Compromising Over Technology, Security, and Privacy

Commentary

GUS HOSEIN
Privacy International, UK

The post-Snowden debates have often referred to an alleged trade-off between human rights and security that digital citizens need to negotiate, and to a balance that needs to be struck by policy makers. In this brief commentary, Gus Hosein problematizes the often uncritical discussion over an alleged balance between rights and security by addressing the recent conflict between Apple and the FBI over the encryption of mobile phones. He argues that an increase in privacy will also enhance the security of digital citizens.

Keywords: privacy, security, Apple, FBI, encryption, policy

How do we balance the need to secure society with the individual's right to privacy? Debates on surveillance and ubiquitous data monitoring by intelligence agencies often boil down to this question. It sounds logical and it allows us to reduce a complex technological issue to a widely understandable social concern. However, as I will argue, this is not a helpful way of approaching one of the key debates of our times.

To imagine a balance is to imagine that there are only two entities. Yet to limit our thinking to either the protection of privacy in the modern era, or the maintenance of a secure society, is a simplification that is inadequate for understanding the complex interplay between security and privacy. *Complex* here means that a far wider range of issues need to be considered than just the individual's demand for privacy and society's need to protect itself and its citizenry. Technology is one such, particularly elusive, issue.

The latest high-profile example of the interplay between security and privacy is the Apple and FBI court case from February 2016. In this case, the FBI asked the court to demand that Apple assist the FBI to gain access to the work phone of one of the San Bernardino attackers.[1] The device was secured by Apple's operating system, which included encryption that made the data inaccessible to the FBI. The FBI argued that Apple needed to compromise and build a system that allowed for government access to this one phone. This led to discussion in the United States and beyond about the balance between security and privacy, focused on issues of encryption. In March 2016, the U.S. attorney general stated that she

[1] In December 2015, two attackers killed and seriously injured several dozen people at a San Bernardino County Department of Public Health training event and Christmas party.

supported “strong encryption,” but not “warrant-proof encryption” (Geller, 2016). President Obama explained his position as follows:

> We recognize that just like all of our other rights, freedom of speech, freedom of religion, etc., that there are going to be some constraints imposed to ensure we are safe.
>
> I am of the view that there are very real reasons why we want to make sure the government cannot just wily-nilly [sic] get into everyone’s iPhones or smartphones that are full of very personal information or very personal data.
>
> We also want really strong encryption . . . [though] there has to be some concession to the need to be able to get to that information somehow.
>
> I suspect the answer will come down to how can we make sure the encryption is as strong as possible, the key is as strong as possible, it’s accessible by the smallest number of people possible, for a subset of issues that we agree are important. (quoted in Constine, 2016, paras. 12–15)

His take appears nuanced, and the attorney general’s distinction sounds logical. Both suggest that some form of political compromise is possible: Access could be given to phones belonging to a small number of reasonably targeted individuals, but not to the general public. Both point to a necessary balance—an equilibrium that involves taking a bit from one side (privacy) to give it to the other (security). This narrative presents a solution, as it states that compromise is possible and reasonable. And it is convenient because it simplifies complex problems.

Complicating Compromise

However, once we start dealing with technology, this act of compromise becomes far less clear. The specific characteristics, challenges, and opportunities of technology make the distinction between strong and warrant-proof encryption equivalent to supporting drinkable water, but not clean water. On the surface, the distinction may sound logical, but if we look at the details, it becomes more difficult.

To better understand this conundrum, we may turn toward the voices of experts. These “epistemic communities” have proven influential in challenging technology and science policy debates: In environmental debates, they are climate scientists; in food safety, they are biologists and agriculture experts. They may disagree among themselves on specifics, but on most matters, there is a common understanding.

In this current debate around privacy and security, and many related debates in our field, the experts are security researchers. They analyze the complications and risks of security, and the vast majority agree on the core issues. These include a widespread consensus that compromising encryption inevitably results in undermining the security of communication systems, and thus the security and privacy of Internet users. A number of seminal reports over the past 20 years have consistently explained and reaffirmed this position (Abelson et al., 1997; Abelson et al., 2015). Security experts typically accept that it is possible to build a “warrant-friendly” encryption system but warn that this would create significant risks that are deemed unacceptable to this expert community. According to them, the only safe encryption system is one that is likely to be described as “warrant-proof.”

That coherence within the epistemic community is not shared by governments. As we know, not least, from the Snowden leaks, governments have significant surveillance interests, and they argue for “concessions” (as in the quote from President Obama) to encryption and Internet security. Yet, at the same time, former NSA directors have proclaimed that strong encryption is essential (Franceschi-Bicchierai, 2015). The FBI even once had content on their website advising smartphone users to encrypt their devices (Pagliery, 2016).

