A Patchwork of Policy:
Growing Government Policy with Internet Expansion

Jana Michelle Kovitch
Public Policy Analysis
Senior
Abstract submitted for SPEA Undergraduate Honors Thesis Presentation

Professor Beth Cate
Associate Professor
Adjunct Associate General Counsel
School of Public and Environmental Affairs
Indiana University
Faculty Mentor
A Patchwork of Policy: The Problems with Old Framework for New Ideas

Jana Michelle Kovich
Public Policy Analysis
Senior
Abstract submitted for SPEA Undergraduate Honors Thesis Presentation
May 2012

Professor Beth Cate
Associate Professor
Adjunct Associate General Counsel
School of Public and Environmental Affairs
Indiana University
Faculty Mentor
ABSTRACT

The advent of the Internet brought with it a revolutionary way to disseminate information. E-mail, Facebook, Twitter and YouTube, used by over five hundred million people globally, provide excellent social networking and communication opportunities. Such websites help people continents apart connect, as well as spread ideas such as democracy and revolution. Individuals can also connect through blogs, forums, chats, or websites dedicated to publishing factual and often sensitive information, such as the controversial Wikileaks. The constant flow of data that defines the twenty-first century also poses a new question for American policy. Policy makers in the United States and around the world must find the balance between the public good promoted by free expression and the potential damage done by dissemination of military and other classified or sensitive information.

First, I address the background and current legal status of Wikileaks and other groups focused on freedom of information, such as Anonymous. I then explore the actions the United States is taking against further dissemination of secret information from our government. A variety of statutes, treaties, judicial opinions and guidelines form the backbone of cyber security laws. Information presented on the Internet, however, transcends domestic laws into the realm of international law. To understand how American security needs and freedom of expression principles stack up against international treaties and agreements, one must view the question from a forward-looking perspective.

The legal frame that a patchwork of legislation and precedent provides is not substantial enough to effectively stand against global propagation of sensitive data. Policy makers must examine if law is even the appropriate mechanism for combatting these issues. Further policy regarding proper E-mail and social networking procedures for government employees can help reduce the risk of improper information dissemination. This field will continue to expand exponentially, and policy must adapt to ever-changing technological circumstances.
The Internet defines the twenty-first century. It shapes research, self-expression and social interactions. It allows split-second proliferation of ideas and participation in commerce across the globe. The advent of the Internet has shrunk borders and brought people together from across the globe. Each year what one can accomplish online grows exponentially.

With increased data sharing online comes increased risk that sensitive or even classified information will appear on the Internet. Despite the accelerated rate at which the Internet has come to steer modern life, policy and law governing what data disclosures are, and are not, appropriate are slow to catch up. A patchwork of policy and legal precepts forms the backbone of American cyber security law. This current system for evaluating the legality of online (and thus generally cross-border) information sharing creates a dilemma for policymakers.

This essay provides an overview of current online data security practices and policies, the associated complications, and a survey and analysis of potential solutions suited for the twenty-first century. The examination of new groups such as WikiLeaks and Anonymous in juxtaposition with a patchwork of old policy set to combat information leaks reveals serious cyber threats to international security and substantiates concerns about protecting freedom of speech. Any proposed solution must find a balance between these two competing interests to protect both American security and freedoms. To create a proper solution, the type of truly harmful information that necessitates protection by law from dissemination must be examined. This responsibility to national security then must be weighed against the government's duty to uphold free speech, as well as the benefits derived from
increased communication between the government and citizens and the accountability that comes with a well-informed populace.

To understand the depth of the problem with current policy, the trends of Internet users and dissemination of information online must be appropriately assessed. Over 2.2 billion people worldwide use the Internet in all six inhabited continents.¹ Each of these users can access information posted online, although in some cases with restrictions. Although this global usage of the Internet continues to shrink borders and connect people worldwide, it also poses a threat to protected information. The threats may come from a variety of online activities and communications; three Internet phenomena on which this paper focuses are activities designed to combat government secrecy and promote transparency and accountability (for convenience, “anti-secrecy”); hacking, including “hactivism”; and social networking by government employees.

