servers, and they drew a distinction between giving the government access to its servers and giving them specific data in response to individual court orders, including FISA orders.[52] As the *New York Times* notes:

> The negotiations, and the technical systems for sharing data with the government, fit in that category because they involve access to data under individual FISA requests. And in some cases, the data is transmitted to the government electronically, using a company's servers.[53]

The initial individual responses from companies were quick to distance themselves.

From Google:

> Google cares deeply about the security of our users' data. We disclose user data to government in accordance with the law, and we review all such requests carefully. From time to time, people allege that we have created a government "back door" into our systems, but Google does not have a "back door" for the government to access private user data.[54]

From Facebook:

> When Facebook is asked for data or information about specific individuals, we carefully scrutinize any such request for compliance with all applicable laws, and provide information only to the extent required by law.[55]

From Microsoft:

> We provide customer data only when we receive a legally binding order or subpoena to do so, and never on a voluntary basis. In addition we only ever comply with orders for requests about specific accounts or identifiers. If the government has a broader voluntary national security program to gather customer data we don't participate in it.

And from Yahoo!:

> Yahoo! takes users' privacy very seriously . . . We do not provide the government with direct access to our servers, systems, or network.[56]

Under FISA such government requests for company information would be legally enforceable. According to the *New York Times*, of the companies that negotiated with the government, those source(s) who were briefed on those discussions would only speak with the paper on the condition of anonymity, since they "were prohibited by law from discussing the content of FISA requests or even acknowledging their existence."[57]

The *New York Times* reported:

> in at least two cases, at Google and Facebook, one of the plans discussed was to build separate, secure portals, like a digital version of the secure physical rooms that have long existed for classified information, in some instances on company servers. Through these online rooms, the government would request data, companies would deposit it and the government would retrieve it, people briefed on the discussions said.[58]

In the very brief time that has passed since the Snowden leak, some of the same Internet service providers that were originally signaled out as taking part in the government surveillance programs have called for more openness. Yahoo! filed a motion with the FISC on June 14, 2013, asking it to release a 2008 FISC judgment that required the company to comply with government requests for user information under FISA.[59] On June 18, 2013, Google asked the FISC for permission to release the number of government requests it has received for user data, and a similar request was put forward by

Microsoft in June 19, 2013, for permission to share data about NSA requests for customer information.[60] As of writing this article, there has been no decision regarding the Google and Microsoft requests. However, in a surprise July 15, 2013, decision, FISC judge Reggie Walton ruled in Yahoo!'s favor, ordering the government to conduct a "declassification review."[61] The same FISC order provides the government with the opportunity to redact information it deems sensitive to national security, leading many to speculate how forthcoming the government will be when conducting its declassification review.[62]

The Government Response to the Leaks

The government response has been to defend the NSA programs. In a statement on June 7, 2013, President Obama responded to press questions regarding the government's surveillance of phones and Internet, by saying:

> When I came into this office, I made two commitments that are more important than any commitment I made: Number one, to keep the American people safe; and number two, to uphold the Constitution.[63]

With regard to all these programs, he responded that they were secret in the sense that they're classified, but that "the relevant intelligence committees are fully briefed on these programs. These are programs that have been authorized by broad bipartisan majorities repeatedly since 2006."[64]

Responding to the issue of telephone surveillance, the president went on to assure the public that "nobody is listening to your telephone calls."[65] He continued by saying that the intelligence community looks only at phone numbers and durations of calls. By sifting through this metadata, they may identify potential leads related to terrorism. The president made the claim that if the intelligence community wants to listen to a telephone call they would require approval from the FISC.[66]

With respect to the Internet surveillance, the president stated that such surveillance does not apply to U.S. citizens or people living in the United States. In summing up these programs, the president said that they were originally authorized by Congress, have been repeatedly authorized by Congress, and that Congress is continually briefed on how they are conducted. He emphasized that there were a range of safeguards in place, and that federal judges were overseeing the entire program.[67]

Perhaps of the more interesting remarks made by the president in his response to questions about the surveillance program were his comments regarding the need to balance liberty and security:

> One of the things that we're going to have to discuss and debate is how are we striking this balance between the need to keep the American people safe and our concerns about privacy? Because there are some tradeoffs involved.[68]

In regard to the issue of telephone surveillance, the president referred to any encroachments on individual privacy as modest and worth doing. He also stated that you can't have 100 percent security and also then have 100 percent privacy, noting that the American public would have to make some choices as a society. In evaluating the programs, the president said:

> They make a difference in our capacity to anticipate and prevent possible terrorist activity. And the fact that they're under very strict supervision by all three branches of government and that they do not involve listening to people's phone calls, do not involve reading the emails of U.S. citizens or U.S. residents absent further action by a federal court that is entirely consistent with what we would do, for example, in a criminal investigation—I think on balance, we have established a process and a procedure that the American people should feel comfortable about.[69]

The U.S. director of National Intelligence, James R. Clapper, in a June 8, 2013, statement, described the disclosure of PRISM as a "reckless disclosures of intelligence community measures used to keep Americans safe."[70] In the same statement he acknowledged existence of the PRISM program by name and said it had been mischaracterized by the media. He also defended the program as lawful and conducted under authorities approved by Congress.[71]

Since news of the story broke, the reaction from lawmakers has been mixed. Although there was quick and widespread condemnation of the Edward Snowden leak, many lawmakers from both parties have expressed skepticism about the bulk collection of Americans' telephone records, with some threatening not to renew the legislative authority that has been used to sanction the program.[72] According to a July 17, 2013, article in the *Washington Post*:

