Governments, commercial actors, and private citizens considering new cybersecurity deployment measures either explicitly or implicitly balance the costs to be incurred against the benefits to be derived from the new steps under consideration

Servers in a data center
(BalticServers / CC BY-SA 4.0)

How Much Does a "Privacy" Weigh?

Paul Rosenzweig

Benjamin Franklin is famous, in part, for having said, "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety." Though historical evidence suggests Franklin's quote has been misinterpreted,[1] the aphorism has come to stand for the proposition that privacy and security stand in opposition to each other, where every increase in security likely results in a commensurate decrease in privacy, and vice versa.

Couched in those terms, the privacy/security trade-off is a grim prospect. We naturally want both privacy and security to the greatest extent possible. But Franklin tells us this is impossible — that privacy and security are locked in a zero-sum game where the gain of one comes only at the loss of the other.

Of course, this characterization is assuredly flawed; it is certainly possible to adopt systems that maximize both privacy and security in a Pareto optimal way. That is one of the reasons why so many privacy and security experts simply revile the "balancing" metaphor — it obscures more than it illuminates.

But let us, for now, put this debate aside and acknowledge that the balance metaphor is a partially accurate depiction of reality. At least in some instances, increases in security *do* necessitate decreases in privacy, and vice versa. The long-standing debate over encryption technology, for example, appears to be a clear case where tradeoffs are inherent to any policy decision.[2]

This acknowledgment challenges us in many ways, at least one of which has garnered only infrequent notice. It boils down to two questions: How do we measure privacy? How do we measure security? This short commentary highlights these questions and begins to outline some thoughts about its resolution.

These two queries would seem to be natural ones. After all, if we are going to trade security for privacy (or the reverse), we need to assign each a metric value of some sort in order to judge whether the tradeoff is worthwhile. Most people, for example, might be willing to trade a tiny bit of privacy for a thousand-fold increase in security. Conversely, most would not likely be willing to sacrifice substantial privacy for a negligible security gain.

Buried in that commonsense consensus are some hard issues of measurement: What is a "tiny bit"? How do we measure a "thousand-fold increase"? And what makes something "substantial" or "negligible?"

MEASURING SECURITY

How do we quantify security? This fundamental question underlies almost all modern national and commercial security decisions. The cost-benefit analysis inherent in measuring security drives decisions on new car safety devices, airplane maintenance schedules, and the deployment of border security systems. Indeed, in a world where resources are finite, some assessment of risk necessarily attends any decision — whether implicitly or explicitly.

What is true generally is equally true in the field of cybersecurity. Governments, commercial actors, and private citizens considering new cybersecurity deployment measures either explicitly or implicitly balance the costs to be incurred — whether monetary or in terms of changes to enterprise efficiency — against the benefits to be derived from the new steps under consideration.

The problem with this rather straightforward account of enterprise decision-making is that no universally recognized and generally accepted metric exists to measure and describe security improvements. Unlike, say, the science of electricity, where the general safety of a new electric outlet can be measured and described in a way that can be replicated by others, security generally (and cybersecurity, in particular) remains more art than science.

For example, we can and do understand that a new

Passengers use Global Entry kiosks at an international airport (James Tourtellotte / Public Domain)

intrusion detection system improves the security of an enterprise, but we cannot say with any confidence by how much it does so. Likewise, we can and do say that any deployment of a new system — say, an upgrade to an accounting package — will bring with it unknown or previously nonexistent vulnerabilities that might manifest themselves. And yet again, we cannot with confidence measure the change.

Grappling with this challenge and others like it is fundamental to the maturation of an enterprise cybersecurity model. When a corporate board faces a security investment decision, it cannot rationally decide how to proceed without some concrete ability to measure the costs and benefits of its actions, nor can it choose between competing investments if the comparative value of those investments cannot be measured. Likewise, when governments choose to invest public resources in a security measure or otherwise regulate private-sector activities, they must do so with as much information as possible.

MEASURING PRIVACY

The same problems exist, to an even greater degree, when we turn to the question of measuring privacy.

To begin, privacy seems to be inherently less capable of measurement than security. At least in the security context, we can imagine some concepts that lead to neutral, objective metrics of success. Security might, for example, be measured by lives saved, intrusions prevented, crime reduced, or even malicious actors captured. We might even decide, in some contexts, that we care less about the harm caused by the security breach than we do about recovery from the breach, and thus choose a security metric based on how quickly we can overcome the effects of a security failure. None of these measurements would be perfect, but in theory, we might begin the discussion.

In the case of privacy, we are more skeptical of the existence of neutral, objective metrics. This is, in part, because privacy is in many ways a hedonic value, which is to say that different individuals assess it in varying ways. Some would gladly trade personal data privacy for increased physical privacy, as evidenced by the fact that many participate in Global Entry and the Transportation Security Administration's (TSA) Pre-Check program, which allows the government to screen their data for threat indicators in exchange for an easier physical screening experience when traveling. Others, however, might make the contrary choice, preferring data privacy while accepting an increased compromise of their physical privacy. We know of no way of determining which one is "right" and which is "wrong" in that assessment.