The Platforms for Propagation

Anti-Secrecy Efforts

Australian national Julian Assange founded the anonymous media organization and antisecrecy website WikiLeaks.org in 2006 on the principle that the operations of governments and corporations should be transparent, and thereby accountable, to citizens and shareholders.² WikiLeaks first sparked national interest in 2008, when an American federal judge took notice of the website, which

since its founding had published over a million government and corporate
documents gained from undisclosed sources, including thousands of documents
concerning the conduct of the wars in Iraq and Afghanistan. The federal judge
ordered WikiLeaks’ domain provider to shut down the web address, evoking a
response from many concerned citizens, journalists and bloggers, who believed this
mandate to violate First Amendment rights. The judge reversed his order to
disable the website after he experienced a large amount of criticism and court filings
citing First Amendment violation. The judge, Jeffrey Wise of San Francisco, stated
that, “We live in an age...when people can do some good things and people can do
some terrible things without accountability necessarily in a court of law.” Since this
2008 reversal, WikiLeaks has gone on to publish thousands of additional records,
including diplomatic cables and other sensitive information.

In Fall 2011, WikiLeaks published over 100,000 non-redacted cables, which
quickly were quickly picked up and reproduced on other websites all over the
Internet. Up until this point, WikiLeaks had worked with several newspapers, such
as The New York Times and the UK’s The Guardian, to gradually publish cables that
had sensitive identities redacted. WikiLeaks reported to the press shortly after

---

http://www.nytimes.com/2008/02/21/opinion/21thu3.html?_r=1&ref=wikileaks
7 Shane, Scott. “Spread of Leaked Cable...”
that its change in approach and consequent rapid publication of the sensitive information was done in alignment with WikiLeaks’ mission to provide information to all for the purpose of “bringing important news and information to the public” in an “innovative, secure and anonymous way for sources”. In the cables, names of confidential informants to the US government were released. This action, and WikiLeaks’ prior disclosure of war records, put WikiLeaks center-stage in a debate about American security and government secrecy. Government officials condemned WikiLeaks, claiming that releasing sensitive or classified information such as names of foreign citizens working with the State Department or other US agencies put those people in danger. Critics of governmental secrecy denounced the US government for keeping information classified even after WikiLeaks released that information online. For example, the ACLU requested in April 2011 diplomatic cables regarding Guantanamo from the State Department. The cables were some of the thousands that WikiLeaks released later that year, but after WikiLeaks’ disclosure the State Department still responded that half of the cables could not be released to the ACLU because they constituted classified information, and the other half would first be redacted to remove sensitive information. The ACLU litigator Ben Wizner knew that the State Department would react in this way, but he

---


9 Ibid.

wanted to “in part...expose the absurdity of the U.S. secrecy regime.”

Because WikiLeaks published the same materials without excisions, it is easy to see what kind of content the State Department classifies; the vast majority is content that would perhaps cause tension in international relations, such as reports from the London embassy about the British government’s negative view on Pakistan. Although the State Department claims this information could pose a threat to national security, it calls into question what kind of information is truly sensitive and deserves classification, as discussed in further detail below.

In the past two years, the US government and other governments around the world have made efforts to punish the individuals involved in WikiLeaks—both those leaking documents to WikiLeaks, and WikiLeaks itself for publishing the documents. Legally, the framework for punishing the original leakers is more well established, as discussed further below. In the US, former Private Bradley Manning stands trial this year on the charges of leaking over 350,000 secret cables to WikiLeaks in violation of several different laws disallowing dissemination of classified information. Private Manning could face life in prison if convicted. Overseas, the Swedish government continues to work on an extradition request for Assange to be transferred from Britain, where he is currently under house arrest, so

11 Ibid.
12 Ibid.
that he may face charges of sexual misconduct against a pair of Swedish WikiLeaks volunteers.\textsuperscript{15} A grand jury in the United States is currently investigating whether the U.S. may prosecute Julian Assange and other high-level WikiLeaks activists for publishing classified information, though such previous actions against publishers for leakages have been unsuccessful due to freedom of speech complications.\textsuperscript{16} Prosecution in the US, just as the current charges in Sweden, requires extradition, which adds an additional complication, discussed in more detail below.