> The backlash appeared to focus on the concern that the Obama administration's interpretation of its powers far exceeds what lawmakers intended. At a hearing of the House Judiciary Committee, lawmakers

forcefully pressed officials from the National Security Agency, the Justice Department, the FBI and the Office of the Director of National Intelligence (ODNI) to justify the government's collection and storage of the communications records of vast numbers of Americans.[73]

Legal Challenges Ahead

While there is a public debate concerning the constitutional limits of such programs, there are important legal challenges underway. On June 11, 2013, the ACLU and the New York Civil Liberties Union filed a constitutional challenge to the telephone surveillance program. The plaintiffs in the lawsuit argue that the program violates the First Amendment protection of free speech and association and the Fourth Amendment protection against unreasonable search and seizure. There are also charges that the program exceeds the congressional authority provided by the PATRIOT Act.[74] As was noted, in the previous *ACLU v. NSA*, the plaintiffs were unable to prove legal standing. Taking into account that the government has acknowledged the existence of the telephone surveillance program and that the ACLU is a customer of Verizon Business Network Services, it would seem that they may now be able to argue that they have legal standing.[75] According to ProPublica's NSA Surveillance Lawsuit Tracker, as of July 16, 2013, a total of ten legal challenges and petitions had been filed. These challenges include the ACLU suit just discussed, as well as the Yahoo! petition for the FISC to release court documents showing how the company "objected strenuously" to an order compelling it to turn over customer data; the separate filings by Google and Microsoft asking the FISC for permission to release aggregate data about any FISC orders that each has received; and the Electronic Privacy Information Center (EPIC) petition asking the Supreme Court to void a secret court order compelling Verizon to provide customer data to the government; as well as the recent development in the Electronic Frontier Foundation's *Jewel v. NSA* (a class action lawsuit against AT&T for its role in the TSP) in which District Court judge Jeffrey S. White rejected the government's state secrets defense on July 8, 2013.[76]

The resurrection of the *Jewel* case is of particular interest for the following reasons. The case against the government was originally filed in 2008. In 2009, the Obama administration moved to dismiss

the suit, arguing that the information necessary to litigate the claims was subject to the state secrets privilege.[77] Without addressing the state secrets argument, the District Court instead dismissed the case on the grounds that the plaintiffs lacked standing. In 2011, the Court of Appeals reversed the district court's dismissal of *Jewel* and remanded, "with instructions to consider, among other claims and defenses, whether the government's assertion that the state secrets privilege bars this litigation."[78]

The July 8, 2013, ruling by Judge White rejecting the government's state secrets argument means that the important constitutional claims—that the program violates the First and Fourth Amendments of the U.S. Constitution—can now continue.[79]

Ethical Concerns

The response to the past disclosure of the TSP under President Bush, and the recent telephone and Internet surveillance programs operating under President Obama, both pro and con, require serious consideration. Utilitarian arguments concerning the prevention of harm—that is, the protection of national security interests—have been used as the justification for keeping such programs secret. The whistleblowers that made their existence known, in the government's view, have committed an act of treason. In releasing classified information, their actions, according to this view, had the potential to place the country in harm's way by revealing to the enemy the methods being used to collect information on terrorist activities—perhaps tipping off the enemy to use alternative means of communication in order to avoid detection. That being said, given the nature of the programs—which are secret—the only way to justify its existence on utilitarian grounds is to take the word of those officials who are party to the program. The consequentialist approach would seem to require lexically that: 1) it has in some demonstrable way prevented terrorist attacks, and 2) that the overall good it has achieved in meeting this goal has outweighed any harmful effect that has resulted in the reduction of civil liberties for those whose communications have been caught up in the sweep of the program.

In contrast to the utilitarian arguments, those who have expressed their concern that these programs violated protected Fourth Amendment rights under the Constitution have appealed largely to contractarian/rights-based arguments. In the case of the TSP, the fact that

this program operated under such a high level of secrecy, that it lay outside of the normal checks and balances, disregarding FISA as set out by Congress, and operating outside the normal judicial oversight of the FISC, makes it difficult, although not impossible, to defend on contractarian grounds. The caveat here is that to defend it on such grounds requires that the commander-in-chief arguments must be held above all others in the ordering of conflicting constitutional claims. In terms of wartime presidential power, this argument would certainly hold sway and would, most likely, be justified under a Rawlsian approach. However, as we have seen above, this argument is harder to defend in a perpetual war on terror where the threat level is increasingly difficult to measure and relies on a paternalistic, "trust us" approach to information sharing.

Although President Obama has used no such wartime-presidential-powers arguments in defense of the telephone and Internet surveillance programs that he has authorized, this does not make the arguments in favor of such programs any less paternalistic if the merits of the legal challenges now underway prove successful in demonstrating an overreach of power beyond what the Congress had intended for the president.

Given the secret nature of these programs and their intended purpose, which is to act as one of the many tools at the government's disposal to guard against future terrorist attacks, it becomes hard to evaluate the programs in the absence of specifics. Although those in the media have suggested what they think is going on through a number of confidential sources/whistleblowers,[80] these programs remain highly guarded, and thus it is not clear how they are actually operating.

Like many of the post-9/11 ethical debates, the defense of these programs has been framed in a utilitarian light, one that requires that the citizen trust the few members of the executive, and now legislative and judicial branches, who have been involved in the program to protect the greater good of their national security.

