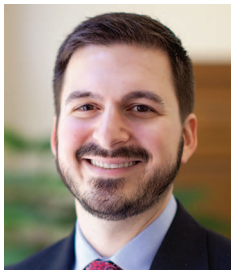

GREGORY CONTI | LISA SHAY | WOODROW HARTZOG

Deconstructing the Relationship Between Privacy and Security

From a government or law-enforcement perspective, one common model of privacy and security postulates that security and privacy are opposite ends of a single continuum. While this model has appealing properties, it is overly simplistic. The relationship between privacy and security is not a binary operation in which one can be traded for the other until a balance is found. One fallacy common in privacy and security discourse is that trade-offs are effective or even necessary. Consider the remarks of New York Police Department Commissioner Ray Kelly shortly after the Boston Marathon bombing, "I'm a major proponent of cameras. I think the privacy issue has really been taken off the table" [1].

Poorly-designed security measures can consume significant resources without achieving either security or privacy; others can increase security at the expense of privacy. However, with careful consideration, there are solutions that benefit privacy *and* security.

Organizational consideration of privacy and security is skewed by organizational missions, leadership opinions, current events, and media coverage, among numerous other factors. As a result, institutions are tempted to view either security or privacy as having an overwhelming importance. Businesses apply economic analyses to determine the appropriate balance for their organization. Law enforcement and government officials often heavily weight security. Citizens' opinions will vary, but are influenced by media coverage, such as the public outcry surrounding the revelations of Edward Snowden.

Those charged with defending national infrastructure are aware of the importance of privacy and civil liberties. For example, recent policy from the U.S. Department of Defense seeks to mitigate cyber security risks, while at the same time "protect and respect the principles of privacy and civil liberties, free expression, and innovation that have made cyberspace an integral part of U.S. prosperity and security" [2]. Unfortunately, it is easy to compromise privacy and civil liberties when seeking to improve security. Yet, the difficulty in achieving a balance should not prevent officials from striving for this harmony. We present a model to guide stakeholders in finding solutions that improve both security and privacy.

Four Quadrants

One reason privacy and security cannot be considered direct tradeoffs is that implementation is not always effective. Thus, we conceptualize the effectiveness of security solutions and their impact on privacy and civil liberties on continuous spectra ranging from harmful to beneficial using perpendicular axes as shown in Fig. 1. The resultant figure contains four quadrants, each representing a major class of security solution. We describe each class in the following

Digital Object Identifier 10.1109/MTS.2014.2319897
Date of publication: 4 June 2014

sections from the perspective of a private citizen, not that of government or law enforcement. By using this quadrant framing instead of a simple binary operation, stakeholders can pursue Quadrant IV solutions that achieve both security and privacy objectives.

Quadrant One: Security Theater (Accomplishes Neither Security nor Privacy Objectives)

The worst implementations degrade privacy without enhancing security. Bruce Schneier uses the term security theater, where deliberately visible security measures have only a minimal effect on actual security [3]. However, we consider Quadrant One to include any security measures that degrade privacy, while offering no real gain in security, whether visible or not. Consider easily-bypassed security measures, such as guards who wave pizza deliverymen through checkpoints and password recovery systems based on easily guessable personal information. Quadrant One solutions occur when well-intentioned, but ill-informed managers implement solutions that appear to be plausible.

Remediation of these systems is often problematic. Bureaucracies can be slow to respond to criticism and often citizens are not empowered to confront bad policies. For example, the U.S. Transportation Security Agency (TSA), has been under intense pressure to justify the logic behind its actions [4], [5]. Those affected must understand the necessity for and true benefit of security measures.

Quadrant Two: Show Me Your Papers (Accomplishes Security Objectives While Degrading Privacy)

Quadrant Two represents implementations that improve security while degrading privacy; for example, initiatives to create Internet driver's licenses. These credentials would require verification of a user's identity in the physical world before performing certain activities online. Other examples include the long-term retention of Internet users' online activities by ISPs and searches of electronic devices at national borders. While meeting security objectives, we should strive to do better than Quadrant Two solutions.

