1-1-2016

A Response to the AIS Bright ICT Initiative

Glen Sagers
Illinois State University

Douglas P. Twitchell
Boise State University

A Response to the AIS Bright ICT Initiative

Full paper

Glen Sagers
Illinois State University
gsagers@ilstu.edu

Douglas P. Twitchell
Boise State University
twitched@gmail.com

Abstract

In 2015, the President of the Associate for Information Systems introduced the Bright ICT Initiative (Lee 2015), which provides a framework for improving Internet security based on four principles: origin responsibility, deliverer responsibility, rule-based digital search warrants, and traceable anonymity. We review these principles and show that at least three of these principles are at odds with the United Nation's Universal Declaration of Human Rights and the founding principles of the Internet and may actually decrease individual security. We conclude giving suggestions for developing principles more in line with human rights.

Keywords (Required)

Bright ICT, human rights, surveillance, privacy, warrants, anonymity

Introduction

In June 2015, the President of the Associate for Information Systems introduced the Bright ICT Initiative in a Guest Editorial in MISQ (Lee 2015). In his editorial, President Lee describes the current Internet as "a chaotic superhighway without appropriate traffic lights or police." He proposes the Bright ICT initiative as a fundamental change to the Internet to address its negative side effects.

In this paper we show that the initiative's principles are at odds with fundamental democratic values expressed in the United Nation's Universal Declaration of Human Rights (UDHR) ("The Universal Declaration of Human Rights" n.d.) and the founding principles of the Internet. We discuss how the initiative's principles may actually decrease individual security and stifle innovation. We conclude with suggestions for developing new principles.

The Bright ICT Principles

In the guest editorial, introduces the following four principles upon which the Bright ICT Initiative is based:

- **Origin Responsibility** puts the responsibility for ensuring data is not malicious on the origin rather than the destination which currently has *de facto* responsibility.
- **Deliverer Responsibility.** Deliverers of data, such as Internet service providers, should also share in the responsibility of ensuring data is not malicious.
- **Rule-Based Digital Search Warrants.** Data in transit should be surveilled and, according to rules established by governments, forwarded to authorities when those authorities are granted a search warrant.
- **Traceable Anonymity.** ICT technologies should provide anonymity generally, but according to rules and when granted warrants, authorities may discover identities.

The Bright ICT Initiative and Fundamental Human Rights

The United Nations and most democracies are founded on the idea that individuals have fundamental rights that are intrinsic. The UDHR describes these rights as "inalienable" and "fundamental." These rights are not granted by governments; they are independent of and precede governments and their laws. Any grand initiative to fundamentally change the Internet, currently used by one-third of humanity as a means of communication, should recognize and adhere to the rights described in the UDHR.

As we will show throughout this paper, underlying all of the principles of the Bright ICT Initiative is the assumption that governments are benevolent and their laws are just. The principles cite law, as defined by each country, as the arbiter of when to violate rights such as the right to privacy in the name of security. History, however, is replete with examples of corrupt, despotic, otherwise unjust governments, and even just governments who simply make mistakes. In fact, it is this history that led to the UDHR. As the UDHR itself says:

> *Whereas disregard and contempt for human rights have resulted in barbarous acts which have outraged the conscience of mankind, and the advent of a world in which human beings shall enjoy freedom of speech and belief and freedom from fear and want has been proclaimed as the highest aspiration of the common people*

Laws, as written by governments, can be an expression of the will of the people of the nation, but in other cases they are in place to serve the interests of the powerful and privileged. As was experienced throughout the Arab Spring movement of 2010 – 2012, the Internet and associated social media can provide a means for the oppressed to move against their oppressors (Howard et al. 2011). With the Bright ICT principles in place, however, movements such as the Arab Spring may not be possible.

Additionally, the Internet itself is built on principles that emphasize the decentralization of technology and empowerment of individuals. The Internet Society, a non-profit organization created by the Internet founders and supported by UNESCO, the Human Rights Council, and many others, has as part of its core values:

> *The social, political, and economic benefits of the Internet are substantially diminished by excessively restrictive governmental or private controls on computer hardware or software, telecommunications infrastructure, or Internet content. (The Internet Society n.d.)*

The Bright ICT principles, as currently constituted, would require restrictive governmental controls on the telecommunications infrastructure and Internet content that would create human rights violations around the globe. In the remainder of this paper we will discuss each of the Bright ICT principles individually and show how they imply mechanisms that are contrary to the human rights principles established above.