First is the issue of how corporations are used in the operation of such programs. In order to gather the data from which the NSA may mine for possible terrorist threats, the cooperation of telecommunications companies and major Internet service providers is required. If corporations are pressured into cooperation for fear of lost business or other reprisals, the government's position begins to lose some of that moral-high-ground luster.

Second, there remains the overarching concern about right to privacy as constitutionally guaranteed. Richard A. Posner asserts that in the chain of events (interception, data mining, and human searches) it is only the last event that raises constitutional and legal concern. His argument is that computer-generated searches are not actual impairments to an individual's privacy rights, but is this actually the case? The potential for targets being deemed of interest or appearing on watch lists before human searches are able to rule them out as false positives would arguably be just as damaging, if not more. To assert, as he does, that "[c]omputer searches do not invade privacy because search programs are not sentient beings"[81] appears disingenuous.

The concerns that these programs raise within the debate over privacy rights during times of insecurity have the potential to shape future legislation and to influence policy decisions at the highest levels. What is crucial here is the ability to maintain some kind of balance between the security concerns that the programs were set up to address and the civil liberties concerns that any infringement of protected Fourth Amendment rights entails.

The Path Forward: Seeking Proportionality among Competing Claims

In order to advance a means for moving forward, there is no simple calculus for how to balance liberty and security since both are equally important. That does not mean that there is no way forward, or that the discussion of the two will not bear fruit; it is merely to say that this research does not provide a calculus. What it aims to do is to advocate a test for achieving some kind of proportionality that is compatible with protecting the security of Americans while at the same time respecting their rights to privacy.

The potential for catastrophic consequences from acts of terrorism has reached a new peak, on par with acts of war perpetrated by individual states. As was seen on 9/11, the need for some sort of preemptive surveillance is crucial in order to prevent such attacks. That being said, the need for oversight and accountability to ensure that such preemptive collection of data is within the scope of the law is paramount. Several authors have advanced the idea of incorporating the proportionality of a "Terry stop" into electronic surveillance investigations where Fourth Amendment rights may be infringed.

Taking a cue from these authors, this article will now seek to build upon their ideas with a proposal that the courts use a more rigorous form of proportionality standard than that which the Terry stop currently provides.

Rather than inventing a new legal test, this work looks to the two-pronged test as laid out in the Canadian case of *R. v. Oakes*,[82] which seeks to do precisely that: balance the competing ethical concerns in cases in which an individual's rights may be limited under the Canadian Charter of Rights and Freedoms.[83] The proportionality model advocated in this paper is a modified version of the Oakes test. Although this model is based on Canadian rather than American jurisprudence, this should not be a deterrent to its use or applicability since what is of interest here is the ethical test itself—a test for balancing competing contractarian and utilitarian claims. Additionally it should be noted that there is an overwhelming mass of legal doctrine supporting the principle of proportionality from various foreign jurisdictions.[84]

Terry v. Ohio:[85] *Proportionality*

In the seminal case of *Terry v. Ohio* (1968), the U.S. Supreme Court held that the Fourth Amendment prohibition on unreasonable searches and seizures had not been violated in a case of a stop and frisk where a police officer had reasonable suspicion that a crime was about to be committed. In *Terry*, a plainclothes police officer observed two men whom he believed were "casing" a storefront with the intention of committing an armed robbery of the store. Upon a pat down[86] of the two men's clothing, weapons were discovered and seized. The Court ruled that such searches could be conducted without probable cause, so long as the officer had a reasonable suspicion that a crime had been, was being, or was about to be committed. Reasonable suspicion in such cases could not be based on mere intuition or a hunch, but rather it had to be based on "specific and articulable facts."[87] In its ruling the Court found that "there is 'no ready test for determining reasonableness other than by balancing the need to search (or seize) against the invasion which the search (or seizure) entails.'"[88]

This idea of incorporating the reasonableness of a search and seizure into the discussion of balancing liberty and security concerns is one that authors such as Christopher Slobogin, K. A. Taipale, and

Stephanie Cooper Blum have advocated. Slobogin in his work *Privacy at Risk* sets out a framework for proportionality that is built on two propositions. The first proposition is that the interest that the Fourth Amendment protects is security from unjustified government infringement on individuals' property, autonomy (in the sense of the ability to control one's movements), and privacy. The second proposition is that the greater the threat to that security, the greater justification the government should have to show.[89]

Starting with these two propositions, Slobogin seeks to use *Terry v. Ohio* as a case for proportionality that is compatible with any limitation on Fourth Amendment rights, one that is not just limited to a brief stop and frisk but one that might be applicable to various forms of government surveillance. His first proposition suggests that we need to protect against unjustified intrusions upon the right—but he does not suggest that no intrusion would ever be permissible. His second proposition suggests that any relaxation of the Fourth Amendment in the name of national security should not be automatic. That is to say, the government requires legal justification for any intrusion upon the right in question.

For Taipale, the use of a reasonable suspicion standard as found in *Terry* would combine the statutory mechanism for congressional authorization and oversight with an explicit statutory basis for judicial orders and review.[90] What is interesting here is that Taipale's proposal also incorporates the idea that "legitimate foreign intelligence requirements can be met without resorting to unilateral secret executive branch approvals or by shoehorning 'innovative' solutions not explicitly anticipated under *FISA*."[91] The idea of placing the ability to determine reasonableness, in this case balancing the need to search (or seize) against the intrusion that such a search presents for Fourth Amendment rights, back in the hands of the court is a promising one.

