GOVERNMENT SURVEILLANCE, SECURITY AND PRIVACY: DOES SECURITY ALWAYS WIN? (PART 1)

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

In 1949 George Orwell penned a novel that described a world where government surveillance is all pervasive. When we read 1984 today we are struck by the remarkable, and sometimes chilling similarities between the dystopian vision of the author and the pervasive nature of mass surveillance in 2017. However – does this mean that we are faced with an 'either / or' proposition? Can there be a reasonable and acceptable balance between the necessity for surveillance in an ever more dangerous world and an individual's right to privacy?

Can we, as individuals, manage to operate and live in a connected world and still retain some semblance of privacy where our online lives are subject to snooping by criminals, governments and commercial interests? This question is becoming ever more important as we realise that it is no longer feasible to go 'off the grid' and still maintain a 'normal' life. Governments across the globe cite the ever increasing risk of terrorism and security as justification for ever more broad surveillance powers. In these days of big data this question is becoming even more urgent. In the days before big data it was possible to compartmentalise our lives. We all present a persona (a 'face') to the world in our professional lives, a different one in our home lives and perhaps a third social persona in our interactions with friends. We may even have other personas on different social media platforms.

A Single Identity.

Today we're always online and plugged in, creating a stream of continuous data 24/7 and the separation of our personas simply isn't possible anymore. Your LinkedIn, your Facebook, your Grindr, your Ashley Madison, your E-Harmony, all your tweets, all of your calls, your location data, your Fit Bit/wearables, all the apps that you download and all the data that goes in and out of those apps are recorded and they collectively define you and your life, particularly to governments, to companies and to criminals – and the Internet of things will only make it worse.

Four hundred years ago, Cardinal Richelieu reportedly said "if you give me six lines written by the hand of the most honest of men, I will find something in them which will hang him." When our lives are recorded as an on-going and continuous stream of data that we all generate every day from cradle to grave, how difficult would it be for a current or future government to find something in that stream that 'violates' a law? It would seem that Cardinal's statement made 400 years ago is more true today than ever before.

The days of predictive intervention (before crime takes place) based on big data may not be far off. How many have seen the Hollywood blockbuster Minority Report? The premise of that movie was the ability to arrest somebody prior to them committing a crime based on a prediction of their behaviour. Think about that, if you have enough data about somebody, and enough processing power, you could potentially predict behaviour. If you can predict behaviour, while you may not

make a pre-crime arrest you might, however, target law enforcement and physical surveillance assets on a person/group, or make an arrest if that person/group takes a step towards the completion of the predicted crime -which may not in fact be a crime in itself. We're not that far off from that day.

Big Data is Not All Bad.

But big data and government access isn't all bad. Big data provides us with functionality never before possible. Convenience, communication, power, health monitoring, online banking – we experience the benefits of big data every single day. Many, many crimes, very serious crimes, are solved today as a result of lawful government access to cloud and device-based digital information. Electronic and surveillance communications solve many crimes, sometimes even on par with DNA evidence. In our desire to protect privacy, we must not forget that there is a legitimate place for lawful government access of data through lawful process with adequate protection of our rights. The question is where to draw the line, and unfortunately today, we see many examples of governments around the world expanding their powers because technology enables such expansion. Technology should not be the driving factor when it comes to defining the power of governments as this will assuredly lead to the 1984 scenario of George Orwell.

The Transparency Check.

Polls indicate that most people would trust their own national government more than they trust foreign governments when it comes to access of their personal data. That's natural. The question is how do you allow one government access to data and prevent other governments from getting access? As an example, say you are messaging someone from Singapore, while both parties are in Singapore but one party is a resident of Thailand. The conversation is on the subject of the Thai military and the King. It's a conversation that is not in any way illegal in Singapore. Let's assume it would be considered unlawful in Thailand. Should the Thai government, in that instance, have access to those online messages? If that access was granted then it is possible that the person would get arrested on his return to Thailand.

Conversely, what if I am in Thailand making statement that might be considered illegal in Singapore but not in Thailand? Should the Singapore government, the Thai government, or if the message goes through a U.S. intelligence collection system some place, the U.S. government, be able to intercept and read my private messages? Would it make any difference if the information is not out there in the cloud but is stored on my phone? Once you let the genie out of the bottle and grant governments access by a lawful legal process, how can we contain it? Governments (by their

nature) and law enforcement and intelligence agencies, in particular, want all your information and data. But what keeps them in check? I would argue that one factor is the requirement for disclosure and transparency.

Revisiting Apple vs The U.S. Government.

From a bit of a different perspective than what you might have seen or read about in the news, let's consider what the FBI already had before it tried to compel Apple to compromise its own iPhone security (a subject that has been covered from a legal perspective in previous editions of this newsletter – ed). From Apple, the FBI already obtained all of the data that had been previously backed up to iCloud from the iPhone in question. The phone was owned by the county of San Bernardino. It was not the suspect's iPhone. The county of San Bernardino could give consent and, in fact did give consent to search, but the FBI went ahead and got a search warrant as well.

The suspect had turned on the iCloud backup but then turned it off, some time prior to the attack. Apple had already provided the FBI with all of the information that had been backed up to the iCloud. How could Apple do that? Apple holds the encryption keys for the information in iCloud. Therefore, when faced with lawful government access request, i.e. a search warrant, Apple could and did provide that information to the FBI.

From the telecom provider, the FBI already had the call records, the SMS information, the tower location and all the other meta data information. In fact, the only data that the FBI sought in the case was any data that was stored physically in the phone.

Should a company, or for that matter an individual, be permitted to create a digital 'safe place' that not even the company could enter even on orders of the government? According to the Director of the FBI, he believes there should be no way to go dark – there should be no safe place.

The Director's argument is that before the Internet, before electronic evidence, the entire purpose of the United States 4th Amendment in the Constitution, was to protect individuals from unreasonable and warrantless searches. But that didn't mean that the government couldn't access the information, it only meant that it had to have probable cause and obtain a warrant from a judge.

An individual who had some evidence, perhaps documents or perhaps a weapon, might put that evidence in a safe in his house and throw away the key – but that did not mean the government wasn't able to get that evidence. It meant the government might have to break into the safe or use a locksmith or other mechanism to actually get into the safe. With the proper legal process followed, the FBI's position is that there is no place where you can go dark.

Of course, today, much of the critical digital data of our lives is sitting in the cloud or is stored in digital devices. Moreover, today, we are effectively compelled to give that information to third parties to hold and store on our behalf. It's quite different than if you have some evidence and you are hiding it under the carpet in the floor in your living room. Today you must give your personal information to third parties, and you are entrusting that information to a third party whether it's a telephone company or a bank or another party. Under current U.S. law, absent a specific statute, data you provide to a third party (e.g. bank, Waze history, Quicken financial data) has no reasonable expectation of privacy, and is reachable by the government. The world has changed but the law has been slow to keep up – and this is a key area where the tension between privacy and lawful government access arises.

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)