Although this dissonance seems confusing, it is sensible. A department of defense or national defense agency of any given country should resist another country’s warrant-friendly encryption being forced on their own citizens because they would know that their citizens and government officials are subject to foreign attack and therefore need the strongest forms of protection. Law enforcement officials who want to see a reduction in phone thefts and identity fraud would welcome stronger locks and the use of encryption. At the same time, this may not be in the interest of the national security agent who wants to know what a foreign terrorist is doing and the law enforcement officials who investigate child porn, drugs, and gang activity.

What emerges from this perspective is that a distinction of security versus privacy is inadequate and simplistic. We can fight a war of rhetoric on the simple balance of those two entities, which is typically reflected in front pages and unnuanced court cases. Or we can seek to introduce new voices and narratives and show how complex and fascinating this problem is. Then we may come to some resolution.

Does It Move?

As executive director of an organization campaigning on civil liberties, it is easy to extoll the virtues of these alternative voices because, in this debate, those voices endorse my worldview. But at the moment, at least on digital security, they have the more profound arguments than the mere balancing of the goods of state security and user privacy.

We need to understand the social issues around us (laws, practices, cultures) as both movable and immovable, just as the technological issues around us (mathematics, security engineering, physics of materials, biology of DNA) are sometimes immovable and sometimes quite movable. In highly emotive debates about state power, national security, and the rule of law, the fact that these issues are mobile dynamics is sometimes forgotten.

For instance, for years we asked companies to include encryption in their products, but their engineers and business teams said it would be too expensive and users did not demand it. Those were supposedly the scientific realities. Yet we have managed to change their minds, to some extent, although government abuses and security failures also helped along the way. Now, as a result of our work (a bit) and the work of Edward Snowden (mostly), the articulations of the companies' engineers, and now some CEOs, are very different: Security has become a part of privacy.

The Apple v. FBI fight has demonstrated this. At long last, after years of civil libertarians saying so, Apple says that building strong security into their products is essential. Experts have found their voices and articulated a similar concern. The U.S. government argued in the court case that Apple should build a mechanism so that it could get access to the iPhone, to undo the security. It argued that this would only be used in this particular case and was not a substantial demand for such a rich company.

Experts varied in their opinions on this specific point, and Apple raised many security contentions. My own organization contributed to the debate by stating in our amicus brief that the international precedent is too great. Others spoke out on the political and legal implications. But everyone agreed on the fundamental premise—even the attorney general and the president of the United States have now said it: Building strong security into our systems is essential.

The FBI almost stands alone in saying that there is no risk in building a single solution to compromise the security of a single phone. And when you start including in the balance the importance of the security measures in the phone, the value of digital security to our economy, how global commerce and social infrastructure relies on this security, and how Apple operates in many different markets and under different legal regimes, the problem becomes too complex to point to a simple balance.

A compromise here is not easy nor necessarily desirable. I relish this complexity. Now we only hope that courts everywhere will also relish it. Our legislatures, we hope, shall too. And so must the public.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., . . . Schneier, B. (1997). *The risks of key recovery, key escrow, and trusted third-party encryption.* Retrieved from https://www.schneier.com/cryptography/archives/1997/04/the_risks_of_key_rec.html

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., . . . Weitzner, D. J. (2015). Keys under doormats: Mandating insecurity by requiring government access to all data and communications. *Journal of Cybersecurity, 1*(1), 69–79. Retrieved from http://cybersecurity.oxfordjournals.org/content/early/2015/11/17/cybsec.tyv009.full?ijkey=mjwJomF75oqYdwm&keytype=ref

Constine, J. (2016, March 11). What Obama said about encryption and tech's double-edged sword at SXSW. *Tech Crunch*. Retrieved from https://techcrunch.com/2016/03/11/obama-sxsw/

Franceschi-Bicchierai, L. (2015, October 6). Former NSA chief: I “would not support” encryption backdoors. *Motherboard*. Retrieved from http://motherboard.vice.com/read/former-nsa-chief-strongly-disagrees-with-current-nsa-chief-on-encryption

Geller, E. (2016, March 9). U.S. attorney general defends fight against Apple over terrorist’s iPhone. *The Daily Dot*. Retrieved from http://www.dailydot.com/layer8/apple-doj-encryption-loretta-lynch-senate-judiciary-hearing/

Pagliery, J. (2016, January 13). Ex-NSA boss says FBI director is wrong on encryption. *CNN*. Retrieved from http://money.cnn.com/2016/01/13/technology/nsa-michael-hayden-encryption/