While Assange remains in Britain, debate continues over the impact of WikiLeaks' activities and whether the initial shock and awe of WikiLeaks has faded. Some believe WikiLeaks is quickly becoming irrelevant, including New York Time's journalist Ben Keller. He wrote in his article “WikiLeaks, A Postscript,” that WikiLeaks did not, in fact, change the world all that much. He highlights a very interesting effect that WikiLeaks has had on the information world. Rather than inspiring a deluge of leaks and uprising of whistleblowers, WikiLeaks has encouraged agencies to tighten security, making leaks even more difficult to come by.\textsuperscript{17} Keller suggests that this effect may have changed the world in the opposite way of what WikiLeaks intended—making information leakages harder to come by and easier to prevent. Whether or not Keller's views hold true, leaks are unlikely to disappear entirely or even decrease for reasons discussed below regarding


\textsuperscript{16} Shane, Scott. (2011, December 7). “To State Dept...”

hactivism and social media use, and WikiLeaks highlights a serious problem with the legal framework available to prosecute publishers of leaked classified information and stop online dissemination of the information once it is first published. For example, the grand jury in the U.S. remains in deliberations while the legal battle that Assange fights today has nothing to do with the Internet, but rather criminal charges for sexual misconduct. The lack of action against Assange underscores the potential for serious issues in the event of further leakages, especially those published overseas such as WikiLeaks; there is a perceived lack of legal footing for prosecution in such cases.

Currently, WikiLeaks struggles to stay afloat due to lack of funding and the house arrest of its founder. On its front page, WikiLeaks displays a plea for donation, citing legal fees of $1,200,000 in addition to more than $2,000,000 in other operational costs. Despite the seeming inability to prosecute the publisher, however, the United States government has made strides to punish employee offenders and tighten security. No major leaks have since been reported, and the new reign of transparent government action and revolution in journalism revolution that Assange envisioned has not materialized.

**Hacking**

“Hacktivist” groups such as Anonymous comprise a second, related threat to classified information sharing. Anonymous is a group of hackers from around the

---

19 Keller, Bill.
world, loosely coordinated and connected via chat rooms and forums. They have pledged support of WikiLeaks, aiming at many of the same anti-secrecy and governmental transparency goals. The methods by which they help achieve these goals, however, is vastly different. In 2010, many payment-processing companies such as PayPal and Mastercard refused to accept donations for WikiLeaks. In an act of “hactivism,” Anonymous began attacking the websites of these companies, making access unavailable or very slow. In late 2011, Anonymous continued its support of WikiLeaks by hacking into a geopolitical analysis firm called Stratfor, which kept several files on WikiLeaks and founder Julian Assange, and forwarding e-mails on to Assange for release on WikiLeaks. Separate from WikiLeaks, Anonymous posted the names, e-mails and credit card information for Stratfor subscribers online. Although these actions may be easily prosecuted in court using federal and state computer trespass laws described further later on, it is difficult to locate the perpetrators. WikiLeaks may be slowly fading from the public eye, but groups like Anonymous keep it afloat and in the news when they commit serious acts such as the Stratfor hacking and use WikiLeaks at least in part for the release of information it obtains.

Social media use

22 Ibid.
Finally, social networking outlets such as Facebook and Twitter provide an excellent platform for the dissemination of information. Facebook, on which users can create a free online “profile” and make connections with “friends,” allows account holders to share their opinions through comments, photos, statuses, posts and notes. On Twitter, tweeters around the world can microblog—publishing up to 140 characters at a time. People all over the world use these websites to share their daily lives. Recently, Facebook and Twitter played major roles in many Arab Spring uprisings, such as that in Egypt and Tunisia in 2011. Many revolutionaries in both nations used these social media sites to spread information about planned protests during these early Arab Spring events, causing Twitter and Facebook to be labeled as new weapons in a revolution.

