THE HUFFINGTON POST

A Fourth Amendment for the 21st Century

By: Julian Sanchez – November 28th, 2012

The resignation of CIA Director David Petraeus has thrown a spotlight on the FBI's sweeping power to sift through the most intimate details of our digital lives -- often with little or no judicial supervision. On Thursday, the Senate Judiciary Committee will consider legislation that would modestly improve the outdated law governing police access to our emails and other electronic records -- yet even this first step toward meaningful online privacy reform is encountering strong resistance.

Most Americans know that the Fourth Amendment protects us against "unreasonable searches and seizures" -- requiring a judge to issue a specific warrant based on "probable cause" before government agents can search our homes, open our mail or wiretap our phones. Most probably assume that the same protection applies to their email conversations and other sensitive information stored in "the cloud," such as documents, photos, chat logs and records of their Web browsing habits. Unfortunately, under the misnamed Electronic Communications Privacy Act of 1986, that's not true.

Back when ECPA was written, "going online" meant dialing up services that charged astronomical per-minute access fees, and the digital storage capacity found on an ordinary smartphone would have cost roughly a million dollars. Naturally, it was assumed that email would almost always be downloaded to the user's computer, where it would enjoy the traditional protections of the Fourth Amendment against physical search. So the law required a traditional warrant to access unopened email in "temporary" storage. But on the government's interpretation, opened emails, other remotely stored files and unopened emails older than six months, are accessible with a court order based on a claim of mere "relevance" to an investigation, and sometimes even a mere subpoena. A few courts have required warrants for email contents, but sensitive logs that can reveal online reading habits, and even real-world movements, remain unprotected.

Unlike phone wiretaps, most forms of digital surveillance don't have to be publicly reported, which means we have no clear idea how often these tools are used -- but what we do know suggests they're increasingly popular. In just the past six months, Google

alone fielded 7,969 requests for user data from the U.S. government, covering 16,281 accounts -- and that doesn't include requests under secret intelligence authorities. Owing in part to the increasing popularity of location tracking using cell phones, mobile providers dealt with a staggering 1.3 million requests in the past year. In many instances, the targets never have to be informed they've been spied upon.

Legislation to amend ECPA introduced by Sen. Patrick Leahy (D-Vt.) would finally require a search warrant *whenever* the government wants to read the contents of emails and other private documents. Law enforcement agencies have been pushing back against this common-sense requirement, often citing dramatic scenarios involving kidnappings or death threats. Yet the law already contains a clear exception to the warrant requirement for such emergency situations, which nobody has proposed eliminating. Meanwhile, a variety of government agencies have pushed for their own exceptions for regulatory inquiries.

Leahy's proposal is a fine start -- but even better would be the heightened standards that apply to phone wiretaps. In the 1967 case *Berger v. New York*, the Supreme Court suggested that because wiretaps are generally secret (unlike searches of homes) and capture many innocent conversations, extra protections are necessary. Federal law requires law enforcement to show they can't get the evidence they need by less intrusive methods, and to avoid recording irrelevant material. The same arguments apply to our electronic accounts, which often host years of intimate conversations -- like those between Petraeus and his mistress, which the FBI unearthed as part of an investigation into supposed "cyberstalking."

Congress and the courts should also heed Supreme Court Justice Sonia Sotomayor's recent suggestion that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." Under current Supreme Court doctrine, such information is generally assumed to lack constitutional protection, because individuals "assume the risk" that companies will reveal it -- even if they are legally obligated not to, and even when the government compels them to do so. "This approach," Sotomayor observed, "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks," ranging from their physical location to their reading habits and political or religious associations.

This doesn't necessarily mean *all* digital records should require a full-blown search warrant, heightened judicial scrutiny should surely be required in certain cases. Using subpoenas to strip away a speaker's anonymity, as the FBI did in the Petraeus investigation, implicates our long-established First Amendment right to anonymous speech. Similarly, e-mail logs can reveal membership in controversial groups, which the Supreme Court has held can chill our right to free association.

Given the resistance we've seen even to limited reform efforts, achieving these changes will no doubt require a long and difficult fight. Without them, however, our constitutional privacy guarantees will be limited to the world of ink and parchment, even as our private lives inhabit a world of bits and pixels.