Posted 11/23/15

SOMETIMES THERE IS NO "SECOND CHANCE"

Preventing horrific terrorist attacks may require new legal rules

By Julius (Jay) Wachtel. Last week, at a gathering of cybersecurity experts, an exasperated CIA Director conveyed the intelligence community's growing frustration over restrictions imposed on its information-gathering capabilities:

> In the past several years, because of a number of unauthorized disclosures and a lot of hammering over the government's role in the effort to try to uncover these terrorists, there have been some policy and other legal actions that make our ability – collectively, internationally – to find these terrorists much more challenging.

Not that those wielding the "hammers" lacked a reason. Perhaps the most eye-popping of the "unauthorized disclosures" took place nearly a decade ago when *USA Today* blew the whistle on "Mainway." This was no ordinary program. Kicked off in great secret soon after 9/11, it had been vacuuming up the particulars (but not the content) of nearly every domestic and international telephone call originating in the U.S., including date, time, duration and the identities of subscribers on both ends. With the cooperation of America's telephone carriers, and unencumbered by judicial oversight (after all, it *was* just a "catalogue"), Mainway had ballooned into a repository of *hundreds of billions* of entries.

Daylight didn't sink the effort. Despite substantial public concerns about *why*, the administration swiftly anointed Mainway as a "business record" and placed it under the purview of the the Patriot Act. FBI agents then kept things chugging along with perpetually renewable 90-day orders issued by a secret intelligence court. Finally in 2015 a Federal appellate panel ruled that the Patriot Act was, um, *inapplicable*. To head off a nasty dispute, Congress enacted the "Freedom Act." Mainway was ordered to cease operation by December 2015, and the information it collected would henceforth remain with the carriers and be obtained through conventional means, that is, by demonstrating probable cause to a judge on a case-by-case basis.

Mainway wasn't the only extraordinary tool in the government's intelligence arsenal. According to Edward Snowden and other whistleblowers, the events of 9/11 triggered numerous efforts to mine assumedly protected communications. Among these is a project that resembled Mainway but focused on Internet-based chatter, primarily e-mails, where at least one party to the communication was outside the U.S., or "for which no communicant was known to be a citizen of the United States."

Neither Mainway not its e-mail twin warehoused content. Other programs did. Secret government documents published in 2013 by the *Washington Post* revealed NSA's "PRISM" initiative, which downloaded e-mail, text, voice and data messages directly from the computer servers of Microsoft, Yahoo, Google, Facebook, Pal Talk, AOL, Skype, YouTube, and Apple. Querying this database required that FBI analysts demonstrate "fifty-one percent confidence" that their targets were foreign nationals located overseas. Another initiative, "NUCLEON," apparently did the same for telephone calls, spurring

complaints that it clashed in spirit if not substance with laws requiring that warrantless interceptions have the consent of at least one party to a communication.

Here it's probably useful to bring in an example. Your author spent most of his career chasing after gun traffickers. One source of information was a database that stored the sales history of guns recovered by police. Scanning these entries identified possible illegal resellers, and surveillance occasionally led to catching them in the act. Just like in drug and other conventional crimes, their arrest was nearly always "after the fact." That was thought perfectly acceptable.

But terrorism is different in two important ways. Its potentially catastrophic consequences scream that there be no "first time." Terrorist organizations also leave few clues and are notoriously difficult to penetrate. So it's hardly surprising that investigators are greedy for anything they can get. Maybe – just maybe – that additional straw will help recognize a pending threat. Therein lies the rub, as gathering terrorism intelligence is bound by the same legal strictures that apply to ordinary crime. That's a source of deep frustration for intelligence executives. One potential adjustment might be to lower the evidentiary standard for interceptions from probable cause to, say, "reasonable suspicion," the criterion for stop-and-frisk.

And there's a new complication. Message encryption has become commonplace in the Internet. Until recently device makers and service providers held on to decryption keys and made them available on presentation of a court order. New hardware and software designs, though, prevent decoding without a user password. At a recent gathering of cybersecurity professionals, Manhattan D.A. Cyrus Vance complained that Apple's implementation of these protocols in their new iphones frustrated more than one-hundred interceptions sought by his office this past year:

> Last fall, a decision by a single company changed the way those of us in law enforcement work to keep the public safe and bring justice to victims and their families. We risk losing crucial evidence in serious cases if the contents of passcode protected smartphones remain immune to a warrant.

Warning that ISIS was already using encryption technology, another speaker, FBI Director James B. Comey, delivered an even gloomier assessment. Privacy advocates, device makers and even the *New York Times* reporter who wrote about the session reacted skeptically. After all, French detectives found the organizer of the recent Paris attack thanks to an (unencrypted) message left on a female jihadist's discarded cell phone. Of course, in the brave new world of perfect anonymity, all that the bad guys (and gals) will need to prevent future slip-ups is readily available at the Apple store.