Although bringing people together for democracy is arguably a positive impact of social networking websites, the free flow of information via these sites poses serious policy questions for the American governmental agencies. For instance, Marines Sargent Gary Stein may face dismissal from the Marine Corps for posting his political opinions on a Facebook group. Stein, a declared Tea Party member, created a Facebook group called "Armed Forces Tea Party," which is now under fire as the Pentagon declared Stein in violation of a policy barring political

---

involvement by members of the armed forces. Although this situation will continue to play out in the media and in court, it sheds light on a complication that social networking outlets pose to sensitive information. Stein used Facebook to communicate opinions, but government employees can also use this medium to pass along other types of information to the public. In an age where self-expression is possible in a split second via a Facebook status update or Tweet, government employees on social media sites poses a new risk. For example, if Stein continued using the Internet and social media sites to express his feelings about the Tea Party and his reprimand, the U.S. Marine Corps may suffer from internal disagreements or need to engage in costly public relations. Further risks of social media sites could be accidental leaks via photos or content posted online that inadvertently reveal protected information, or intentional leaks from disgruntled employees. Although the government may punish offenders using current laws, once the information is online it is almost impossible to take back—even basic personal information is difficult and time consuming to get removed. Government agencies may combat this risk with policies preventing dissemination of information, but the possibility of inadvertent information sharing over Facebook or Twitter must also be explored. Additionally, complications with free speech rights or potential lawsuits may also


occur if government bodies attempt to prevent social networking, as discussed in detail later in this essay.

**What data is sensitive?**

To properly analyze the risk associated with each of these three types of online actors and activities, the nature of the information shared must be assessed. As per the Supreme Court, the President of the United States has the authority to classify, and thereby restrict dissemination of, information whose release may jeopardize national security. The Court lists this power as stemming directly from the investment of power in the President from Article II of the Constitution. There are three categories of classified information: Top Secret, Secret, and confidential. The classifications are broken down as follows: a reasonable person must expect Top Secret information to cause “exceptionally grave damage” to national security, Secret to cause “serious damage” and confidential to cause “damage.” To receive classified status, information must deal with:

- military plans, weapons systems or operations;
- foreign government information; intelligence activities, intelligence sources/methods, cryptology;
- foreign relations or foreign activities of the U.S., including confidential sources;
- scientific, technological, or economic matters relating to national security;

---

• federal programs for safeguarding nuclear materials or facilities;
• vulnerabilities or capabilities of national security systems; or
• weapons of mass destruction

The classifying officer must support his classification, and set the information for declassification no earlier than 10 years later. The Information Security Oversight Office (ISOO), located in the National Archives and Records Administration, creates procedures for each agency with classified information to use in protecting classified information. The ISOO offers policies for everything from handling or storing to destroying classified information. Employees that violate these policies can face consequences ranging from reprimand to termination of employment.

The Freedom of Information Act (FOIA) strives to find a balance between the public interest of government transparency as well as the necessity for the government to protect some information. FOIA, implemented in 1967, asserts that all citizens have the right to federal government information, and establishes a request system citizens may utilize to gain access to information. FOIA contains nine exceptions that let the government withhold information from disclosure, however. The first listed exception is any information relating to national security,
immediately removing all levels of classified information from the scope of FOIA.\textsuperscript{34} Other exceptions include internal personnel rules, trade secrets, and privileged intra- and interagency memoranda.\textsuperscript{35} These exemptions from public information sharing help explain why there was so much government alarm when WikiLeaks published state department cables and other classified information. The information was never intended for the public via the federal information classification system, nor would most of it have been disclosable under the Freedom of Information Act. FOIA also supports the decision to not release state department cables to the ACLU after they had already been published on WikiLeaks, as discussed previously. Despite WikiLeaks bringing these cables to the public, they are still protected under FOIA and it is within the government’s purview to deny access.

\textbf{Current parameters}

\textit{The legal framework}

FOIA introduces the legal framework that exists to protect information sharing by disallowing the sharing of classified information by government agencies. Each of the aforementioned information-sharing activities has a surrounding legal framework that currently dictates its participants’ legal limits (or lack thereof).


\textsuperscript{35} \textit{Ibid.} Other exceptions include information exemption by other statutes, personal information affecting a person’s individual privacy, law enforcement records, records of financial institutions, and geographical information concerning wells.
The most-clear cut of these frameworks is that for hacking groups. Groups like Anonymous could be easily prosecuted under law such as the federal Computer Fraud and Abuse Act, which disallows unauthorized access, or exceeding authorized access, to any computer used in interstate commerce, or individual state computer trespass laws, which make unauthorized access to computer systems or networks punishable—from a misdemeanor to felony in some states.\textsuperscript{36,37} The singular complication with bringing hackers to justice is catching them—because they hide under proxy names and fake IP addresses, it is extremely difficult for law enforcement forces to find and arrest members of groups such as Anonymous. Although police have made some major arrests of Anonymous hackers this year,\textsuperscript{38} they are due primarily to the hackers they caught slipping up in their anonymity routines. For example, Hector Xavier Monsegur (“Sabu”), the leader of a hacker group called LulzSec and active “hacktivist” in Anonymous, failed to shield his IP address one time when he logged into an online chat, leading investigators directly to his location.\textsuperscript{39}

