GOVERNMENT SURVEILLANCE, SECURITY AND PRIVACY: DOES SECURITY ALWAYS WIN? (PART 2)

Jeffrey J. Blatt (/january/?author=58897153db29d65fe80f56a3) · Data Privacy (/january/?category=Data+Privacy)

A question posed during the Data Privacy Asia 2016 conference held in Singapore in November 2016 was should there be a digital safe place where a person can go dark and be beyond the reach of government?

When attendees of the Data Privacy Asia 2016 conference were polled, a significant portion said they don't trust their own government and, of course, they didn't trust any other government either when it came to issues of privacy. At the same time attendees firmly believed that there should be a digital safe place, a place where we can 'go dark', a place that we can call our own. This is very fundamental. The EU concept that privacy is a fundamental human right was by and large reflected by the opinion of the conference attendees – and that we cherish our privacy and it's important to us.

At the same time law enforcement has a legitimate need, using lawful processes such as search warrants for lawful interception and access, to obtain digital data to solve serious crimes. When we consider the question of digital privacy, we cannot ignore the lawful and reasonable need for law enforcement access. The problem is, unfortunately, that governments around the world have different definitions of what a 'crime' is. While we would all agree that murder, rape, kidnapping and other violent crimes justify government access to digital data, on a showing of probable cause and a warrant, what about overly broad definitions of sedition, lese majeste, defamation? When spoken words, Facebook 'likes' and posts are considered criminal for expressing an opinion in certain countries, we start to cringe and seek safe places where we can express views without fear of arrest. It is at the fringes, not at the core, that many of us would say a government has gone too far.

The Search for Balance.

It's becoming more and more apparent that the right to privacy must be balanced – and that there is an obligation by a government to still do good old-fashioned police work, based on strong legal principles, and not just vacuum up our personal digital data when we consider where the line should be drawn. In the Apple/FBI case, there existed a situation where the company had created effectively a digital 'safe place'. Apple, as a company, decided that they were going to strongly encrypt data on the iPhone, such that even in the face of a search warrant, they were unable to help the government obtain a person's data on their phone. The action by Apple represented a shift in the source of personal liberty and rights. Should we have to rely on tech companies to make these decisions for us? I think there's an argument that the law should actually provide that safe place, but the reality is this – Apple decided to level the playing field around the world for us all. In the face of differing laws in nations around the world as to what constitutes a 'crime' and differing scope of nations' laws, Apple gave us something that, one could argue nations should be providing, namely, a digital safe place. This is unprecedented – that private tech companies (mostly from the U.S.A.) are empowering us where governments are generally moving in the opposite direction.

Should a foreign government have the legal right to remotely hack, compromise, or search a digital device for domestic criminal investigation in that country and then pass that evidence onto the country that you call home? This is not a theoretical issue. Actually, the U.S. government regularly engages in hacking of computers that it calls network investigative techniques or NITs under rule 41 of the U.S. Federal Rules of Criminal Procedure.

Just how valuable these powers can be became apparent during what is known as the 'Playpen Case'. In this case the FBI seized a child pornography site that was run on the 'Dark Web' and assumed control. The FBI for a time then ran the site seeking to identify those downloading child porn. The FBI deployed a network investigative techniques where they created malware such that anybody that went to that site to download illegal porn unknowingly downloaded the NIT malware that reported the user's real IP address back to the FBI. Many of those IP addresses were in the U.S., some were in Europe, and some were in Asia. Arrests were made in the U.S., and for suspects outside the U.S. the FBI reported that information back to the respective countries for prosecution. This was done under a search warrant that extended to computers all over the US and to all over the world.

Since Playpen, Rule 41 has expanded – allowing U.S. judges to issue warrants when somebody is using TOR or they're using a VPN such that the individual is masking the actual location of their computer and the real IP address. Effectively, U.S. investigations are now worldwide, extraterritorial and independent of local nations' laws – and of course, other countries can take similar approaches deploying their own malware globally for various objectives they define (e.g. political, criminal or national security). This global extension of search powers extraterritorially has rendered these investigations borderless and effectively resulted in a free for all in the sense that regardless of where you are and what local laws apply, no one is safe from a foreign or local government search (via malware). Of course, this has always been the case in terms of cyber criminals also seeking to gain access to our data.

