THE NEW YORKER

Wiretapping the Web

By: Tim Wu – May 14, 2013

The federal power to wiretap, a central issue during the Bush years, has made a comeback. The White House seems ready to endorse an expansion of wiretapping laws to give the federal government greater power to demand access to Web communications like Facebook chats. Meanwhile, the Associated Press just revealed that the Justice Department seized, without a warrant, two months' worth of its reporters' telephone records.

Critics are, unsurprisingly, up in arms about both matters. House Republicans, recently born again as staunch civil-rights defenders, are depicting the Obama Administration as, in the words of Zeke Miller and Michael Crowley, "a Big Brother–style tyrant in charge of a power-abusing surveillance state." Techies, for their part, simply hate the idea of Web-tapping. Julian Sanchez, for *Wired*, writes, "The Obama administration needs to dump this ill-conceived scheme on the trash heap where it belongs." But the issue, once you get into it, is actually rather complicated.

Wiretapping the Web provokes a visceral reaction for more than one reason. First and foremost, like any electronic surveillance, it's a massive invasion of privacy by the world's most powerful government. As Justice Louis Brandeis wrote, in 1928, "As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wiretapping." A wiretapping law can incidentally create a terrible innovation policy. "Build your system this way" has rarely yielded good results, and never when Congress is involved. Finally, some technologists believe that a Web-tapping law will create new Internet security risks, because it would force firms to build backdoors into their systems, which malicious hackers could then exploit.

Nonetheless, the F.B.I. and other law-enforcement agencies present a persuasive argument for increased powers (in particular, increased sanctions for Internet firms who do not comply with wiretap orders). While it is easy to dislike government surveillance in the abstract, the case for tapping becomes extremely strong when facing the actual investigation of a serious crime, like a murder, a planned terrorist attack, or a powerful criminal organization (think "The Wire"). That need to gain evidence in individual cases has led us roughly to where we are (at least for criminal matters—anti-terrorism is a whole different story). Wiretapping is permitted, but usually limited to serious crimes, and only allowed when subject to appropriate protections and oversight, depending on the intrusiveness of the tap. A comprehensive set of laws and regulations governs when the F.B.I. can wiretap telephones, and they are mostly reasonable.

If wiretapping is strongly justified in individual cases, then, argues the F.B.I, as communication technologies change, so, too, must those laws and regulations. Hence, as new technologies emerge, or as existing ones become harder to tap, the wiretapping

power needs to be adjusted to maintain roughly the same balance. This essential concept of balance is what's behind the F.B.I's argument that it needs more power lest its ability to wiretap "go dark."

But there are two essential conditions for this balance argument to make any sense. First, if it is to have more powers, the Justice Department should also agree that Web communications and stored records are generally subject to the strict standards demanded by the Fourth Amendment (as are the content of telephone calls). As it stands, the Justice Department has been evasive on this point. It has argued against the need for warrants for things like e-mail messages, and often appears to believe that a mere subpoena (a document issued by a prosecutor) should be sufficient to obtain any record stored on the Web or otherwise.

The F.B.I. and Justice Department cannot credibly declare that they need to restore balance with more warrant power, and at the same time campaign against the need for warrants in the first place, and abuse their subpoena powers. If the argument for preserving a balance between security and privacy compels a stronger wiretap power, it must also means a broader statutory warrant requirement, one that covers most of what we do on the Web and covers most records. Otherwise, the balance argument works against the Justice Department.

Consider the seizure of the A.P.'s calling records, which was accomplished not with a warrant but with subpoenas sent to the telephone companies. The legal fiction is that the reporters, when making phone calls, voluntary handed over their calling records to the phone companies; ergo the seizure of those records has nothing to do with the Constitution.

Relying on that fiction (which, unfortunately, was created by the Supreme Court in 1979), the Justice Department broadly believes that stuff stored on the Web has also been handed over to a third party and therefore merits very limited protection. But that old legal fiction—which, in the words of Wayne LaFave, a law professor emeritus at the University of Illinois, "makes a mockery of the Fourth Amendment"—grows more indefensible every day, and becomes further at odds with personal and technological reality. Courts, especially the Sixth Circuit Court of Appeals, are ahead of the Justice Department in their recognition that the data we all store on the Internet nowadays has become core to American privacy.

What we store online is really more akin to the old home filing cabinet than the telephone. Yes, the telephone conversation may be intimate, but it at least has the feeling of an external projection: one reaches out to make calls. Records, writings, and personal correspondence are often more sensitive, whether they're stored at home or online. We often do as much if not more on the Web than we did on the telephone—writing personal thoughts, or dealing with matters that were previously handled in person and in private, like renting videos or researching embarrassing medical problems. The expectation of privacy in one's online records is obvious to anyone who lives in this century.

The second condition needed for the F.B.I.'s balance argument to work is the limitation of highly intrusive monitoring to cases of serious crimes with clear victims. Federal law is chock-full of offenses, which make everyone a potential criminal and, in turn, at least potentially subject to tapping. This is another problem with the A.P. investigation: while

leaks of classified information can be important, their investigation cannot plausibly justify the mass seizure of the calling records of a major news organization.

The whole idea of balance in this area must also be put in the context of a growing "surveillance state," as Hendrik Hertzberg calls it. As intense as F.B.I. surveillance can be, at least the F.B.I. regards the Constitution as a serious constraint, unlike the National Security Agency, which has repeatedly spied on Americans without a warrant, reaching its maximum level of abuse during the Bush years. That doesn't mean we should be thankful, exactly, for F.B.I. monitoring, but let's just say things could be worse.

The bottom line is that we should demand the following: no increase in the power to wiretap without a statutory recognition of a broader warrant requirement that reflects the reality of the privacy interest in stuff stored on the Web. And we must demand some proportionality: that the most intrusive methods of federal surveillance be reserved for the most serious crimes. Finally, and ideally, we'd take a harder look at what actually constitutes a federal crime, but that's a whole different story.

Tim Wu, @superwuster on Twitter, is a professor at Columbia Law School and the author of "The Master Switch."