The analogy of using a traditional Terry stop, when trying to decide whether a warrantless search is justified, is one that Cooper Blum believes could be useful in any future amendment of FISA. According to Blum, "Congress should amend *FISA* to require probable cause that a terrorist (not just a foreign national as the FISA Amendments Act of 2008 (FAA) currently requires) has had contact with a U.S. person."[92] Cooper Blum incorporates Taipale's Terry stop suggestion as a means for continued surveillance for a given period on the U.S. person to determine if he is a terrorist. The use of

a Terry stop in the conducting of electronic surveillance, under these circumstances, would allow an authorized period for additional monitoring or initial investigation to determine whether the communications have any intelligence value.[93] As Cooper Blum notes, "If this follow-up surveillance revealed that the U.S. person was an agent of a foreign power, then a traditional *FISA* warrant could be obtained based on probable cause."[94] The end result would allow that "probable cause could still be the predicate standard for FISC ex ante review—but it would apply to a very different inquiry than is currently required under *FISA* and the *FAA*."[95]

As Slobogin, Taipale, and Cooper Blum note, the idea of a Terry-stop equivalent for electronic surveillance provides a useful analogy for potential FISA and FAA modification in instances involving U.S. persons (since these persons' communications would be outside the scope of FISA). If applied to cases involving electronic surveillance for foreign intelligence purposes, the flexibility that this new standard would allow—that is, a shift from probable cause to reasonable suspicion—would enable the government to engage in electronic surveillance for the purposes of identifying whether a U.S. person was actually engaged in the planning and/or commission of, or had already committed, a terrorist act.

A More Rigorous Proportionality: Oakes Test

The Court in *Terry v. Ohio* found that there is no ready test for determining reasonableness other than balancing the need to search (or seize) against the infringement of the right in question. The Court, in its ruling, has clarified that there must be proportionality in terms of the government's need to protect public safety and security against any infringement of an individual's Fourth Amendment rights. The need to balance these competing interests is evident in the Court's decision; however, the balancing mechanism used in *Terry* could be further clarified by incorporating another balancing mechanism used by the Canadian judiciary to ascertain when a protected charter right may be subject to limitation.

In the Canadian context, the use of the Oakes test for determining when a charter right[96] may be subject to limitation is compatible with the need for proportionality as demonstrated in *Terry*. In the case of *R. v. Oakes*, David Edwin Oakes was arrested by police officers, who found eight one-gram vials of hash oil in his possession.

At that time Section 8 of the Narcotics Act stipulated that once the Court has determined that an individual was in possession of illegal narcotics, the burden of proof was on the individual to demonstrate that he or she was not in possession of them for the purposes of trafficking (a much more serious crime). Oakes challenged that the reverse onus of proof was contrary to Section 11 (d) of the Canadian Charter of Rights and Freedoms, which guarantees the right to be "presumed innocent until proven guilty."[97] In addressing the charter challenge, the Supreme Court of Canada had to consider whether Section 8 of the Narcotics Act could be saved under Section 1 of the charter, which states that:

> The Canadian Charter of Rights and Freedoms guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.[98]

In addressing this concern, the Court developed what has come to be known as the Oakes test, which is a test that is used to determine the constitutionality of legal limitations on charter rights as a whole (although this case dealt with a search and seizure, the test is applicable to all charter rights). This test is the model used in Canada to determine if a limitation by the government on a protected charter right is a reasonable limitation of the right being infringed. The Court found that the Crown must be able to demonstrate, on the balance of probabilities, the following:

1. Purpose or Objective of the Law
   The law must be a response to a *pressing and substantial* problem in order to consider overriding a charter right.
2. Proportionality
   In order to arrive at a calculation of the suitability of the means used to pursue the law's objective, the following three questions must be answered:
   (a) Are the means rational and nonarbitrary?
   (b) Is there minimal impairment to the right?
   (c) Is the good that will be achieved by these means sufficient to outweigh the negative effects caused by the infringement of the right in question?

The resulting test in *Oakes* is really an ethical test that seeks to balance the contractarian concerns (upholding the right itself) against

the utilitarian concerns (protecting the greater good), and its application should not be simply limited to the Canadian context. Indeed, the Court's ruling in *Terry v. Ohio*, which called for balancing the need to search (or seize) against the invasion that the search or seizure entails, demonstrates that the Court knew it needed to address both concerns, making it compatible with the proportionality test as laid out in the Oakes test.

When applying the Oakes test to the Fourth Amendment cases, the following two objectives must be satisfied in order to override the right in question: (1) the law must be a response to a pressing and substantial concern; (2) the law must be proportional; that is, that the good that will be achieved by the law in question must outweigh the negative effects caused by the law. Proportionality is further determined by the application of the three-part proportionality test (outlined above). The first part of this test requires that the limit on the right be rationally connected to the legislative objective of the law. Second, the government must demonstrate that the limit on the right in question represents the least restrictive means of achieving this objective. And lastly, the third part examines whether the collective benefits to society as a whole outweigh its individual costs.[99] The Oakes test combines both contractarian (2.a & 2.b) and utilitarian elements (2.c) in its assessment of the overall proportionality of any legislation that impinges on a protected right.

Slobogin, Taipale, and Cooper Blum point to the need for a proportionality standard in conducting electronic surveillance; however, the level of proportionality afforded by *Terry* is insufficient to this task. If we examine the circumstances in *Terry* and apply them against the Oakes test criteria, this becomes clearer. In terms of the purpose or objective of the law (part 1 of the Oakes test), *Terry* allows for a reduction of the probable-cause standard to one of reasonable suspicion in order to allow law enforcement officials to apply investigative techniques in situations in which they believe a crime has, is, or will be committed by a potentially armed suspect. The case could be made that combating this type of crime is a "pressing and substantial" concern for society as a whole and thus requires a relaxation in the standard so that law enforcement officials have an additional tool at their disposal to best address the problem. In terms of the proportionality aspect (part 2), *Terry* only really addresses the last part of the proportionality test (2.c); that is, the utilitarian aspect of the test.

