How Secrecy Leads to Bad Public Technology

Julia Slupska
Center for Doctoral Training in Cybersecurity
Oxford Internet Institute

Jeanette Lowrie
Tech Worker Coalition, San Diego

Dr. Lilly Irani
Associate Professor
Institute for Practical Ethics
Design Lab
UC San Diego

Dr. Deian Stefan
Crypto and Security Group
Computer Science Engineering
UC San Diego

UC San Diego
ARTS AND HUMANITIES
Institute for Practical Ethics

UC San Diego
THE DESIGN LAB

"Security through obscurity" is not an effective way to maintain cybersecurity in systems.

System security should not depend on the secrecy of its implementation (National Institute of Standards and Technology 2008). A widely accepted principle of cryptography, Kerckoff's Principle, argues that cybersecurity must be robust against an enemy that knows how the system is constructed. Systems that rely on secrecy are vulnerable to breaches. Further, commercial systems cannot be kept secret as they are sold on the market. Best practices for Internet of Things and smart city cybersecurity include clear expectations about maintaining the security of infrastructure and data flows (Goodman 2020). This allows technical experts and members of the public to review and identify potential problems before data breaches happen (Bellovin & Bush 2002).

Allowing law enforcement to keep some technologies secret is a disservice both to the public and to law enforcement.

The premise of the "anti-circumvention argument" is that police must keep secrets in order to preserve their investigative advantage over sophisticated criminals. But secrecy also imposes costs on the law enforcement agencies in terms of public confidence, public input, and open exchanges of best practices (Manes 2020). "Transparency strengthens, and the perception of secrecy weakens, public confidence and trust in law enforcement" (Brechner Center for Freedom of Information, 2018). If a steward of a technology does not disclose some of its capabilities, this may mean they do not have a clear understanding of its functions, including legal and technical limitations. This creates an ineffective self-regulation regime "in which law enforcement agencies write their own rules, behind closed doors, about how they can deploy technologies" (Manes 2020). As law enforcement may lack the necessary expertise to investigate the technology, they often rely on information from the vendor, who has an incentive to overreport efficacy and downplay risks.

Vaguely worded "security concerns" can be and have been used to target protestors or channel suspicion against marginalized communities.

Police surveillance techniques are used ''to disrupt or discredit the activities of groups and individuals deemed a threat to the social order'' (U.S. Senate 1976, cited in Gilham

2011). This often includes surveilling protestors--such as on anti-war, anti-police brutality, civil rights and union groups--both during and *between* protest events (Gilham 2011). Such surveillance threatens free speech and the right to assemble, particularly under conditions of secrecy. As Manes (2020) points out, "if the public does not know the rules under which surveillance technology can be deployed, the threat to civil liberties is greater" as this uncertainty creates a chilling effect beyond the actual capabilities of the technology. Furthermore, discrimination on the basis of race, ethnicity and religion shapes which groups are likely to be deemed a threat; this is evident in the way Muslim communities in the US and the UK have been criminalised due to Islamophobic approaches to antiextremism (Kundnani 2015).

Excessive secrecy renders accountability mechanisms largely meaningless.

This has played out at the national level in post 9/11 decision-making which "stymies most efforts to hold the government accountable for its abuses" (Setty 2015). Such forms of regulation "mimic and ultimately undermine the rule of law" by becoming relevant only when leaked information becomes available (Setty 2015). Secrecy also delays the development of laws governing novel technologies, widening the gap between technological development and regulation enforcing civil liberties and police conduct (Manes 2020).

Bibliography

Bellovin, Steven; Bush, Randy (February 2002), Security Through Obscurity Considered Dangerous, Internet Engineering Task Force (IETF), retrieved December 1, 2018

Brechner Center for Freedom of Information. (2018). Transparency and media relations in high-profile police cases. Retrieved from: http://brechner.org/wp-content/uploads/2018/06/2018-06-07-UF-Brechner-report-and-recommendations-re-KCSO-Public-Information-Practices.pdf

Goodman, Ellen P., Smart City Ethics: The Challenge to Democratic Governance in the Oxford Handbook of Ethics of AI (edited by Markus D. Dubber, Frank Pasquale, and Sunit Das) (July 2020). Oxford Handbook of the Ethics of Artificial Intelligence (Forthcoming), Available at SSRN: https://ssrn.com/abstract=3391388 or http://dx.doi.org/10.2139/ssrn.3391388

Gillham, P.F. (2011), Securitizing America: Strategic Incapacitation and the Policing of Protest Since the 11 September 2001 Terrorist Attacks. Sociology Compass, 5: 636-652. https://doi.org/10.1111/j.1751-9020.2011.00394.x

"Guide to General Server Security" (PDF). National Institute of Standards and Technology. July 2008. Retrieved 2 October 2011.

Kundnani, A. (2015). *The Muslims are Coming!: Islamophobia, Extremism, and the Domestic War on Terror*. London: Verso.

Manes, Jonathan, Secrecy & Evasion in Police Surveillance Technology (January 1, 2020). 34 Berkeley Technology Law Journal 503 (2019), University at Buffalo School of Law Legal Studies Research Paper No. 2018-006, Available at SSRN: https://ssrn.com/abstract=3265072

Setty, Sudha Surveillance, Secrecy, and the Search for Meaningful Accountability, 51 STAN. J. INT'L L 69 (2015).

U.S. Senate. 1976. Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, 94th Congress, Second Session, Book II. Washington, DC: U.S. Government Printing Office.