Surveillance Resistant Systems

8 November 2018

When we design and construct systems within a democratic society, we must first ask ourselves who the systems are being designed for.

Historically, we have not built systems that serve the needs of the marginalized, and the resulting asymmetrical power distribution has led to surveillance and censorship at best, and genocide at worst. Today, the threat to the marginalized is still often from the institutions that ostensibly exist to keep our society safe. Black and indigenous people of colour, queer people, trans and non-binary people, sex workers, and people with low/no income still face tremendous power asymmetries in the systems we have constructed and force them to interact with. Colonialism and white supremacy are baked into the core of our political and social systems and, while we might all have a superficial desire to reject those concepts, they are nevertheless weaved into our institutions of law enforcement, government, intelligence, education, and media.

Thus when we speak about building robust, secure computing infrastructure, we must look around and see who is not present at our table. We must speak about building systems which actively resist surveillance and censorship, and which enforce consent and promote privacy. We must speak about systems that are designed to resist our weakest authoritarian impulses, and be resilient to subversion from both inside and out while our progress as a society unfolds.

Encryption is a fundamental building block in the construction of robust computing infrastructure. While questions have been raised about whether strong encryption practices should be curtailed, we argue that encryption is under-used in modern systems, and efforts should be made to *increase* the promotion, adoption and development of strong, usable, pervasive, default encryption. Many solutions have been proposed (formally or informally) to weaken encryption (or force compelled decryption), deploy censorship filters, and otherwise increase the ability of the government to surveil the people it serves. The nature of systems that facilitate censorship, surveillance and exploitation is that they—by design—leave holes open in the systems they target. These holes are not only exploitable by those who know how to access them now, but also by enemies who gain access in the future. Deliberately perforating our critical (social) infrastructure under the assumption that it will only be exploited by the good guys is negligence and should not be tolerated.

Similarly, we can address the issue of "dual purpose software," i.e. software that can both be used to test a target system for vulnerabilities and also to exploit it. The development of such software is essential to building a secure society. How can we fix holes if we do not allow our researchers to find them first? This is why it is essential that the government place no burdens or restrictions on those developing and distributing such tools.

What of so called "information operations," i.e. the explicit targeting of certain kinds of speech that intend to alter the public discourse? Propaganda is not a new phenomena; governments, corporations and activists have used information warfare for as long as there have been causes. The first response

to negative propaganda is typically to try and censor it; we must resist that urge, and instead promote schemes that provide greater access to information, equitable education opportunities, and the development of artificially intelligent personal filters for those who are faced with harassment. We can make people aware of dangers they might face, without simultaneously forcing them through a deluge of grotesque messages every day. Further, an ability to censor implies an ability to surveil, and we assert that it is not the place of government and law enforcement to interfere in the speech that takes place between people. Such approaches are counter to the goal of a free society that upholds the principles of freedom of speech and association.

Security is, fundamentally, a subset of privacy. When we speak of efforts to improve cybersecurity, we do ourselves a disservice if we do not build those efforts on a strong foundation of privacy; a foundation not rooted in regulation but in real, technologically enabled, enforced, consent. We must not just passively allow but instead actively encourage individuals to acquire as much consent over their lives as possible.

Only on that basis, through pervasive encryption, data sovereignty, and a focus on the needs, concerns and consent of the most marginalized in our society, can we build a secure future.

Sarah Jamie Lewis
Executive Director, Open Privacy Research Society