EVERSHEDS SUTHERLAND

Michael Bahar

Statement for the record

May 31, 2019

As difficult as it is to pass laws, especially potentially controversial laws, sunset provisions on national security legislation provide an opportunity to re-assess effectiveness, impacts on privacy, and opportunity costs.

Five years ago, the Privacy and Civil Liberties Oversight Board (PCLOB) published an important assessment of the Telephone Records Program conducted under Section 215 of the USA PATRIOT Act, and I am encouraged to see the Board undertaking a similarly rigorous assessment of the program that replaced it.

It has been almost five years since Congress passed the USA FREEDOM Act, which re-authorized and significantly reformed the 215 program. As both Minority Staff Director and General Counsel for House Permanent Select Committee on Intelligence (HPSCI) at the time, I worked closely on this Act, and got the opportunity to work with my colleagues in the then-Majority, in the Senate, and in the Administration to forge a compromise that would eliminate the bulk collection of telephone metadata, but retain the capability to query call detail records (CDRs). The USA FREEDOM Act also contained other meaningful reforms to the Foreign Intelligence Surveillance Act (FISA) to further enhance privacy and civil liberties.

In that five years, a lot of has changed. ***First***, the dangers of the misuse or abuse of personal information *in general* has become increasingly apparent, whether done by foreign actors, corporate actors, or individuals.

Second, technology has continued its advance. Now more than ever, individual, disparate pieces of information can more readily be put together to create whole pictures of individuals, not only of who they are, but what they want, what they do, what they fear, what they desire, and which way they vote (or could be persuaded to vote). At the same time, terrorists have increasing means to evade discovery via their call chains (not to mention the knowledge of their need to do so).

Third, US and global regulators, recognizing these two developments, have passed laws to try to shift the pendulum back toward greater privacy protections and individual control and ownership over personal information. Many of these regulations apply to governments as well as to the private sector.

One principle that emerges from these regulations, which I think is particularly helpful here, is a necessity/proportionality assessment. Under certain privacy regulations, when a company collects personal information, they are increasingly required to disclose and articulate how and why they are collecting that data, on what basis, and for how long they plan to keep it. In other words, regulations are trying to move industry away from collecting and retaining data simply because a company can. Now in civilian practice, I tend to advise companies that even if you have a legitimate business purpose for regulatory purposes, keeping vast troves of personal information may still prove inordinately costly from a business perspective, particularly in light of the growing cyber threat. The more data you have, the more data you have to protect, and the more data you may have to notify about in case of a breach.

So, I would recommend that the PCLOB, as well as the Executive Branch and Congress, look first to assess the current necessity of the CDRs collected under this authority. We are all aware of the issues the National Security Agency has had in the past year with collecting CDRs from the telecoms, but if we strip all that away, and assume the program functions as designed, is valuable intelligence being obtained? If so, how much? The PCLOB report of 2014 found that the Section 215 program provided "minimal value" in safeguarding the nation from terrorism. The Administration, at the time, insisted that there was real value in the program, often for tipping and cueing, as well as ruling out investigative avenues. They provided classified and unclassified briefings, and the Congress took a very strong look. Ultimately, Congress made the determination that the capability—if not the method—was worth retaining.

Five years later, it is worth reassessing to see whether the revised program is providing valuable intelligence, or could be if certain changes are made.

But, even if it is providing valuable intelligence, is the value sufficient to overcome the impacts on US persons? Is its effectiveness, or necessity, proportional to the privacy impacts? In this ever-increasing era of Big Data, advanced analytics and Artificial Intelligence, even metadata is becoming increasingly privacy-revealing, so it is quite possible that the privacy costs have been increasing over the past five years, and may continue to increase, which could change the equation.

In addition, recalling the original arguments to us five years ago, we heard that even if the intelligence was not that valuable yet, it *could* be—and no one wants to eliminate a tool that *could* stop a terrorist.

Five years on, it is worth re-assessing this justification as well. Is the CDR program more likely or less likely to provide valuable intelligence, and—importantly—how have the opportunity costs changed? If analysts are spending time and money on "could bes," are they spending insufficient time on "should bes"? Recall that the Congress passed the USA FREEDOM Act in 2015. In 2016, while working to pass the annual Intelligence Authorization Act, both the Chairman and Ranking Member at the time publically questioned whether too many of the nation's Intelligence Community (IC) resources were devoted to the counterterrorism (CT) fight, and not to the larger geopolitical concerns. As the years have passed, we have seen the re-emergence of geopolitics, and it is worth noting that the CDR tool is just to be used to "protect against international terrorism." Depending on what you find, that can cut in favor of expanding the program beyond CT, or it can cut in favor of eliminating the program in favor of re-allocating those resources to programs that defend the country, our allies and partners from threats posed by nation states.

It is also only fair that if we are assessing potential benefits, we assess potential costs as well. It is worth noting what the PCLOB found in 2014, that there was no "significant intentional misuse" of the 215 program, nor did it find "any evidence of bad faith or misconduct on the part of any government officials or agents involved with the program." From my firsthand knowledge of the IC, that didn't surprise me. From everything I had the honor of seeing, IC professionals were truly that: professionals. I think the vast majority remain that way. But, we shouldn't fall back too much on trust when designing intelligence systems, even though a degree of trust is always inevitable, and not necessarily a bad thing. It is also worth noting that the history of this program is not that long. This country has not been immune to intelligence abuse in the past.

Of course, another benefit of a sunset is that if the decision is made that a program is worth it, the required legislation presents the opportunity for reform. In other words, the equation can change, as Congress undertook to do five years ago. This time around, the same question can be asked: are there structural improvements and are there additional protections that can lower the privacy impacts and potential for misuse? Can we clarify and strengthen the protections for "activities protected by the first amendment of the Constitution," for example?

Finally, we should assess what would, or could, happen if the authorities were to expire. One of the arguments that weighed particularly heavily on Congress five years ago was that with congressional authorization comes statutory restrictions and oversight. Absent legislative authorization, those restrictions and oversight largely go away should a president one day rely again on executive authority to collect telephone records.

So, with that, I look forward to your questions.

Thank you.

© Eversheds Sutherland Ltd. 2019. All rights are reserved to their respective owners.
Eversheds Sutherland (International) LLP and Eversheds Sutherland (US) LLP are part of a global legal practice, operating through various separate and distinct legal entities, under Eversheds Sutherland. For a full description of the structure and a list of offices, visit eversheds-sutherland.com. US20117_061219