Quadrant Three: I Know My Rights (Accomplishes Privacy Objectives While Reducing Security)

Security solutions are unlikely to fall into Quadrant Three by design, as those who develop security systems do not seek to make security worse while improving privacy. Nonetheless, technical or policy countermeasures, such as those discussed at the 2013 IEEE International Symposium on Technology and Society [6] sometimes shift security solutions toward or into Quadrant Three. For example, consider the U.S. v. Jones decision by the U.S. Supreme

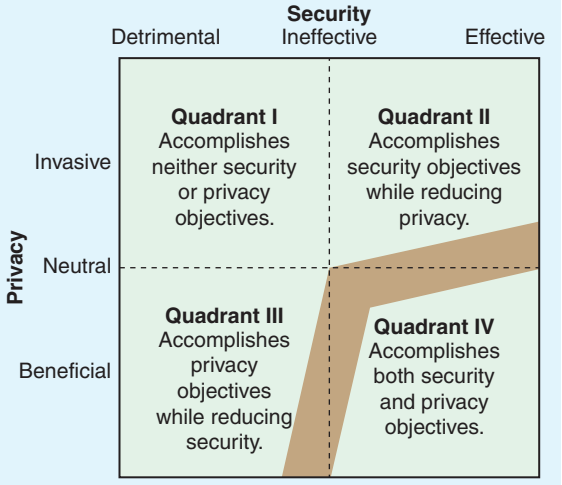

Fig. 1. The effectiveness of a security measure is plotted against its impact on privacy. Optimal solutions improve both security and privacy (Quadrant IV). The gray region indicates zones of potentially reasonable tradeoffs.

Court which found that the government's use of a GPS tracking device to follow a vehicle's movements constituted a search under the Fourth Amendment. This decision constrains law enforcement's future use of such tracking techniques. Quadrant Three solutions improve privacy, but have negative security impacts.

Quadrant Four: Win-Win Privacy and Security (Accomplishes both Security and Privacy Objectives)

Optimal solutions improve both security and privacy. These win-win solutions will be elusive, but we argue that they must be aggressively pursued. Consider Secure Sockets Layer (SSL), which makes most consumer financial activities possible on the Internet by reducing exposure of sensitive data in transit. Solutions in Quadrant Four may require some compromises, for example an employer who places an SSL proxy between employee machines and the Internet for intrusion detection purposes, but the end result improves security and privacy. Other potential Quadrant Four solutions, such as full disk encryption, offer privacy and security gains in some contexts, but must be carefully analyzed along other vectors not indicated in Fig. 1, such as cost, speed, and usability to ensure their long-term viability.

The design of Quadrant Four solutions begins with proper communication, planning, and education. We can learn much by studying insights from the privacy by design community [7]. Organizations should facilitate dialog among security solution developers, end users, and experts in privacy and civil liberties as early in the design process as possible. It is important to educate government and corporate officials on the importance of privacy and civil liberties and to transparently inform key privacy advocates of underlying

national security challenges in order to facilitate a cooperative mindset and mutual respect.

There are numerous areas of common ground that we believe most security and privacy advocates will support, such as government-funded and transparent code audits of heavily relied upon security technologies such as SSL and SSH, assistance in funding the deployment of DNSsec, and the continued development of high-quality guides to securing systems [8]. Governments could also support the continued development of robust open-source security tools and operating systems and encourage broader use of SSL for routine web activities [9]. Governments also possess unique and valuable security situational awareness data. For example, appropriate sharing of previously undisclosed malware signatures with ISPs and the sharing of generalized security breach data and trends along with timely and meaningful alerts could prove very beneficial.

