Event Recap: What Are the Consequences of Backdoors for Online Privacy?

Kir Nuthi

April 18, 2023

Law enforcement agencies are concerned about Apple's new end-to-end encryption protections for iCloud, arguing more warrant-proof encryption compromises their ability to protect the global public and even calling for "lawful access by design." The Center for Data Innovation convened experts to discuss end-to-end encryption's potential benefits and costs and what law enforcement access to data could look like in the future.

Katie Noyes, Section Chief of the Science & Technology Branch of the Federal Bureau of Investigations (FBI), discussed how the FBI is asking for security-by-design where the capabilities of lawful access are implemented during the design phase and not as an afterthought. She emphasized that the FBI does not want to weaken security and even wants strong encryption, and instead wants a balanced approach between strong privacy or cybersecurity and lawful access in place. Noyes described what the FBI wants as modernization that balances the security encryption provides with lawful access. She believes the FBI's goal for a balanced approach would preserve privacy and find justice for victims.

Patrick Eddington, Senior Fellow at the Cato Institute, described end-to-end encryption to be as American as apple pie and focused on the constitutional importance of free speech when discussing encrypted communications. Eddington also argued that compromising end-to-end encrypted services would make journalists, confidential sources, and even government assets more vulnerable. Eddington also pointed out that cars are routinely misused, but the U.S. government doesn't try to ban them, which is unlike how law enforcement proposes to treat end-to-end encryption.

Jumana Musa, the Fourth Amendment Center Director for the National Association of Criminal Defense Lawyers, focused on the place warrants have in the encryption conversation. Warrants keep law enforcement from rifling through people's things for evidence. Warrants, however, do not guarantee that law enforcement will find what it is looking for or understand what it finds. Additionally, Musa focused on how law enforcement can perform smartphone extractions that get around much of the end-to-end encryption messaging protections once the phone is opened. While it would be useful and convenient for law enforcement to get into smart devices more easily through lawful access, that does not make those tactics constitutional or lawful. Musa warned that there is no balance when it comes to the Constitution and that the United States needs to protect fundamental constitutional provisions that keep people's privacy protected and ensure the government does not have constant access to the public's personal information

Gabriel Kaptchuk, Research Professor in Computer Science and Research Development Fellow for Boston University's Hariri Institute for Computing, brought the technologist's perspective to the discussion. Kaptchuk argued that today's encrypted messaging tools and hardware do well at protecting people's privacy. Additionally, encrypted messaging is a strong way to protect many marginalized or vulnerable communities from the government and bad actors. Kaptchuk also argued that lawful access is unlikely without significant conversations about what is and isn't technically possible.

Much of the debate focuses on whether lawful access should be a conversation about getting the bad guy or protecting civil rights. Noyes wanted to shift the debate to focus on bringing criminals to account and victims into the conversation. Eddington, however, worried that law enforcement's get-the-bad-guy mentality was an overarching problem in the end-to-end encryption debate. According to Eddington, minimizing the number of victims through lawful access could and would unintentionally create more victims through those same backdoors. Musa added that protecting victims also involved protecting people from government overreach and cited cases of FBI interactions with the Black Panthers, protest movements, and mosques. While no conclusion was reached, Noyes asked to continue the conversation offline. She wanted the FBI to collaborate and partner with civil society organizations as they continue to engage in the conversation surrounding lawful access. The lack of consensus helped highlight the importance of end-to-end encryption for privacy, free speech, and security, as well as how any method of finding and prosecuting bad actors cannot risk the online safety end-to-end encryption provides.