TAPROOT® security

Adam Klein
Chairman
Privacy and Civil Liberties Oversight Board

June 24, 2019

Dear Chairman Klein and Board members,

Thank you for your dedication to balancing America's national security and privacy needs in our post 9/11 era.

My firm Taproot Security advises clients and policymakers on cybersecurity matters, primarily federal agencies and financial institutions. I have experience in both classified intelligence work and legislative policy. I was chairman of the Financial Services Roundtable's Cybersecurity Legislation Working Group.

I write today regarding your review of the FISA Section 215 **Call Detail Records** (CDR) program as modified by the USA Freedom Act. I appreciate PCLOB's invitation for public comments. Congress will naturally look to you for leadership on CDR before its 12/15/2019 sunset.

I believe CDR is increasingly ineffective as a counter-terrorism tool. The threat landscape has shifted from the command-and-control model of Al Qaeda to the more decentralized model of ISIS and the domestic accomplices it inspires (often indirectly). As a result, traffic analysis of known targets is less likely to surface actionable intelligence. The technology landscape has also shifted, with encrypted messaging and social network apps replacing phone calls and texts. (Even texts are moving from SMS to apps like Apple iMessage, which do not generate CDRs). As a result, the 215 program has blind spots that allow terrorists to fly under its radar. Communications that still generate CDRs increasingly belong to innocent American bystanders, not terrorists.

To the extent call/text metadata does reveal useful intelligence about targets -- relationships, location, politics, religion, travel, purchases, health, etc. -- it also reveals the same information about bystanders. This is the CDR security/privacy tradeoff. Unfortunately, with the shifting threat and technology landscapes, that balance is now tipping from security benefits to privacy harms.

The USA Freedom Act changes to Section 215 exacerbated bystander privacy risk by adding the automatic second hop. This leads to a "Six Degrees of Kevin Bacon" problem whereby huge quantities of records can be released for a small set of targets. The post Freedom Act program still permits access to tens of thousands of CDRs with a single query, largely as a result of the automatic second hop. Yet any terrorist familiar with the Snowden material evades 2-hop detection simply by stretching communication chains to 3 hops.

The mere existence of large CDR databases, whether hosted in government facilities or telecom facilities, makes an attractive cybersecurity target for foreign adversaries. A breach could have grave consequences for national security as well as citizen privacy. News reports indicate even NSA and CIA fall victim to nation state actor breaches.

Other aspects of Section 215 should be preserved (traditional FBI surveillance, lone wolf, etc.) but *we recommend the CDR authority be stripped* when the USA Freedom Act is renewed for 2020. At minimum, Congress should remove the program's automatic second hop provision.

Thank you for this opportunity to share our perspective on security and privacy implications of the Section 215 CDR program.

Sincerely,

Michael McCormick
President, Taproot Security
www.taprootsecurity.com
mike@taprootsecurity.com