The government could serve an important role in facilitating reports of security vulnerabilities to private-sector companies. Many researchers are fearful of the repercussions of reporting vulnerabilities directly to the company affected. Those companies are often hostile to the news that their products and services have security problems and respond by ignoring the report or threatening the researcher with litigation. Furthermore, companies have little incentive to fix these problems. They face not only the expense of addressing the issue, but also a possible public relations firestorm and even litigation if the flaw becomes publicly known. With all these possible downsides, vendors often choose to do nothing, leaving users at risk. A government role in this process could encourage companies to fix security flaws that might otherwise go unpatched.

Win-Win Mindset

Many security solutions come at the cost of privacy. Some, like security theater, improve neither security nor privacy and are merely a waste of time and money. Other solutions degrade privacy and civil liberties with only marginal gains in security, risking significant negative effects on societal norms, freedom of speech, rights of assembly, and innovation. Through education and rational analysis we can accomplish both security and privacy. It is important to develop a win-win mindset in all participants as they develop solutions. Seeking common ground among all major parties often serves as a solid starting point. We must also consider implications beyond security and privacy, including safety, cost, time, efficacy, and inconvenience to understand the true net value of a security measure.

Win-win solutions will be more palatable to government decision makers with minimal risk of pushback from privacy advocates, the media, and citizens. Despite these advantages, we must tread carefully. Perfect security and perfect privacy are dubious and likely unattainable goals. Thus, we should be mindful of diminishing returns in order to efficiently pursue privacy and security without a mandate for perfection.

Acknowledgment

We would like to thank participants of the Senior Conference held at West Point in June 2012 who provided useful potential solutions that increase both privacy and security. The views in this article are the authors' and do not reflect the official policy or position of the U.S. Military Academy, Department of the Army, Department of Defense, or the U.S. Government.

Author Information

Gregory Conti is an associate professor in the U.S. Military Academy's Department of Electrical Engineering and Computer Science and is Director of West Point's Cyber Research Center. Email: gregory.conti@usma.edu.

Lisa Shay is an associate professor in the U.S. Military Academy's Department of Electrical Engineering and Computer Science and is Director of West Point's Electrical Engineering program. Email: lisa.shay@usma.edu.

Woodrow Hartzog is an assistant professor at the Cumberland School of Law at Samford University, Birmingham, AL, and an Affiliate Scholar with the Center for Internet and Society at Stanford Law School, Stanford, CA. Contact him at whartzog@samford.edu.

References

[1] T. Hunte, A. Fertoli, and C. Hamilton, "NYPD Commissioner calls for more surveillance cameras," *WNYC News*, Apr. 22, 2013.

[2] "Department of Defense Strategy for Operating in Cyberspace." U.S. Department of Defense, July 2011.

[3] B. Schneier. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*. Springer, 2003.

[4] K. Hawley. "Why airport security is broken – and how to fix it," *Wall Street J*., Apr. 15, 2012; http://online.wsj.com/article/SB10001424052702303815404577335783535660546.html.

[5] "Response to 'bag check' cartoon," *The TSA Blog*, Oct. 23, 2009; http://blog.tsa.gov/2009/10/response-to-bag-check-cartoon.html.

[6] L. Shay, W. Hartzog, and G. Conti, "Beyond sunglasses and spray paint: A taxonomy of surveillance countermeasures" presented at Int. Symp. Technology & Society (Toronto, Canada), June 27–29, 2013.

[7] A. Cavoukian, "Privacy by design;" http://privacybydesign.ca/, accessed Nov. 20, 2012.

[8] A. Kingsley-Hughes. "Are you following the NSA's 'Home Network Security Best Practices'?," *Harware 2.0*, ZDNet, May 2, 2011; http://www.zdnet.com/blog/hardware/are-you-following-the-nsas-home-network-security-best-practices/12589.

[9] "HTTPS everywhere," *Electronic Frontier Foundation*; https://www.eff.org/https-everywhere, accessed Nov. 9, 2012.