Applying *Terry* to the proportionality test in part 2 of the Oakes test is revealing. Responding to each of the questions posed in part 2 reveal the following:

2. (a) Are the means rational and nonarbitrary?

The stop and frisk for weapons is connected to protecting the safety of the officers investigating a person who they believe has, is, or is about to commit a crime. The lowered standard from one of probable cause to reasonable suspicion is deemed necessary for the protection of the officers. The reduced standard also ensures that the exclusionary rule[100] is not applicable on the grounds of unlawful search and seizure. The Court has specified that the only restriction on this reduced standard is that the officers must be able to demonstrate "specific and articulable facts"[101]—this reasonableness criterion is one that the court has said there is "no ready test for determining reasonableness other than by balancing the need to search [or seize] against the invasion which the search [or seizure] entails."[102] What would have otherwise been a contractarian test in *Oakes* would now seem to rest on a utilitarian calculus as a result of this last criterion, which is slightly problematic because the "right" is now subject to a weighing of harms rather than having the emphasis remain on whether or not the right has actually been infringed in any absolute sense.

2. (b) Is there minimal impairment to the right?

The Court in *Terry* has pointed to the need to balance the "search (or seize) against the invasion which the search (or seizure) entails,"[103] suggesting that minimal impairment to the right is key to the successful application of the Terry stop standard; however, the court does not enter into a discussion of possible alternatives that might take the place of a Terry stop.

2. (c) Is the good that will be achieved by these means sufficient to outweigh the negative effects caused by the infringement of the right in question?

The implication in *Terry* is that the answer is yes—that a stop and frisk that results in the apprehension of an individual who has, is, or is about to commit a crime and is believed to be armed with a weapon outweighs the negative effects so long as it is based on reasonable suspicion rather than a mere hunch.

A simple application of the grounds laid out in *Oakes* would demonstrate the utilitarian nature of the original decision in *Terry*. The real strength in *Oakes* is that it combines both the contractarian and

utilitarian tests in order to provide a better overall protection for rights against purely utilitarian reasoning. *Oakes* provides a test that is easily generalizable and transferable, making application of the test by subsequent courts consistent—unlike the American decisions that have cited *Terry* in their rationale. These courts have worked to expand the definition of a Terry stop by extrapolation rather than through the application of a clearly defined test like the one laid out in *Oakes*.[104]

In the Canadian context, the Oakes test is used to test limitations on all Canadian charter rights, not just those involving search and seizure, which would require that the principles laid out in the test could be applied to all such protected rights. The reasoning implied in the Terry stop is utilitarian in nature; combining it with the contractarian principles in the Oakes test would yield better protections for the Fourth Amendment rights in a way that is generalizable enough to easily encompass electronic surveillance under FISA. A modified Oakes test could take the following form:

1. Purpose or Objective of the Law
   The law must be a response to a *pressing and substantial* problem in order to reduce the standard of probable cause to one of reasonable suspicion under the Fourth Amendment.
2. Proportionality
   In order to determine the suitability of this lowered standard, the infringing statute must:
   (a) be rational and nonarbitrary
   (b) result in minimal impairment to the right
   (c) demonstrate that the good that will be achieved by such infringement sufficiently outweighs any deleterious effect on the Fourth Amendment

This modified version of the Oakes test, unlike the Terry stop advocated by Slobogin and others, would provide the courts with a more rigorous tool for calculating the proportionality of any proposed limitation on Fourth Amendment rights under FISA regarding the standard accorded to electronic surveillance: reasonable suspicion versus probable cause. If the proposed amendments were able to prevail over what is essentially a combination of contractarian and utilitarian tests, the Court would be in a better position to actually determine the reasonableness of a search or seizure rather than

simply having to appeal to a utilitarian calculus for "balancing the need to search (or seize) against the invasion which the search (or seizure) entails."[105]

The Future of Privacy in Post-9/11 America

What are the boundaries limiting government intrusion on privacy rights, and how are such boundaries drawn?

As a central research question, this is a complicated and difficult question to attempt to answer. Regardless, it is a question that needs to be asked. The Terrorist Surveillance Program (TSP) under President Bush, and telephone and Internet surveillance programs under President Obama, raise questions concerning the constitutional limits of such surveillance programs and provide a means for testing the above research question in a way that is narrowly focused on the government's use of electronic surveillance and its impact on protected Fourth Amendment rights.

The ethical, legal, and political considerations with regard to the collection, classification, and dissemination of intelligence information are many. Clearly the government has a duty to protect the national security of its citizens, but that duty must also be balanced against a competing duty to uphold the Constitution. In the American context, the place of Fourth Amendment rights in foreign intelligence investigations has been vigorously debated in the post-9/11 period. The need to balance competing rights claims is not simply an academic exercise; it is of practical concern at a time in which heightened security concerns have indeed resulted in an encroachment on civil liberties. The final outcomes of the current legal challenges facing the government in regard to its surveillance programs will further define the boundaries of such intrusions on otherwise protected rights.