The Principles of the Bright ICT Initiative

Origin Responsibility

The principle of origin responsibility as described in President Lee's editorial (Lee 2015) is that the originator of data is responsible for the content of that data. Currently, according to the editorial, the destination of data is *de facto* responsible for determining whether incoming data is malicious. This is true, but the alternative of data origin responsibility may not be better. President Lee's editorial focuses on reducing spam email as an example of the possible benefits of origin responsibility.

While the idea of origin responsibility seems great on the surface, no real innovation is suggested. Monitoring outgoing email to see if it contains spam, based on user feedback from destination servers is has very few differences what what Spamhaus and others are doing, except it's moving responsibility to the server side.

The concept of origin at four levels (user, server, company and country) as describe in the editorial is problematic from several perspectives. While the levels themselves make sense (many spam blacklists

block IPs, organizations, or even whole countries), the mechanics of a government enforcing companies to behave ethically seems overly optimistic. A look at the financial scandals that resulted in the passage of the Sarbanes-Oxley act in the US, or the various international scandals involving vehicle brakes, ignition systems, airbags and emissions shows that companies cover up when it is in their own self-interest and that government punishments after the fact don't stop future issues from occurring.

Raising this enforcement to international levels merely highlights the fact that the UN has been mostly unable to enforce its own directives since its inception. One critical failure of the UN, that is extremely relevant here, is its inability to act back against nations that have violated the UDHR. The passage of further treaties to collect taxes and penalties to enforce origin responsibility will be difficult. As an illustrative example of an issue that many agree is pressing, take carbon emissions and global warming. Despite widespread calls for action, the countries of the world have not been able come to many binding agreements, until perhaps the Paris climate summit in late 2015 (Davenport 2015). When an initiative such as Bright ICT is proposed, which may have public benefits but has many private costs, it seems unlikely that citizens of many countries will embrace it.

Further, the reference model used by President Lee for origin responsibility is based upon the European Union's Directive on Waste Electrical & Electronic Equipment (WEEE). It's not clear why this directive is used as a basis for the model, as it seems to have very limited, if any applicability. In the WEEE directive at least two phases take place. First, the producer of an electrical or electronic good is required to reduce harmful waste during design and production phases of their equipment. This is specified as "cooperation between producers and recyclers… facilitating the re-use, dismantling, and recovery of WEEE, its components and materials" (Directive 2012/19/EU, Article 4). This particular portion of the WEEE Directive has no applicability to Bright ICT because there is no harmful waste to eliminate in the generation of emails or other Internet traffic.

Article 5 of the WEEE provides for the other phase cited by President Lee in his model. Specifically, the "Separate Collection" principle provides that systems shall be set up to allow final holders and distributors of electronic goods to return waste goods at least free of charge. This recycling channel simply provides for the return of equipment, it does not specify financial penalties or rewards for compliance. It is also unclear how this phase of the WEEE directive applies to origin responsibility because there is no product that could be returned after an email transaction.

How could an individual producer, or the origin server, of spam be induced to reduce the volume of spam produced? Spam is already against the law in the US (the CAN-SPAM Act & others), the EU (EU Privacy and Electronic Communications Directive), and many other countries. Simply making more laws, even with possibly harsher penalties, will not, in itself, reduce the volume of spam. Similarly, unlike physical goods such as waste electronics, there's no recycling or scrap value for spam, meaning no entities would be interested in collecting it to stop it. While the WEEE directive is simply used to build a model of origin responsibility, the fact that only this largely irrelevant directive (at least to Bright ICT directly) is the only example supporting this principle is troubling.

