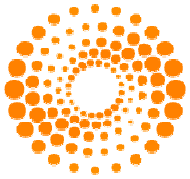

Collateral damage of our surveillance state

By Julian Sanchez - NOVEMBER 15, 2012

As the surreal sex scandal that forced CIA Director David Petraeus' resignation reveals another prominent general's "flirtatious" emails, the serious scandal here may well be the breadth of the FBI's power to launch fishing expeditions through Americans' most intimate communications.

This investigation began in May, as we now know from copious FBI leaks, with a series of rude anonymous emails to Tampa socialite Jill Kelley. The messages criticized her cozy relationships with military officers at a local base, where she volunteers as a social planner. Although the e-mails have been described as "cat-fight stuff" rather than threats, a friend of Kelley's at the FBI, Frederick W. Humphries II- who had sent Kelley shirtless photos and was ultimately barred from the case by superiors worried he had become "obsessed" - urged the bureau to investigate.

The FBI obliged - apparently obtaining subpoenas for Internet Protocol logs, which allowed them to connect the sender's anonymous Google Mail account to others accessed from the same computers, accounts that belonged to Petraeus biographer Paula Broadwell. The bureau could then subpoena guest records from hotels, tracking the WiFi networks, and confirm that they matched Broadwell's travel history. None of this would have required judicial approval - let alone a Fourth Amendment search warrant based on probable cause.

While we don't know the investigators' other methods, the FBI has an impressive arsenal of tools to track Broadwell's digital footprints — all without a warrant. On a mere showing of "relevance," they can obtain a court order for cell phone location records, providing a detailed history of her movements, as well as all people she called. Little wonder that law enforcement requests to cell providers have exploded — with a staggering 1.3 million demands for user data just last year, according to major carriers.

An order under this same weak standard could reveal all her e-mail correspondents and Web surfing activity. With the rapid decline of data storage costs, an ever larger treasure trove is routinely retained for ever longer time periods by phone and Internet companies.

Had the FBI chosen to pursue this investigation as a counterintelligence inquiry rather than a cyberstalking case, much of that data could have been obtained without even a subpoena. National Security Letters, secret tools for obtaining sensitive financial and telecommunications records, require only the say-so of an FBI field office chief.

Though President Barack Obama once pledged to end the use of these letters to siphon up sensitive information about innocent Americans without judicial oversight, they have been issued in unprecedented numbers during his administration. More than 14,000 Americans were affected just during his first year in office. Internal audits have revealed "widespread and serious misuse" of this authority, yet Congress has not acted to restrict it.

Unlike conventional wiretaps or physical searches, many of these methods can be used without the targets ever being told - regardless of whether evidence of a crime is found. Americans remain largely in the dark about how widely or frequently they are used.

While federal courts must report on the number of wiretap orders issued each year, there's no similar requirement for most other forms of digital surveillance. Where reporting requirements exist, they are routinely flouted by the Justice Department, which sometimes waits years to provide Congress with mandatory reports.

With Broadwell identified as the anonymous emailer - explaining her surprising knowledge of Petraeus' social calendar - one might have expected the investigation to be closed. Yet, though Justice Department attorneys seem to have ultimately determined that Broadwell committed no crime, the bureau didn't stop.

Rather than questioning Broadwell or Petraeus at this point, the FBI sought access to the contents of her email accounts and uncovered thousands of intimate messages, largely irrelevant to the purpose of this inquiry, that revealed an illicit affair between the married CIA director and his Boswell.

Humphries—whose "worldview," according to FBI sources, led him to fear a pre-election coverup to protect Obama — then re-emerged as a "whistleblower" and leaked the sordid investigation details to House Majority Leader Eric Cantor (R-Va.).

At some point—it's still unclear how— the FBI also obtained "flirtatious" e-mails between Kelley and General John Allen, which were later disclosed to the military. These, too, appear to have been non-criminal, however allegedly "inappropriate."

Petraeus seems to have behaved stupidly on every possible level. But this chain of events should still be profoundly disturbing to anyone familiar with the FBI's long and ugly history of using targeted leaks from electronic surveillance in an attempt to destroy political adversaries. Perhaps the most notorious example remains J. Edgar Hoover's attempt to drive Martin Luther King Jr. to suicide, using tapes of his extramarital liaisons, so that he could be replaced by what the bureau euphemistically called "the right kind of Negro leader."

This incredible record of abuse was uncovered only years - and in some cases decades - after the fact, following an intensive Senate investigation.

Concerns about the bureau's power should only be more pressing in an age where cheap data storage and a fear-fueled blank check for intelligence agencies combine to give the government a detailed portrait of our virtual lives that would have staggered even Hoover. The demand for access to Broadwell's emails was just one of 6,321 requests for user data—covering 16,281 user accounts—fielded by Google alone in the past six months. Those requests may expose not just current correspondence but years' worth of e-mails and chats, as they did with Broadwell.

Though technology continues to advance at a breathtaking pace, the federal digital privacy rules were written in 1986 - when Atari was king. Investigators often don't even

need a Fourth Amendment search warrant to go fishing through your emails. For messages on a server longer than six months, a prosecutor's subpoena or a court order based on that same weak showing of "relevance" to an investigation can do the trick.

Even if you don't use Google and aren't currently under suspicion, there's no guarantee that some of your communications aren't sitting in a database awaiting a curious agent's query. Under the 2008 amendments to the Federal Intelligence Security Act (FISA), the National Security Agency now has broad power to vacuum up international communications without the need for individual warrants - power that has predictably resulted in "over-collection" of even domestic emails on a massive scale.

The Senate Intelligence Committee has robust oversight powers under the FISA ruling, but the NSA has repeatedly refused to give even a rough estimate of how many American citizens' communications are now stored in their vast database.

You don't have to sympathize with Petraeus to wonder whether any prominent national figure who runs afoul of the FBI—or another influential official, for that matter—could survive the kind of humiliating exposure our modern surveillance state makes commonplace. If everyone has a skeleton or two in the closet, information is the power to decide whose careers will survive.

We have unwittingly constructed a legal and technological architecture that brings point-and-click simplicity to the politics of personal destruction. The Petraeus affair has, for a moment, exposed that invisible scaffolding - and provided a rare opportunity to revisit outdated laws and reconsider the expanded surveillance powers doled out over the past panicked decade.

Congress should seize the opportunity to re-examine and revise these myriad surveillance techniques and update the oversight process. At a bare minimum, lawmakers should drag the 1986 Electronic Communications Privacy Act into the 21st century - requiring a warrant for all law-enforcement access to communications contents and tightening the rules for access to sensitive information, such as cellphone location data. They should also demand more answers about the use of programmatic surveillance under the FISA Amendments Act—and refuse to reauthorize the law until they get them.

If we don't take steps to rein in the burgeoning surveillance state now, there's no guarantee we'll even be aware of the ways in which control is exercised through this information architecture. We will all remain exposed - but the extent of our exposure, and the potential damage done to democracy, is likely to remain invisible.