Initially 9/11 provided the exceptional circumstances that seemed to justify a reduction in privacy rights in the interest of national security. The TSP revelations of 2005 and the revelations concerning the telephone and Internet surveillance programs operating in 2013 bring those same privacy concerns to the forefront. The need for a public discussion (of the sort President Obama claims he welcomes) about the reasonableness of such limitations on civil liberties, particularly Fourth Amendment rights in the face of terrorist threats,

is of the utmost importance, because such a debate will inform the steps taken by lawmakers to either amend or draft new legislation related to foreign intelligence surveillance.

Developing an Ethical Framework

The ethical framework advanced in this paper seeks to incorporate individual rights–based (contractarian) concerns along with the collective consequentialist (utilitarian) concerns that arise from any threat to national security. This is not to suggest that other ethical theories could not have been used to address this question—for example, Kantian and Communitarian ethical theories could be used to address the same questions. The underlying rationale for trying to incorporate the utilitarian and contractarian approaches was based largely on the fact that these two ethical approaches have been used at cross-purposes with no ground for compromise. If the choices are framed as civil liberties versus national security, there clearly will be no room for compromise.

The cornerstone argument for programs such as the TSP and other NSA telephone and Internet surveillance programs are for the most part utilitarian "prevention of harm" ethical arguments. But do such utilitarian arguments suffice? Part of the problem in assessing whether or not the means used to prevent such harm to national security is justified is the fact that much of the information required to make such a calculation is secret and therefore beyond the bounds of discussion. That is not to diminish an administration's need for secret information—clearly there is a need for that—but such information requires a certain level of congressional and judicial oversight if the administration is to be held accountable for its actions and the absence of such oversight paves the road for potential abuses. This is precisely why the legal challenges will prove so important, since the judiciary is in a position to compel the government to provide the requisite information needed in order to arrive at any such calculation regarding the proportionality of any infringement upon otherwise protected Fourth Amendment rights arising from the operation of the surveillance programs in question.

Need for Checks and Balances

What are the boundaries limiting government intrusion on privacy rights, and how are such boundaries drawn?

From a legal and political point of view, this research question implies that there should be some sort of check on government power. The fundamental means by which the U.S. Constitution establishes such a check is through the division of powers. By establishing a system of government with three distinct branches—executive, legislative, and judicial—the founding fathers were clear in their intention to build a system that possessed the necessary checks and balances. Thus, any discussion on the limitation of government powers should also involve a discussion of all three branches and their ability to keep each other in check. That is to say, that except for any true instances of presidential wartime powers, of the sort that James E. Baker describes, the executive does not have a monopoly on determining the limitation of Fourth Amendment rights in times of increased threats to national security.

All three branches of government need to be involved in the discussion of civil liberties in a time of heightened threats to national security. The need for reasonableness in any attempt to override a constitutionally protected right, such as the Fourth Amendment, should be of the highest concern for each of these branches. Building upon the suggestions put forth by authors such as Christopher Slobogin, K. A. Taipale, and Stephanie Cooper Blum, to incorporate the equivalent of a Terry stop for determining the reasonableness of electronic surveillance under FISA where American persons are involved, this research has outlined the limitations of *Terry* and instead advocated for the use of a modified Canadian Oakes test as a model for achieving a more rigorous form of proportionality test.

The modified Oakes test as presented in this paper balances the contractarian concerns—that is, the importance of the right being infringed against the utilitarian concerns—with the government's need for the limitation of the right in instances in which a lack of limitation has the potential for great harm. If the courts were to apply such a test to any of the legal challenges cited in this paper, the application of such a precedent would be instructive to both the executive and legislative branches in their lawmaking. If such a test were to be adopted by the courts, it would provide all three branches with a tool for assessing whether any potential override or limitation upon a protected right is indeed permissible under the Constitution and is ethically based. It would be particularly instructive for lawmakers in that it would allow them to theoretically test any new or amended legislation before it reaches a stage at which the courts are

asked do so for them in a constitutional legal challenge, such as the ones they are now facing.

Notes

1. Glenn Greenwald, Ewen MacAskill, and Laura Poitras, "Edward Snowden: The Whistleblower behind the NSA Surveillance Revelations," *Guardian*, June 9, 2013, http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

2. Ibid.

3. Greenwald, MacAskill, and Poitras, "Edward Snowden: The Whistleblower."

4. Utilitarianism is a form of consequentialism first expounded by Jeremy Bentham that views pleasure as being unquestionably good and pain and suffering as unquestionably bad. The rightness or wrongness of an action, law, or policy depends upon its ability to maximize pleasure and/or minimize suffering.

5. Contractarianism is a rights-based approach to morality and ethics that takes into account the differing types of rights, both positive and negative, and the roles and responsibilities of citizens and governments to uphold and protect those rights. This relationship between citizens and their government takes the form of a social contract.

6. The case of *Jewel v. NSA* was filed by the Electronic Frontier Foundation against the NSA on behalf of AT&T customers in response to the revelations regarding the government's surveillance of communications on AT&T networks. On July 8, 2013, District Court Judge Jeffrey S. White refused to dismiss the lawsuit under the state secrets privilege.

7. James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers without Courts," *New York Times*, December 16, 2005, http://www.nytimes.com/2005/12/16/politics/16program.html?ex=1292389200&en=e32070e08c623ac1&ei=5089.

8. Katherine Wong, "The NSA Terrorist Surveillance Program," *Harvard Journal on Legislation* 43, no. 2 (2006): 517.

9. *New York Times*, "Bush on the Patriot Act and Eavesdropping," December 18, 2005, http://query.nytimes.com/gst/fullpage.html?res=9A05E6D61630F93BA25751C1A9639C8B63.