Beyond the issues with using waste reduction as a model basis, the concept of responsibility of origin at the country level may result in skewing of the responsibility in two ways. Current Spamhaus rankings of the ten worst spam countries are as follows ("The Spamhaus Project - The Top 10 Worst Countries" n.d.):

1. US
2. China
3. Russian Federation
4. Japan
5. Ukraine
6. United Kingdom
7. Brazil
8. India
9. Germany
10. Hong Kong

Spamhaus claims that these countries have weak or non-existent spam laws, but that doesn't explain the whole list. Another factor that influences which countries appear on this list is simply the level of IT in

that country. The list above contains some countries that have large IT infrastructures, as well as countries that historically have ties to spam and organized and cybercrime (Krebs 2014), and some which aren't particularly tied to either weak laws or high cybercrime rates. This skewing toward countries with a high number of Internet-connected computers would persist in the face of Bright ICT laws, as there are simply more computers in those countries to exploit.

Today, most spam originates from botnets, not individual servers (Zorabedian 2014). Such botnets are already illegal, and many ISPs, and some countries, shut them down as soon as possible (Krebs 2014). However, given the relative ease of coopting machines of random Internet subscribers, only modest inroads have been made in truly reducing the number of botnets. A governmental agency shutting down and cleaning infected machines does not remove the cost of spam filtering; it simply moves the costs of spam prevention. Currently, for-profit companies filter spam. Government intervention would shift the cost to a non-responsible, non-related entity, adding to tax burdens. Uniform global laws may make it easier to shut down botnets, but won't completely stop spam.

In short, origin responsibility has some potential to reduce spam, but at an extremely high cost, which will not be borne by the actual criminals responsible for spam. It seems unlikely that spam producers can be induced to reduce the volume created, leaving individuals, ISPs, and governments to pay the costs. This exactly matches the current situation, and further policies and laws have almost no chance of changing that.

Unlike the remaining principles, origin responsibility is not a human rights issue. Rather, it is mostly a technical issue of implementation. If the ICT community can overcome the implementation issues, especially ensuring the responsible party bears the cost, then we feel this principle has the most merit.

Deliverer Responsibility

The deliverer responsibility principle places responsibility for malicious content on the deliverer rather than the destination, the current *de facto* responsible party. Implementation of deliverer responsibility would require deliverers to have full knowledge of the contents of messages delivered over their networks, a technique called *deep packet inspection*. Many deliverers are already engaged in deep packet inspection, such as companies inspecting all traffic to find and prevent loss of sensitive data, Internet service providers inspecting traffic to block peer-to-peer traffic and inject advertisements into web pages, and countries erecting firewalls to censor their citizens access (Davidson 2016; Ohlhorst 2014; Whoriskey 2008). Deep packet inspection is defeated using widely deployed end-to-end encryption protocols such as TLS.

An example of the lengths governments may take to enforce deliverer responsibility came recently from Kazakhstan. The Kazakhstani telecommunications provider posted a notice in late 2015 that all devices connected to the Internet must install a root certificate authority giving the Kazakhstani government the ability to set up "man-in-the-middle" attacks to decrypt, read, and re-encrypt TLS protected communications (Waddell 2015). If the government goes through with its posted intentions, Internet users in Kazakhstan will no longer have the authentication and confidentiality guarantees provided by TLS. Implementation of deliverer responsibility would require similar compromises in authentication and confidentiality.

Deliverer responsibility is presented from two standpoints, first, that deliverers can monitor message content in order to filter fraudulent content, and second, that deliverers may not be guilty of willful negligence. To enforce message filtering, Bright ICT suggests digital search warrants, which we cover below.

To enforce security of message deliverer's systems, Bright ICT suggests that penalties be applied to those systems which forward harmful messages. It is unclear from President Lee's editorial whether the Bright ICT proposal would penalize only willfully negligent deliverers or whether "Ignorance or negligence cannot be a justification to exempt one from responsibility", meaning that any deliverer would be penalized (Lee, 2015, p. vii), but the wording of the editorial suggests the latter.

President Lee's editorial suggests "deliverers should have checked their own systems to detect whether they were infected with malware prior to sending spam messages", and "deliverers have a legal responsibility to prevent harmful attacks and they cannot be willfully negligent", (Lee, 2015, p. vii). While

it is unknown, and probably unknowable, how many owners of computers that become part of a botnet were "willfully negligent", it is likely a very small number. Realistically, what owner of a personal or corporate computer would knowingly allow it to be used for illicit purposes for another's gain? Since this number is small, penalizing those who knowingly participate will not meaningfully reduce the load of spam or other malicious messages. Non-consenting participants in botnets could be penalized, financially or otherwise. Such penalties might decrease the number of active botnets, but at a high cost in government intrusion into daily lives.

