Matt Blaze

Written testimony before the
House Committee on Government Reform
Subcommittee on Military and Foreign Affairs
April 2, 2025

Background

Thank you Chairman Timmons and Ranking Member Subramanyam for the opportunity to offer my perspective on “Salt Typhoon: Securing America’s Telecommunications from State-Sponsored Cyber Attacks” at today’s hearing.

I hold the McDevitt chair in Computer Science and Law at Georgetown University, a joint interdisciplinary professorship spanning the university’s computer science department and law school that is focused on research and teaching at the intersection of technology and law and policy. Before joining Georgetown in 2019, I was a professor of computer and information science at the University of Pennsylvania. Prior to joining Penn, I was part of the research staff at AT&T Bell Laboratories, where I was a founding member of its secure systems research department. I hold a PhD in computer science from Princeton University (1993), an MS in computer science from Columbia (1988), and a BS from the City University of New York (1986).

I offer these comments on my own behalf, and not as a representative of my employer or any other organization.

For more than 30 years, a major focus of my research and scholarship has concerned the protection of modern communications infrastructure against the growing threat of eavesdropping and tampering by malicious actors, a broad category that can include everything from casual pranksters, to organized criminals, to well-funded industrial rivals, to domestic and international terrorists, and to hostile state actors. Much of my work has concerned the risks and tradeoffs introduced by so-called “lawful access” systems that are intended to facilitate court-authorized surveillance, but that inadvertently might expose our nation to illegal wiretaps or espionage. In particular, I have published a number of peer-reviewed research papers and technical reports on risks and security weaknesses introduced by the Communications Assistance for Law Enforcement Act of 1994 and the technologies that implement it. This work comprises much of the context for my testimony today.

Salt Typhoon and “Lawful Intercept”

In 1994, Congress enacted the *Communications Assistance for Law Enforcement Act (CALEA),* which mandates that telecommunications service providers (e.g., telephone companies) incorporate into their switching infrastructure special capabilities to support content and “pen register” wiretaps authorized by court orders. CALEA was a response to concerns raised by law enforcement that while existing analog “wireline” telephone services were relatively straightforward to intercept for wiretaps, newer digital telephony services (which, at the time, included technologies such as ISDN and rapidly growing mobile telephone services) were not compatible with existing wiretapping technology. CALEA shifted the technical burden for implementing wiretaps from law enforcement, where it traditionally had been, into the communications network itself. That is, CALEA required virtually all new telecommunications switching equipment to be designed with explicit capabilities to wiretap traffic. Every switch used to serve every customer would now have to be “wiretap ready”, even when (as is the case for the overwhelming majority of users) no actual wiretap has been authorized against them.

When CALEA was proposed, many technologists and security researchers, including myself, raised concerns that such a sweeping mandate would expose our infrastructure to attack by malicious actors who would find ways to exploit these new universal wiretap capabilities. Unfortunately, these concerns have been proven correct several times, most recently (and consequentially) in the “Salt Typhoon” attacks against the communications of high-value US targets.

While the CALEA mandates have introduced risks from the beginning, those risks have been greatly amplified in practice over the more than 30 years since the law was passed. This is because communications infrastructure, and in particular the parts of that infrastructure in which wiretaps are provisioned, has become increasingly automated and virtualized. In the 1980's and 90's (when CALEA was envisioned), telecom switches involved highly specialized hardware, manufactured by a small handful of vendors, and operated by a small number relatively stable, slow-moving service providers in heavily staffed "central offices". Critically, provisioning wiretaps generally required the intervention of a technician with physical access to the local switching equipment serving the targeted customer. This served as a natural, if somewhat unintentional, security safeguard against large-scale malicious or unauthorized abuse of surveillance capabilities. A human being employed by the telephone company was in the loop, and would be expected to notice and investigate a large scale or anomalous increase in (typically infrequent) wiretap orders if the interfaces were exploited in this way. At the same time, the "backhaul" with the content and call data from these wiretaps was typically served to law enforcement via dedicated "leased lines" running from the central office to the requesting agency. Any unauthorized wiretapper would risk exposure by needing a dedicated line running to their physical location. None of these properties of telephony in the 90's provided absolute protection, but they did add friction to task of an illegal eavesdropper.