Dismantling anti-secrecy groups such as WikiLeaks or preventing users from posting on social media such as Facebook is even more complex than hunting

\textsuperscript{36} The Computer Fraud and Abuse Act. 18 USC § 1030.
\textsuperscript{37} Online Security (2004, May). “Statutes by State—Computer Trespass.” Retrieved April 23, 2012, from http://www.iprotect.com/Community_Forum/statutes-states-ctr-2.php. Some states, such as Kansas, only punish computer trespassing with a misdemeanor charge. Other states, such as North Carolina, will charge up to a Class I Felony for such offenses.
\textsuperscript{38} Others arrested included John Anthony Borell III on two charges of intrusion for allegedly hacking two Utah police websites, and Higinio O. Ochoa (“Anonw0rmer”), a known Anonymous hacktivist.
hactivists hiding behind fake IP addresses. Although websites like Twitter and Facebook have Terms of Use, or stipulations that disallow certain types of posting, protection they give against dissemination of sensitive information is minimal. In most cases, the Facebooks and Twitters of the world implement Terms of Use agreements in order to protect themselves, should any user post something that could cause backlash against the service provider and the provider chooses to take the information down. These Terms of Use agreements may help protect the company, or even educate or dissuade users from posting troublesome content, but they are not failsafe. Although search engines such as Google will often respect governments’ requests for information removal, but with about a trillion websites worldwide, online information proliferation is rapid and containment is difficult.40

A patchwork of different policies exists, implemented with the goal of preventing dissemination of classified information. Certain federal statutes prohibit and punish the disclosure of information based on the “nature of the information, the identity of the discloser, the identity of to whom it was disclosed, and the means by which it was obtained.”41 The most encompassing piece of legislation is the Espionage Act of 1917. The Espionage Act disallows dissemination of information that poses a threat to national security.42 This act hinges on a “bad-faith intent requirement.” If a person, whether authorized or unauthorized, transmits

42 The Espionage Act of 1917. 18 USC § 793.
information intending or knowing that it may be used to endanger national security, he or she is determined to have “bad faith” and may be punished under this act.\textsuperscript{43} Any classified information that is disseminated without authorization automatically fulfills the bad-faith intent requirement, as classification in and of itself, as discussed previously, is considered reason enough to believe that the information could endanger national security. Those found guilty of violating the Espionage Act must pay a fine and may be sentenced to up to ten years in prison.\textsuperscript{44}

Private Bradley Manning, the man who allegedly passed information to WikiLeaks, faces charges under the Espionage Act, among other charges.\textsuperscript{45} Because the information he gave to WikiLeaks was classified information, under the Espionage Act, prosecutors argue, Manning fulfilled the “bad-faith intent” requirement by giving information that could reasonably be assumed to pose a threat to the United States’ national security. The verdict has not yet been given for Bradley Manning, but his case is an excellent example of how a piece of legislation created before the Internet was dreamed of can still apply today in modern settings.

A second major piece of legislation that frames the question of online classified information sharing is the National Security Act of 1947. The National Security Act’s main functions provide for the organization for the intelligence

\textsuperscript{43} Elsea, Jennifer K. Criminal Prohibitions...
\textsuperscript{44} The Espionage Act of 1917. 18 USC § 793 (a)-(c).
community within the US government. It also, however, established procedures in handling classified information. Part of this act makes punishable by fine and/or up to ten years of imprisonment the sharing of information to unauthorized parties containing the identity of covert agents acting on the behalf of the United States.