The social consensus needed to adopt a policy for implementation of a truly adequate policy for deliverer responsibility is enormous. To be able to achieve consensus across all societies that every communication may be monitored is unlikely, especially given the reaction over the last few years to NSA/GCHQ monitoring. Government intrusion into each computer in a country to ensure they're not infected could help prevent unintended participation in botnets, but such a level of intrusion would be unpopular at best.

Finally, there's the cost of monitoring. The Bluffdale, Utah, USA facility recently completed by the NSA to store and monitor many types of communication cost $1.5 billion on record, and likely cost more in undocumented budgets (Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics 2014). Adding to that cost, a system which could truly monitor all communications in real time would require a distributed monitoring system. This system would need to communicate as fast or faster than the packets it filters and forwards to be able to correlate attacks. This would necessitate a new, faster administrative backbone, and the cost could easily reach into the hundreds of billions range. No matter where this money comes from, and how noble the goal, there is an opportunity cost associated with it. What other projects to benefit humankind must be postponed or remain undone in order to fund the Bright Internet Global Governance (BIGG) center?

As shown above, implementing deliverer responsibility be difficult and costly, but more importantly using today's technology it couldn't be done without damaging privacy. However, if techniques such as homomorphic encryption, which may allow for querying and aggregating encrypted data without exposing content (Gentry 2010), become practical, then it may be possible deliverer responsibility could be enforced without exposing lawful data. Until then deliverer responsibility with full privacy remains elusive.

Rule-Based Digital Search Warrants

An example of the kinds of mechanisms needed to realize rule-based digital search warrants is the movement in law enforcement in several countries to force Internet messaging services to have mechanisms allowing law enforcement access with a warrant. Proponents of this movement claim that governments should have the ability to defeat privacy mechanisms such as encryption to execute valid search warrants.

The ability for governments to successfully execute valid search warrants seems unobjectionable, but this actually represents the most troublesome aspect of the Bright ICT initiative. In the first place, if, as President Lee suggests, the deliverer may not be legally allowed to execute surveillance, the initiative is doomed to failure. Laws would first need to be rewritten to allow all deliverers, or at least those who form the backbone of the Internet, to perform the surveillance.

The second main issue with digital search warrants as presented is that they are supposed to "monitor by content and/or user name", (Lee, 2015, p. 3) and simultaneously may only monitor content if the message "violates the rules set by authorities in advance" (ibid). These two directives represent a tautology. If agents are to monitor on content, they must have access to content, therefore, they are monitoring the content. If, on the other hand, they only monitor on username, users who have never committed a crime, or who are not under suspicion would never trip an alarm. Much like the any reactive security measure, such a scheme can only protect against what's already been done, it can't predict new types of attacks. There is no possibility that the claim that the scheme of Principle 3 which states that "the privacy of innocent netizens will not be infringed on by government" can be implemented (ibid). A system with sufficient power to read content must use that power to scan the content in order to carry out its prime directive.

By scanning all packets, regardless of legality of the messages contained, all traffic may be surveilled. This includes packets that have legal but unpleasant speech, such as protest speech. Scanning the content of

such packets, even when no action is taken, interferes with the UDHR's basic human right of freedom of speech, because simply knowing a potentially hostile party is monitoring will reduce free speech (Schauer 1978). The effect has been called a "chilling effect" by the US Supreme Court, and is a primary human rights concern for existing monitoring systems (Cohn 2014).

Such a monitoring system would directly contravene the UN Human Rights Council's First Resolution on Internet Free Speech. Adopted in July, 2012, the resolution states that "the same rights people have offline must also be protected online, in particular, freedom of expression" (Zeldin 2013). Any monitoring systems that can curtail an individual's right to speak freely is a violation of human rights. We would not tolerate microphones listening to our every word, why should we allow every electronic word to be monitored?