Over time, many of these natural safeguards have fallen by the wayside as communications services have evolved. Telecom switches are now smaller and faster, serve many more customers, are often located in unstaffed or low-staffed facilities, and have more in common with general-purpose programmable computers than with the specialized central office hardware of the 20th century. Critically, they are now designed to be remotely programed, configured, and managed, often over the Internet, rather than requiring constant physical intervention by on-site technicians. At the same time, the "backhaul" for wiretaps is now as often as not delivered via the Internet rather than through dedicated leased lines, and now frequently through intermediaries that serve as "wiretap clearinghouses" between law enforcement and telecom providers.

In other words, while the legally-mandated CALEA capability requirements have changed little over the last three decades, the infrastructure that must implement and protect it has changed radically. This has greatly expanded the "attack surface" that must be defended to prevent unauthorized wiretaps, especially at scale. The job of the illegal eavesdropper has gotten significantly easier, with many more options and opportunities for them to exploit. Compromising our telecommunications infrastructure is now little different from performing any other kind of computer intrusion or data breach, a well-known and endemic cybersecurity problem. To put it bluntly, something like Salt Typhoon was inevitable, and will likely happen again unless significant changes are made.

Needless to say, court-authorized wiretaps are an important tool used by law enforcement to investigate crime. But telecommunications services are deeply integrated into the fabric of the digital lives of almost every American, the vast majority of whom will never be the subject of a criminal or national security investigation. Their communications are nonetheless often quite sensitive, and, in many cases, highly attractive targets for criminals and foreign adversaries seeking to steal financial information, obtain industrial trade secrets, or conduct intelligence operations against the United States. That is, the CALEA mandates introduce a sometimes unfavorable tradeoff between *solving* crimes (by permitting more reliable *authorized* wiretaps) while simultaneously exposing us to *new* crimes (by increasing the risk of *unauthorized* wiretaps). Because of the ways in which telecommunications switching infrastructure is evolving, the exposure created by the current CALEA requirements is likely to continue to become more severe over time.

Cryptography and Wiretap Countermeasures

An important countermeasure - for individuals, companies, and government - against large-scale unauthorized wiretapping and espionage is the use of *end-to-end encryption* by users and their devices. End-to-end encryption frustrates the collection of communications content that might be intercepted by a malicious actor who compromises telecom infrastructure (such as with an attack like Salt Typhoon). End-to-end encryption must be implemented on end-user devices (such as smartphones and computers), generally via software such as *Signal*.

While end-to-end encryption is an extremely powerful and valuable countermeasure, it is not completely foolproof or comprehensive. It is only as secure as the device on which it is implement, and complex modern devices like smartphones are known to be vulnerable to targeted attacks that might be employed by intelligence agencies (and, for that matter, by domestic law enforcement through “lawful hacking” efforts). It is also vulnerable to user error, as was rather spectacularly demonstrated in the recent incident involving a journalist being mistakenly added to a Signal chat group being used by high-level government officials to discuss a forthcoming military operation.

Summary and Recommendations

The CALEA wiretap mandates, while well-intentioned, are showing their age and effectively degrade the security of US telecommunications infrastructure. The interfaces provided by CALEA, and the services that have evolved around them, were a significant enabler of Salt Typhoon, a major cyber-intelligence operation against the United States. Similar attacks are likely to occur in the future unless significant changes are made.

The widespread use of end-to-end encryption by the public, industry, and government is an imperfect but broadly effective countermeasure that should be encouraged. But encryption alone does not protect our infrastructure, nor does it prevent the collection of valuable “metadata” about calls and communication patters that can also be obtained through CALEA systems.

Ultimately, is time to re-think CALEA. Requiring new services to be engineered with wiretapping as a central requirement is dangerous, and requiring wiretap interfaces to be present in every switch serving every customer is effectively an open invitation to foreign adversaries. At a minimum, CALEA should be revised incorporate rigorous security testing, reviewed on an ongoing basis and as new services and equipment are introduced. And the capabilities should be required to be off by default, rather than enabled even in facilities where no wiretaps are active.