The Issue of Biometric Keys.

The use of biometric keys is becoming a more and more popular way to protect access to data. For example, fingerprint readers, voice authentication, iris scanners, face scanners. Using biometric keys that are unique to an individual does have the advantage of having a high degree of confidence that the person is who he or she says they are. The problem with the law in the U.S. and many other countries is that biometric attributes are not given the same level of protection as a password stored in somebody's brain. Some U.S. courts have held that a password in somebody's brain is protected under the 5th Amendment of the U.S. Constitution – the right to not incriminate yourself. Why? Because there is some degree of processing or thought process needed for someone

to write or provide that password – and that thought process, if compelled, is effectively testimonial and therefore would be a violation of the 5th (at least according to some U.S. federal court decisions).

A fingerprint, an iris scan, a face scan or things like that are not so protected. For those of you wondering, from a U.S. legal perspective, you're much better off turning off the fingerprint function on your iPhone because in the U.S. you cannot take the 5th and withhold your fingerprint to unlock the phone.

If a court issues, for example, a search warrant for the contents of your iPhone and you don't unlock it, well, physical coercion to actually take your finger and put it on the home button is not going to be a violation of your rights in the United States. Some courts in the U.S. are issuing search warrants for places that include all digital devices found at the location and a requirement that anyone at the location provide their fingers to open such devices. These warrants are not without controversy and the cases and law are not settled, but that is the direction in which the government is moving. In other countries, they may just throw you in jail until you unlock the phone or physically compel you to put your finger on that home button with no further legal process needed. As such, while convenient, the use of biometrics may not be the wisest decision in terms of keeping governments or street criminals from compelling access to you iPhone. If the government or street criminal has physical possession of your device and of your being – the biometric keys will be of little help.

Summary – This is a Complex Issue.

Privacy is a complex issue and will remain a thorny topic of discussion and legislation for the foreseeable future. As our world becomes more connected and devices, as well as data, form a greater part of our lives, we will all be faced with the question: what is too much when it comes to the balance between privacy and security – and should government be allowed unfettered access to information that we, not so long ago, had viewed as private. At the moment, the lines are blurred and technology is driving the discussion as well as the expansion of government powers of mass surveillance and access to each of our digital trails (or digital 'breadcrumbs') that we create 24 hours, 365 days a year now from cradle to grave.

Jeffrey J. Blatt ('Jeff') (/contributors#jeffreyjblatt) is a Silicon Valley pioneer who worked directly with the original founders of groundbreaking technology companies including Apple and Sun to protect and leverage their innovative technologies. He is a cyber security lawyer, privacy evangelist and TMT executive who leads the Tilleke & Gibbins' TMT practice group in Bangkok, Thailand. Jeff is a frequent speaker, author and thought leader on issues relating to data privacy, cyber security, technology, and the intersection of privacy, law enforcement and government action, in addition to technology and telecom matters. In last year's FBI v. Apple case in California, he was one of the first tech lawyers to be interviewed on live TV regarding the court order issued to Apple to assist the FBI in hacking the iPhone. Jeff is consistently recognized as a leading practitioner in TMT by publications such as Chambers Asia-Pacific, The Legal 500 Asia Pacific, and The International Who's Who of Telecoms & Media Lawyers. As recognized in his Chambers ranking, "Jeffrey Blatt is noted to be a dedicated lawyer that goes the extra mile and 'knows technology in detail."

Tagged: Government Surveillance (/january/?tag=Government+Surveillance), Security (/january/?tag=Security), Privacy (/january/?tag=Privacy)

Newer Post
Government Surveillance, Security and Privacy: Does Security Always Win? (Part 1) (/january/2017/1/26/government-surveillance-security-and-privacy-does-security-always-win-part-1)