A system which can implement rule-based search warrants will infringe on the privacy of innocent individuals. This privacy breach will be committed by the citizens' own government, working in conjunction with other governments throughout the world. From there, it is only a matter of time until an employee of the BIGG center blows the whistle on overzealous monitoring, much like Edward Snowden did for the NSA and GCHQ spying a few years ago (Cole and Brunker 2014). The very fact that the Snowden documents exist, and that the NSA and other agencies have admitted to spying on members of the US congress, along with millions of other citizens, is adequate evidence such breaches happen, and will happen again. If the content of every one of millions of corporate or individual messages were leaked, the results would be even more catastrophic than the confirmation that such spying was done. Besides insider revelations, any system which can scan content will be a highly-prized target for hackers, who could subvert it to read messages from thousands or millions of individuals and corporations.

If all countries can agree on a software agent, and have it independently certified, that would be a great step in the right direction. If, as the President Lee's editorial claims, it's unavoidable that different countries have different rules (ibid), how is Bright ICT of benefit to the world? As a simple example, if the US decides to match packets based on their origination from a known botnet composed of machines which are owned in whole or in part by China, but the Chinese government decides that this botnet is aiding their national interests, they will apply no such rule. In short, national policy and security interests would have to be subservient to the BIGG center. In order for Bright ICT to work, all nations must band together to prevent proliferation of weaponized malware and botnets.

A further complication is that automated search warrants are unconstitutional under US law. Article IV of the US bill of rights guarantees that no search may occur unless there is probable cause. While the NSA's PRISM and other programs have, and probably continue to, gather data without warrants, further steps down this road are inadvisable (Risen and Lichtblau 2005; "Timeline of NSA Domestic Spying" 2012). The tide of public opinion against secret monitoring programs has shown that at least US citizens are against government collection of telephone and Internet data, and don't believe that such monitoring serves the public interest (Gao 2015). How, then, can a program like Bright ICT ever get off the ground, since by its very nature, it will be clear that it is monitoring *everything*?

One final complication to rule-based digital warrants is cryptography. In the US, as this article is going to press, the FBI has taken Apple to court to create backdoors to their encryption used on the iPhone. This is not the first salvo in the crypto wars, governments in many countries have asked for ways to circumvent encryption to aid in capturing suspected or known criminals since at least the second World War, when the US predecessor to the NSA and the British GCHQ collaborated with the manufacturer of the Enigma machine to know it (Guy-Ryan 2016). More recently, Facebook subsidiary WhatsApp, a messaging service that implements end-to-end encryption between users, has been in legal trouble in Brazil after authorities ordered it to turn over records in a drug case. WhatsApp is technologically unable to do so, given that end-to-end encryption is in use; further, US law does not permit American companies to provide court-ordered wiretaps to anyone except the US government. None of this has stopped the Brazilian government from detaining and arresting a senior Facebook in Sao Paulo in early spring of 2016 (Phillips and Nakashima 2016). Again, this represents a case where uniform laws could help, but laws that allow government surveillance of all traffic have negative repercussions on personal privacy.

Encrypted messages could not be scanned for content, unless SSL man-in-the-middle attacks (SSL proxies) were implemented, as mentioned above for Kazakhstan. If implemented, all encrypted messages could be scanned for content. This would, of necessity, include bank transactions, online shopping

sessions, and anything else done on secure servers. Who among us would trust that such transactions would remain private, given their value to a hacker?

Traceable Anonymity

"Anonymity is allowed in order to guarantee freedom of expression", writes President Lee (Lee, 2015, p. viii). However, if that "anonymity" is traceable, it is not anonymity. From a human rights standpoint, then, traceable anonymity is a problem. The biggest problem with traceable anonymity would be the ability of totalitarian regimes to crack down on those don't agree with them. Simply write a rule in a filtering system (remember, we've already determined that countries can apply different rules for national policy reasons) that defines bad content as anything against the government, and then shut down not only that message, but imprison or execute the offender. Those who think this won't happen are shortsighted. Indeed, history is replete with examples of messages used to incriminate those who speak out against their government. Recently, for example, a member of Turkish Parliament was prosecuted for simply insulting Turkish president Erdoğan in a series of tweets (France-Presse 2016). Traceable anonymity would be an aid to governments that behave in this manner.