The E-Government Act of 2002 provides another important part of the framework. This act promotes the use of the Internet for the functions of the government, as well as government transparency and access to government information. Part of the E-Government Act is the Federal Information Security Management Act, or FISMA. FISMA exists “to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets.” In short, FISMA ensures that there is a system in place to protect government information online. It requires that each agency have a Chief Information Officer, who implements, keeps track of and reports on the success of information security programs for his or her agency, as well as assists with independent evaluations of these programs. FISMA also gives the National Institute of Standards and Technology (NIST) the duty of creating guidelines and standards for information security methods used by government

---

46 The National Security Act established both the National Security Council (NSC) and the Central Intelligence Agency (CIA).
51 The E-Government Act, 44 USC § 3543-45, 3505 (c) (2002).
agencies. In April 2012, Congress passed an update to FISMA. It increases monitoring requirements from periodical to continuous, helping detect vulnerabilities in the systems used by different agencies and giving reports in the systems' weaknesses. The update will travel next to the Senate for approval as part of the Cybersecurity Act. If passed, the bill will further underscore the government’s mission to reduce network vulnerability to information leakages.

The E-Government Act, and FISMA with it, is another attempt at balancing two government needs. The Act aims to increase productivity and effectiveness of the government by transferring actions to the Internet. FISMA counteracts the potential security risk of this effort by instituting controls and establishing standards of protection for information shared online by agencies. In this way the E-Government Act sets a desirable standard for future policies involving online information sharing; policies should strive to increase government effectiveness while setting safeguards for secure development.

A final consideration in this legal framework is international laws. In the case of WikiLeaks especially, much of the information was published from operatives in other countries, and the founder, Julian Assange, is an Australian national. If the grand jury decided that they would pursue charges against Assange under the Espionage Act or another applicable statute, the Assange would then need to be extradited from the country he was in (at this time, the United Kingdom), to

---

54 Ibid.
the United States to stand trial. Although the United States has extradition treaty agreements with over 100 different states, most modern extradition treaties contain "political offense" exceptions.\textsuperscript{55} Espionage is traditionally treated as a "purely political offense," an act that is directed at the government and does infringe on any individual rights.\textsuperscript{56} This characterization is a rather large stumbling block in hopes of extraditing foreign nationals to stand trial for breaches of the Espionage Act. To use a treaty to extradite the charged individual, the crime he or she is charged with must appear within the treaty.\textsuperscript{57} According to a recent report from the Congressional Research Service, "no U.S. extradition treaty currently in force lists espionage as an extraditable offense."\textsuperscript{58} For these reasons, international law is an obvious weakness in prosecuting leaks of information particular to one government, especially when the offender is not a U.S. citizen.

\textbf{Complications}

Several complications exist when limiting online speech in order to prevent classified information leakage. At the forefront of these complications is the First Amendment right to freedom of speech. When examining whether government efforts to prohibit or punish speech it considers dangerous is consistent with First Amendment rights, the government's role can be viewed two different ways. The first is government as the governing body of the United States, regulating the activities of the people it governs. Under the First Amendment, as interpreted by the Supreme Court, "[t]he Government may ... regulate the content of

\textsuperscript{55} Elsea, Jennifer K. "Criminal Prohibitions..."
\textsuperscript{56} Quinn v. Robinson, 783 F.2d776, 791 (9th Cir. 1986).
\textsuperscript{57} Elsea, Jennifer K. "Criminal Prohibitions..."
\textsuperscript{58} \textit{Ibid.}
constitutionally protected speech in order to promote a compelling interest if it chooses the least restrictive means to further the articulated interest.” 59 This same ruling deemed that a strict scrutiny is required to restrict speech based on its content; the government must produce evidence of compelling interest, such as national security, while using the least restriction possible to serve the government’s interest. Several Supreme Court cases have also established exceptions to free speech, including:

- speech “directed to inciting or producing imminent lawless action…and is likely to incite or produce such action” (incitement); 60
- obscenity; 61
- child pornography; 62
- speech that “tend[s] to incite an immediate breach of the peace” so long as it is a “personally abusive [word] which, when addressed to the ordinary citizen, is, as a matter of common knowledge, inherently likely to provoke violent reaction” (fighting words); 63
- copyrighted speech 64

---

60 Brandenburg v. Ohio, 395 U.S. 444 (1969). The Supreme Court upheld Ku Klux Klan member Clarence Brandenburg’s right to freely denounce non-Caucasians because his speech did not directly incite lawless action.
When private citizens voice their opinions on matters of public interest and do not invoke non-protected language (in the categories listed above) the government may not restrict their speech unless they meet strict scrutiny required by law.