10. WhiteHouse.gov, "The President's Radio Address," December 17, 2005, http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html.

11. Ibid.

12. Wilson R. Huhn, "Congress Has the Power to Enforce the Bill of Rights against the Federal Government; Therefore FISA Is Constitutional

and the President's Terrorist Surveillance Program Is Illegal," *William & Mary Bill of Rights Journal* 16 (2007): 537.

13. WhiteHouse.gov, "The President's Radio Address."

14. Ibid.

15. Jon D. Michaels, "All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror," *California Law Review* 96 (2008): 901 at 907.

16. American Civil Liberties Union, "Fact Sheet: Legal Claims in *ACLU v. National Security Agency*," January 17, 2006, http://www.aclu.org/national-security/fact-sheet-legal-claims-aclu-v-national-security-agency.

17. Ibid.

18. Electronic Frontier Foundation, "NSA Multi-District Litigation," December 8, 2009, http://www.eff.org/cases/att.

19. Stephen Manuel Wolfson, "National Security Surveillance and National Authentication System: The NSA, AT&T, and the Secrets of Room 641A," *I/S: A Journal of Law & Policy for the Information Society* 3 (2008): 411, at 417.

20. Mark Hosenball, "Spying: Giving Out U.S. Names: National Security Agency's Release of Names of Americans on 'Intercept' List," *Newsweek*, May 2, 2006: 10.

21. Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," *USAToday*, May 11, 2006, http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

22. Seymour M. Hersh, "National Security Dept. Listening In," *New Yorker*, May 29, 2006, http://www.newyorker.com/archive/2006/05/29/060529ta_talk_hersh.

23. Ibid.

24. PBS, "Frontline: Spying on the Home Front (streamed video)," 2007, http://www.pbs.org/wgbh/pages/frontline/homefront/.

25. Jim Drinkard, "Verizon Says It Isn"t Giving Call Records to NSA," *USA Today*, May 16, 2006, http://www.usatoday.com/news/washington/2006-05-16-verizon-nsa_x.htm.

26. Ibid.

27. Ryan Singel, "Whistle-Blower Outs NSA Spy Room," *Wired,* April 7, 2006, http://archive.wired.com/science/discoveries/news/2006/04/70619.

28. Richard A. Posner, "Privacy, Surveillance, and Law," *University of Chicago Law Review* 75 (2008): 245, 253.

29. *ACLU v. Nat"l Sec. Agency/Central Sec. Serv.*, 438 F. Supp. 2d 754, 2006 U.S. Dist. LEXIS 57338 (2006).

30. Ibid.

31. Judges have the ability to "stay" a ruling if they know an appeal is imminent. What that means is that rather than changing the law immediately (i.e., striking it down a law as unconstitutional), the judge can provide

their ruling but temporarily suspend it pending the appeal. This means that we have the rationale for their ruling, but the ruling itself cannot take effect either until the proscribed amount of time has passed or the higher court has ruled on the appeal case.

32. *ACLU v. NSA/Central Sec. Serv.*, 467 F.3d 590, 2006 U.S. App. LEXIS 32346 (6th Cir., 2006).

33. After the news of the program broke, Gonzales was making appearances on programs such as PBS's *NewsHour with Jim Lehrer* to defend the president's actions as constitutional. See January 23, 2006, transcript of interview for the program, http://www.pbs.org/newshour/bb/law/jan-june06/gonzales_1-23.html.

34. Eric Lichtblau and David Johnston, "Court to Oversee U.S. Wiretapping in Terror Cases," *New York Times*, January 18, 2007, http://www.nytimes.com/2007/01/18/washington/18intel.html.

35. *ACLU v. NSA*, 493 F.3d 644, 2007 U.S. App. LEXIS 16149 (6th Cir.) (6th Cir. Mich., 2007).

36. Ibid.

37. James E. Baker, *In the Common Defence: National Security Law for Perilous Times* (Cambridge: Cambridge University Press, 2007).

38. Ibid.

39. Ibid.

40. Richard Henry Seamon, "Domestic Surveillance for International Terrorists: Presidential Power and Fourth Amendment Limits," *Hastings Constitutional Law Quarterly* 35, no. 3 (2008): 449 at 466.

41. Ibid.

42. Ibid., 469.

43. Ibid., 469.

44. Ibid., 467.

45. Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *Guardian*, June 5, 2013, http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order.

46. Barton Gellman and Laura Poitras, "U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program," *Washington Post,* June 7, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?tid=ts_carouselhttp://www.washingtonpost.com/investigations/us-inte.

47. Greenwald, "NSA Collecting Phone Records."

48. Ibid.

49. Ibid.

50. Gellman and Poitras, "U.S., British Intelligence Mining Data."

51. Glenn Greenwald and Ewen MacAskill, "NSA Prism Program Taps in to User Data of Apple, Google and Others," *Guardian*, June 6, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