Many who want anonymity today use Tor, as well as other anonymizing technologies such as proxy servers and VPNs. One of Tor's stated goals is to act as an "effective censorship circumvention tool, allowing its users to reach otherwise blocked destinations or content" ("Tor Project" n.d.). Tor has been used by civil and human rights activists, journalists, and law enforcement, as well as military, whistleblowers, and normal citizens who value their privacy. Blocking or outlawing Tor and similar anonymity-protecting technologies, a necessary step for implementing traceable anonymity, will limit human rights activist's ability to be truly anonymous and will reduce human rights efforts around the world.

A final unanswered question about Bright ICT is tangentially raised by Tor's origins. Tor started as a US Navy project. Would Bright ICT apply to government systems? If not, why wouldn't attackers target the government systems more heavily, either to gain access to unmonitored systems or to use those systems for new botnets? This question is unanswered at this point, which isn't surprising given the age of the Bright ICT initiative. However, going forward, this is a very critical question. Are all systems on the planet subject to Bright ICT principles? If not, who determines which are exempt?

Conclusion

We have shown that at least the second, third, and fourth principles underlying the Bright ICT initiative as described in President Lee's editorial (Lee 2015) require enforcement mechanisms that are at odds with fundamental human rights. Any system that implements these principles will likely lead to actions that violate human rights. Why? Because the principles naively assume that governments are benevolent and accountable to those they govern. We believe the examples given above and the UDHR show this is not the case.

Any initiative for protecting Internet users must not only protect them from criminals but also protect them from oppressive governments. We call on those involved in the Bright ICT initiative to reconsider and revise the principles upon which it is based. New principles should include protections from all malicious actors including both criminals and governments. While the Internet is not "safe" at this point in history, it has improved since its inception. Strides toward a more robust, safer Internet are a great idea, but not at the cost of fundamental human rights. We all have a right to privacy, and to personal security. Facilitating the decryption of messages and inspection of content will invade privacy, and the BIGG center itself will become a hacker target, since messages can be read there in plaintext, including usernames and passwords, reducing personal security.

The Internet has grown into the major force for social change. It is likely that with more governance, the Internet would have fewer security issues. However, it would not have been able to penetrate to every corner of the world with heavy-handed regulation. The human rights violations that the Internet has exposed make up for, at least in part, the issues it has caused. In short, while we applaud efforts to make the Internet safer, Bright ICT does not represent the way forward, at least as currently stated. We call on scholars everywhere to carefully consider both intended and unintentional consequences of any protocols,

technologies, and policies adopted to make the Internet safer, especially if they may have bearing on individual human rights, privacy, and security.

REFERENCES

Cohn, C. 2014. "NSA Surveillance Chilling Effects: HRW and ACLU Gather More Evidence," *EFF Deeplinks Blog*, July 28 (available at https://www.eff.org/deeplinks/2014/07/nsa-surveillance-chilling-effects; retrieved April 25, 2016).

Cole, M., and Brunker, M. 2014. "Edward Snowden: A Timeline," *NBC News*, May 26 (available at http://www.nbcnews.com/feature/edward-snowden-interview/edward-snowden-timeline-n114871; retrieved April 26, 2016).

Davenport, C. 2015. "Nations Approve Landmark Climate Accord in Paris," *The New York Times* (available at http://www.nytimes.com/2015/12/13/world/europe/climate-change-accord-paris.html).

Davidson, L. D. O. 4/15/16 at 3:32. 2016. "President Xi should tear down the Great Firewall that censors foreign websites," *Newsweek* (available at http://www.newsweek.com/president-xi-tear-down-great-firewall-447909).

France-Presse, A. 2016. "Former Turkish football star charged with insulting President Erdoğan," *The Guardian* (available at http://www.theguardian.com/world/2016/feb/24/turkish-football-charged-insulting-president-erdogan-hakan-sukur).

Gao, G. 2015. "What Americans think about NSA surveillance, national security and privacy," *Pew Research Center*, May 29 (available at http://www.pewresearch.org/fact-tank/2015/05/29/what-americans-think-about-nsa-surveillance-national-security-and-privacy/; retrieved March 1, 2016).