The second role the government may play is as an employer. This role is relevant to discussion of First Amendment rights on social media websites by government employees, as well as leaks to websites such as WikiLeaks by employees. In the relationship of government as employer, the scrutiny required for speech restriction is less stringent. As an employer, the government must promote its effective execution of duties. As opposed to the strict scrutiny required for private citizens, the government may restrict employee speech when they are speaking as an employee in the fulfillment of his or her job or if they are speaking on a private concern (as opposed to a matter of public interest). The government may also restrict employee speech if the government’s interest in promoting efficient operations outweighs the employee’s individual interest in speaking out.

Further complications are not legal, but managerial. Preventing the free flow of information due to fear of dissemination can negatively affect productivity. If employees expect everything they say or write to appear in the realm of public knowledge, either via leak or full government transparency, they may be more hesitant to voice new, innovative ideas for fear of ridicule. Other danger can stem from internal discussions on policy that is still formulating. For example, if a leak were published detailing possible US policy on Iran, other countries may react before the US may fully formulate and present its policy decision to the international

---

65 First Amendment law and public employees.
66 Ibid.
community. Such a leak could breed international misunderstanding and tension. Finally, further internal communications may be protected to ensure that the US does not suffer from ridicule or bad publicity. The State Department cables discussed above, requested by the ACLU after WikiLeaks published the non-redacted version, are an example of this interest. Although the risk of Pakistan’s irritation with Britain over learning Americans thought the British were pessimistic about Pakistan does not seem like a major risk to national security, it may slow down the multilateral diplomacy process, which is essential to many international decisions.

To find solutions to the various risks posed by online information sharing, policymakers must weigh the risks to national security against these possible complications. As discussed previously, the classifying officer for sensitive information must justify the classification he or she is giving each piece of information. As noted above, the levels of harm supporting classification are exceptionally grave danger to national security (Top Secret), serious danger to national security (Secret), or danger to national security (Confidential). It is important to understand what exactly can pose these varying levels of danger to national security. Primarily the risk is direct harm from enemies, stemming from information detailing US strategies, confidential informants, internal policy and strategy discussions or government weaknesses. WikiLeaks, in its massive publication of some 100,000 State Department cables in Fall 2010, did not redact
the names of some informants, spurring criticism by the government for placing individuals in danger who were helping the United States.67

Over-classification of information must also be considered as part of the problem. Prior to this release, however, WikiLeaks worked with the New York Times and other media outlets to publish cables with information such as names redacted, and the government still criticized the release of dated information with no real risk associated, just on the basis that it was classified.68 The government’s secrecy policies have received much scrutiny and criticism in the years since WikiLeaks began publishing classified documents. Steven Aftergood, the American Federation of Scientists’ director for the Project on Government Secrecy, said that many employees in the State Department “use classified as a default setting.”69 Thomas S. Blanton, executive director at the National Security Archive, compares the current classified settings to a fence around a prairie, when we need “a tall fence around a graveyard.”70 As the United States government makes strides in better protecting its information, it must also differentiate how much information actually needs protection.

The solutions

Two types of solutions exist for the issues that arise from online information sharing. The first are reactive measures. When protected information is shared,

---

67 Shane, Scott. “WikiLeaks Leaves Names...”
68 Ibid.
70 Ibid.
existing laws apply to punish the leakers. The ability of the United States to prosecute the publisher of information, however, is weak due to the reasons discussed above, such as extradition. Although drafting new legislation may ameliorate this problem, the legal system can be a slow mechanism to deal with such a potentially expansive problem. Additionally, legislation would need to be very strictly tailored to uphold free speech rights. To retain public respect as well as provide damage control, several other types of reactive measures are necessary. These include public relations, such as press releases and other communications with the public. The government and any affected agency must be able to effectively communicate with the public about the details of the situation, especially what the government is doing about it. For example, if there were to be another large leak of classified government documents on WikiLeaks, the government would use public relations to communicate the government’s stance on the released documents and inform the public about why documents are classified and how it negatively affects national security when such documents are released. They would also communicate how close they are to catching the whistleblower or hacker associated with the leak, and what they will do to prevent further leakages. Additionally, the government must have the resources to combat further harmful information sharing. For example, setting up a legal team tasked with exploring options for cutting off finances for the site (such as what happened with WikiLeaks to cause their current financial dilemma), as well as communicating with search engines such as Google to
have the leaked content removed.71

