Not that hard for authorities to get to your email

RICHARD LARDNER - Associated Press - Associated Press

Your emails are not nearly as private as you think.

The downfall of CIA Director David Petraeus demonstrates how easy it is for federal law enforcement agents to examine emails and computer records if they believe a crime was committed. With subpoenas and warrants, the FBI and other investigating agencies routinely gain access to electronic inboxes and information about email accounts offered by Google, Yahoo and other Internet providers.

"The government can't just wander through your emails just because they'd like to know what you're thinking or doing," said Stewart Baker, a former assistant secretary at the Homeland Security Department who's now in private law practice. "But if the government is investigating a crime, it has a lot of authority to review people's emails."

Under the 1986 Electronic Communications Privacy Act, federal authorities need only a subpoena approved by a federal prosecutor — not a judge — to obtain electronic messages that are six months old or older. To get more recent communications, a warrant from a judge is required. This is a higher standard that requires proof of probable cause that a crime is being committed.

Public interest groups are pressing Congress for the law to be updated because it was written a quarter-century ago, when most emails were deleted after a few months because the cost of storing them indefinitely was prohibitive. Now, "cloud computing" services provide huge amounts of inexpensive storage capacity. Other technological advances, such as mobile phones, have dramatically increased the amount of communications that are kept in electronic warehouses and can be reviewed by law enforcement authorities carrying a subpoena.

"Technology has evolved in a way that makes the content of more communications available to law enforcement without judicial authorization, and at a very low level of suspicion," said Greg Nojeim, a senior counsel at the Center for Democracy & Technology.

The chairman of the Senate Judiciary Committee, Patrick Leahy, has proposed changing the law to require a warrant for all Internet communications regardless of their age. But law enforcement officials have resisted because they said it would undercut their ability to catch criminals.

A subpoena is usually sufficient to require Internet companies to reveal names and any other information that they have that would identify the owner of a particular email account. Google, which operates the widely used Gmail service, complied with more than 90 percent of the nearly 12,300 requests it received in 2011 from the U.S. government for data about its users, according to figures from the company.

Even if a Gmail account is created with a fictitious name, there are other ways to track down the user. Logs of when messages are sent reveal the Internet address the user used to log onto the account. Matching times and dates with locations allow investigators to piece together the chain.

A Gmail account figured prominently in the FBI investigation that led to Petraeus' stunning resignation last week as the nation's spy chief. Petraeus, a retired Army general, stepped down after he confessed to an extramarital affair with Paula Broadwell, an Army Reserve officer and his biographer.

The inquiry began earlier this year after Jill Kelley, a Florida woman who was friends with Petraeus and his wife, Holly, began receiving harassing emails. Kelley is a socialite in Tampa, Fla., where the military's Central Command and Special Operations Command are located.

Petraeus served as commander at Central Command from 2008 to 2010.

FBI agents eventually determined that the email trail led to Broadwell, according to two federal law enforcement officials, who spoke on condition of anonymity because the sources were not authorized to speak about the matter on the record. As they looked further, the FBI agents came across a private Gmail account that used an alias name. On further investigation, the account turned out to belong to Petraeus.

The contents of several of the exchanges between Petraeus and Broadwell suggested they were having an affair, according to the officials. Investigators determined that no security breach had occurred, but continued their investigation into whether Petraeus had any role in the harassing emails that Broadwell had sent to Kelley, which was a criminal investigation.

Petraeus and Broadwell apparently used a trick, known to terrorists and teenagers alike, to conceal their email traffic.

One of the law enforcement officials said they did not transmit all of their communications as emails from one's inbox to the other's inbox. Rather, they composed some emails in a Gmail account and instead of transmitting them, left them in a draft folder or in an electronic "dropbox." Then the other person could log onto the same account and read the draft emails there. This avoids creating an email trail, which is easier to trace. It's a technique that al-Qaida terrorists began using several years ago and teenagers in many countries have since adopted.

___

Associated Press writer Pete Yost contributed to this report.

Source URL (retrieved on *12/12/2013 - 8:06pm*):
http://www.ecnmag.com/news/2012/11/not-hard-authorities-get-your-email