Gentry, C. 2010. "Computing arbitrary functions of encrypted data," *Communications of the ACM* (53:3), p. 97 (doi: 10.1145/1666420.1666444).

Guy-Ryan, J. 2016. "A Brief History of the U.S. Trying to Add Backdoors Into Encrypted Data," *Atlas Obscura*, February 21 (available at http://www.atlasobscura.com/articles/a-brief-history-of-the-nsa-attempting-to-insert-backdoors-into-encrypted-data; retrieved March 1, 2016).

Howard, P. N., Duffy, A., Freelon, D., Hussain, M. M., Mari, W., and Maziad, M. 2011. "Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?," SSRN Scholarly Paper No. ID 2595096, , Rochester, NY: Social Science Research Network (available at http://papers.ssrn.com/abstract=2595096).

Krebs, B. 2014. *Spam Nation: The Inside Story of Organized Cybercrime-from Global Epidemic to Your Front Door*, Sourcebooks, Inc.

Lee, J. K. 2015. "Guest editorial: research framework for AIS grand vision of the bright ICT initiative," *MIS Quarterly* (39:2), pp. iii–xii.

Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics. 2014. "MilCon Status Report - August 2014 - Undersecretary of Defense for AT&L," (available at http://www.acq.osd.mil/eie/Downloads/FIM/MilCon/MILCON_EOM-AUG_Report_2014-09-17.xlsx).

Ohlhorst, F. 2014. "Why Deep Packet Inspection still matters," *TechRepublic* (available at http://www.techrepublic.com/article/why-deep-packet-inspection-still-matters/).

Phillips, D., and Nakashima, E. 2016. "Senior Facebook executive arrested in Brazil after police are denied access to data," *The Washington Post* (available at https://www.washingtonpost.com/world/national-security/senior-facebook-executive-arrested-in-brazil-after-police-denied-access-to-data/2016/03/01/f66d114c-dfe5-11e5-9c36-e1902f6b6571_story.html).

Risen, J., and Lichtblau, E. 2005. "Bush Lets U.S. Spy on Callers Without Courts," *The New York Times* (available at http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html).

Schauer, F. 1978. "Fear, Risk and the First Amendment: Unraveling the Chilling Effect," *Boston University Law Review* (58), p. 685.

The Internet Society. (n.d.). "Values and Principles," (available at http://www.internetsociety.org/who-we-are/mission/values-and-principles; retrieved February 26, 2016).

"The Spamhaus Project - The Top 10 Worst Countries.," (n.d.). (available at https://www.spamhaus.org/statistics/countries/; retrieved March 1, 2016).

"The Universal Declaration of Human Rights.," (n.d.). (available at http://www.un.org/en/universal-declaration-human-rights/; retrieved February 29, 2016).

"Timeline of NSA Domestic Spying.," 2012. *EFF Deeplinks Blog*, November 30 (available at https://www.eff.org/nsa-spying/timeline; retrieved April 25, 2016).

"Tor Project: Overview.," (n.d.). (available at https://www.torproject.org/about/overview; retrieved March 2, 2016).

Waddell, K. 2015. "Kazakhstan's New Encryption Law Could Be a Preview of U.S. Policy," *The Atlantic* (available at http://www.theatlantic.com/technology/archive/2015/12/kazakhstans-new-encryption-law-could-be-a-preview-of-us-policy/419250/).

Whoriskey, P. 2008. "Every Click You Make," *The Washington Post* (available at http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html).

Zeldin, W. 2013. "U.N. Human Rights Council: First Resolution on Internet Free Speech," *Library of Congress - Global Legal Monitor*, July 12 (available at https://www.loc.gov/law/foreign-news/article/u-n-human-rights-council-first-resolution-on-internet-free-speech/; retrieved April 25, 2016).

Zorabedian, J. 2014. "Spam-Bot Invaders: Which countries send the most spam?," *Sophos Blog*, July 29 (available at https://blogs.sophos.com/2014/07/29/spam-bot-invaders-which-countries-send-the-most-spam-infographic/; retrieved March 2, 2016).