When WikiLeaks burst onto the public scene, the government had little choice but to react as best it could. WikiLeaks had the element of surprise, forcing the government to scramble to communicate with the public, explore the legal options, and slow the functions of WikiLeaks all at once. Although the situation did not lead to a journalism revolution, the United States should dedicate resources to a plan should another leak occur. With WikiLeaks now fading into the background, the government may take this lull to establish a task force trained in providing all of these responses immediately and effectively if another similar leak occurs.

The best solutions, however, are proactive, preventing dissemination of sensitive information from occurring the first place. Although the current laws have flaws as noted above, using the legislative process to fix them may be slow, and new policies specific to certain technologies may become quickly outdated. To avoid over-legislating and increase government effectiveness while striving for better information security, two primary solutions exist. The first is strengthened network security. By tightening network security—making it less vulnerable to outside penetration as well as internal leaks—agencies can help prevent outsiders from getting in and insiders from leaking information out. Congress is working on this preventative measure already, as reflected in the update to FISMA recently passed in the House of Representatives, as discusses above. Second, government agencies can make clear-cut employee policies on how to use new Internet and

Web 2.0 options such as wikis, mash ups and blogs, that explain and highlight the dangers of sharing sensitive information. The US Department of the Navy (DON) does an excellent job with this in a 2008 memorandum. This memorandum explains “use of these [Web 2.0] tools supports Department of Defense and DON goals of achieving an interoperable, net-centric environment by improving the warfighter’s effectiveness through seamless access to critical information”. It further explains the these tools are “useful in a global enterprise...as they enable widely dispersed commands and personnel to more effectively collaborate and share information,” but warns that “their application must not compromise data confidentiality and integrity”. The Department of Navy in this memorandum clearly expresses both the promise and risk of using these new collaborative tools to its employees. To further their goal of safe Internet use, the Navy also has a collection of policies outlining proper Internet and social media use. For example, an all-Navy message in 2010 explained what constituted official use of social network sites and giving guidance as to how to successfully and appropriately use social media in an official capacity.\(^{72}\) The Navy also provides an online PowerPoint for officers to access to better understand the requirements for social media posting in official capacities and the safety measures in place to protect inappropriate use or information leakage.\(^{73}\)

---


Thorough training can make both tighter network security and comprehensive usage policies more effective. By dedicating time at hiring and again each year to explain the policies and clearly express employees’ rights to expression but expectations of professionalism online, correct use of the Internet and network in the work place, and the purpose of online tools, employees will better understand and use the tools around them. Training will also help avoid improper dissemination of information due to operator error. By using tools such as PowerPoint, as demonstrated by the Navy’s clarification presentation discussed above, agencies can maintain open communication and clear up confusion that new policies may bring. Constantly clarifying goals, as well as explaining how the technology used works, will help government agencies prevent unintended future leaks. Maintaining monitoring of the system, such as the continuous monitoring proposed by the FISMA update will help prevent hacking, as well as unauthorized security breaches by employees that could lead to intentional information leaks.

Although the Internet era is rife with risks to network security, it holds the potential for enormous improvements to government efficiency and communications. By applying appropriate existing legislation and drafting new internal policies set to react to and prevent future breaches in network security, the government can avoid some of the larger problems posed by groups such as WikiLeaks and Anonymous and the risks associated with social media.

Policymakers must keep in mind, however, that this is not a finite problem. As the Internet continues to grow and technological capabilities expand, policy and agency procedures must keep up to promote safe and effective government functions.
Bibliography


The Computer Fraud and Abuse Act. 18 USC § 1030.


The Espionage Act of 1917. 18 USC § 793.

Executive Order Number 13,526 § 1.4


Quinn v. Robinson, 783 F.2d776, 791 (9th Cir. 1986).


Shane, Scott. (2011, September 1). “Spread of Leaked Cable on Web Prompts