Even more problematically, we might not only disagree as to which privacy value is superior, we might also disagree on the intensity of our preference. If one person feels strongly about his choice and another person is indifferent to the matter, that makes the privacy measurement difficult. In short, because people experience privacy very differently, it is much harder to imagine a uniform, generally agreed-upon privacy metric.

One way we deal with this uncertainty now is to hide it behind ambiguous phrases that hint at metrics without any actually existing. Regulators in Europe, for example, ask whether privacy disclosures are "proportionate" or whether systems of privacy protection are "adequate." In some ways this is understandable — they are trying to

give expression to the inexpressible. But in the end, this phraseology is little more than the law of the Chancellor's foot, disguising decisionmaker-based policy preferences as some objective criteria.[3]

Another way to deal with the privacy metrics problem is to deny that it is relevant to a policy discussion. The question of metrics, and efforts to answer it, are only of interest to those who begin from the first principle that neither privacy nor security are absolutes. There are some who disagree — notably those who think privacy is an inherent human right that cannot be extinguished or traded away. For them, this entire exercise is an affront.

But this position is surely untenable. Protecting privacy requires acknowledging that both privacy and security are instrumental values and not absolutes. To be sure, this makes policymaking far more difficult. It means, for example, that we need to look at privacy as a construct used to protect other important values — things like autonomy, self-determination, democracy, and liberty of conscience — and try to be clear about connections between them. But the fact that an exercise is difficult does not mean the effort should not be made.[4]

THE SOLUTION

So where does that leave us? Is it impossible to measure privacy or security at all? Is the tradeoff paradigm flawed at the foundation because it demands that which does not yet exist and, worse yet, cannot reasonably be thought to ever be feasible?

One certainly hopes not, for there is another failure mode that is possible — the opposite of valuing privacy as an absolute: the belief that if privacy cannot reasonably be measured, then its value may be assessed as nonexistent. When combined with our security impulse, this lack of a privacy metric can drive us to disregarding privacy altogether. And so, as a result, the pendulum swings — from 9/11 to Snowden and then, perhaps, back again. This sort of schizophrenia leads to bad policy.

How, then, do we square the circle and measure privacy? The answer likely lies in the concept of consequence rather than intrusion.[5] To be more explicit, the measure of privacy — if we can develop one at all — depends on tying privacy intrusions to real-world consequences: insurance denied, job applications rejected, or searches conducted. That sort of variegated, diffuse concept of privacy harm is assuredly difficult, but the lack of any attempt to measure privacy at all is even more problematic.

Because the problem of measuring security and privacy is at the core of sound policy, law, and business judgment, it is critical to get right. The absence of agreed-upon metrics to assess either means that many companies and agencies lack a comprehensive way to measure concrete improvements in their security or privacy protection. To that end, the U.S. government needs to launch an initiative to build a consensus around how to fill that gap. Without measurement, we are doing nothing but expressing our opinions and preferences — and in a time of enhanced threats, constrained resources, and changing notions of privacy, that simply is not an adequate response. In the end, we really must know just how much a "privacy" weighs.

---

[1] Benjamin Wittes, "What Ben Franklin Really Said," Lawfare Blog, July 15, 2011, <https://www.lawfareblog.com/what-ben-franklin-really-said>.

[2] From The Chertoff Group, The Ground Truth About Encryption And The Consequences of Extraordinary Access, 2016, <https://cdn2.hubspot.net/hubfs/3821841/docs/238024-282765.groundtruth.pdf>.

[3] The law of the Chancellor's foot refers to a law that depends exclusively on the predilections and tendencies of the decision-maker. As John Selden put it in the 17th century, "Tis all one as if they should make the standard for the measure we call a foot, a Chancellor's foot; what an uncertain measure would this be? One Chancellor has a long foot, another a short foot, a third an indifferent foot: 'tis the same thing in a Chancellor's conscience." J. Selden, "Table Talk," quoted in Michael Evans, Ian Jack, eds., Sources of English Legal and Constitutional History, at 223–24 (Sydney: Butterworths 1984).

[4] Paul Rosenzweig, "Whither privacy?" Surveillance & Society, 10, 344-47 (2012), <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/whither/whither>.

[5] Paul Rosenzweig, "Privacy as a Utilitarian Value," Lawfare Blog (November 12, 2014), <https://www.lawfareblog.com/privacy-utilitarian-value>.

Paul Rosenzweig

Paul Rosenzweig is a Senior Fellow at the R Street Institute and a Professorial Lecturer in Law at George Washington University. He served as the Deputy Assistant Secretary for Policy at the Department of Homeland Security from 2005 to 2009. He is also the Principal at Red Branch Consulting.