52. Claire Cain Miller, "Tech Companies Concede to Surveillance Program," *New York Times*, June 7, 2013, http://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html?pagewanted=all&pagewanted=print.
53. Ibid.
54. Greenwald and MacAskill, "NSA Prism Program."
55. Barton Gellman and Laura Poitras, "U.S. Mines Internet Firms' Data, Documents Show," *Washington Post*, June 7, 2013, LexisNexis Academic.
56. Ibid.
57. Cain Miller, "Tech Companies Concede to Surveillance Program."
58. Ibid.
59. Benjamin Minegar, "Paper Chase: Secret Court Allows Yahoo to Disclose NSA Data Requests," *JURIST—Legal News and Research*, July 16, 2013, http://jurist.org/paperchase/2013/07/yahoo-allowed-to-disclose-nsa-data-requests-fisc.php.
60. Mark Clayton, "Snowden Leaks Give New Life to Lawsuits Challenging NSA Surveillance Programs," *Christian Science Monitor*, July 18, 2013, http://www.csmonitor.com/USA/Justice/2013/0718/Snowden-leaks-give-new-life-to-lawsuits-challenging-NSA-surveillance-programs.
61. Ryan Gallagher, "Yahoo Wins Crucial FISC Battle in Secret PRISM Spying Case," *Slate Magazine*, July 16, 2013, http://www.slate.com/blogs/future_tense/2013/07/16/yahoo_wins_crucial_fisc_battle_in_secret_prism_spying_case.html.
62. Minegar, "Paper Chase."
63. President Barack Obama, "Statement by the President," The White House, June 7, 2013, http://www.whitehouse.gov/the-press-office/2013/06/07/statement-president.
64. Ibid.
65. Ibid.
66. Ibid.
67. Ibid.
68. Ibid.
69. Ibid.
70. Timothy Gardner and Mark Hosenball, "Spy Agency Seeks Criminal Probe into Leaks," *Reuters*, June 9, 2013, http://www.reuters.com/article/2013/06/09/us-usa-security-clapper-idUSBRE9570GL20130609.
71. Ibid.
72. Sari Horwitz and William Branigin, "Lawmakers of Both Parties Voice Doubts About NSA Surveillance Programs," *Washington Post*, July 17, 2013, http://www.washingtonpost.com/world/national-security/house-committee-holds-hearing-on-nsa-surveillance-programs/2013/07/17/ffc3056c-eee3-11e2-9008-61e94a7ea20d_story.html.
73. Ibid.
74. American Civil Liberties Union, "ACLU Files Lawsuit Challenging Constitutionality of NSA Phone Spying Program," June 11, 2013, http://

www.aclu.org/national-security/aclu-files-lawsuit-challenging-constitutionality-nsa-phone-spying-program.

75. Charlie Savage, "A.C.L.U. Files Lawsuit Seeking to Stop the Collection of Domestic Phone Logs," *New York Times*, June 11, 2013, http://www.nytimes.com/2013/06/12/us/aclu-files-suit-over-phone-surveillance-program.html?pagewanted=all.

76. Kara Brandeisky, "NSA Surveillance Lawsuit Tracker," ProPublica, July 10, 2013, projects.propublica.org/graphics/surveillance-suits.

77. Electronic Frontier Foundation, *Jewel v. NSA*, https://www.eff.org/cases/jewel.

78. *Jewel v. NSA*, 673 F.3d 902, 913-14 (9th Cir. 2011).

79. Electronic Frontier Foundation, *Jewel v. NSA*.

80. Greenwald and MacAskill, "NSA Prism Program."

81. Richard A. Posner, "Privacy, Surveillance, and Law," *University of Chicago Law Review* 75 (2008): 245.

82. *R. v. Oakes* [1986] 1 S.C.R. 103, 26 D.L.R. (4th) 200.

83. Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.) 1982, c. 11. lays out the rights and freedoms that are entrenched in the Canadian Constitution.

84. Jonas Christoffersen, *Fair Balance: Proportionality, Subsidiarity and Primarity in the European Convention on Human Rights* (Leiden, Netherlands: Martinus Nijhoff, 2009), 31.

85. *Terry v. Ohio*, 392 U.S. 1 (1968).

86. The officer did not proceed to search inside the men's clothing until he had felt the weapons. The court viewed the frisk of the outer garments for weapons as being less than a full-blown search.

87. *Terry v. Ohio* as cited in Christopher Slobogin, *Privacy at Risk: The New Government Surveillance and the Fourth Amendment* (Chicago: University of Chicago Press, 2007), 22.

88. Ibid., 21.

89. Ibid., 23.

90. K. A. Taipale, "The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance," *Yale Journal of Law & Technology* 9 (2007): 128 at 161.

91. Ibid., 161.

92. Stephanie Cooper Blum, "What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform," *Boston University Public Interest Law Journal* 18 (2008): 269 at 311.

93. Ibid., 309.

94. Ibid., 309.

95. Ibid., 311.

96. The phrase *charter right* is commonly used to refer to a constitutionally protected right as laid out in the Charter of Rights and Freedoms.

97. *R. v. Oakes* [1986] 1 S.C.R. 103, 26 D.L.R. (4th) 200.

98. Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.) 1982, c. 11.

99. C. P. Manfredi and M. E. Rush, *Judging Democracy* (Peterborough, Ontario: Broadview Press, 2008), 34.

100. If weapons are found, the argument that such evidence should be excluded in Court because the weapons were found as a result of an unlawful search and seizure would not be applicable.

101. *Terry v. Ohio*, 392 U.S. 1 (1968).

102. Ibid.

103. Ibid.

104. The Supreme Court used the precedent set in *Terry v. Ohio* as the grounds for its ruling in *Michigan v. Long*, 463 U.S. 1032 (1983) that car compartments could be searched if an officer had reasonable suspicion that they contained a concealed weapon.

105. Ibid.

Michelle Louise Atkin is the associate librarian at Algoma University and an adjunct law professor in Canada at Algoma University and at Carleton University. This article is based on her recently published book, *Balancing Liberty and Security: An Ethical Study of U.S. Foreign Intelligence Surveillance, 2001–2009* (Rowman & Littlefield, 2014).