THE WALL STREET JOURNAL.
U.S. Edition

WHAT THEY KNOW | October 9, 2011, 10:31 p.m. ET

Secret Orders Target Email

WikiLeaks Backer's Information Sought

By JULIA ANGWIN

The U.S. government has obtained a controversial type of secret court order to force Google Inc. and small Internet provider Sonic.net Inc. to turn over information from the email accounts of WikiLeaks volunteer Jacob Appelbaum, according to documents reviewed by The Wall Street Journal.

Sonic said it fought the government's order and lost, and was forced to turn over information. Challenging the order was "rather expensive, but we felt it was the right thing to do," said Sonic's chief executive, Dane Jasper. The government's request included the email addresses of people Mr. Appelbaum corresponded with the past two years, but not the full emails.

Both Google and Sonic pressed for the right to inform Mr. Appelbaum of the secret court orders, according to people familiar with the investigation. Google declined to comment. Mr. Appelbaum, 28 years old, hasn't been charged with wrongdoing.

The court clashes in the WikiLeaks case provide a rare public window into the growing debate over a federal law that lets the government secretly obtain information from people's email and cellphones without a search warrant. Several court decisions have questioned whether the law, the Electronic Communications Privacy Act, violates the U.S. Constitution's Fourth Amendment protections against unreasonable searches and seizures.

WikiLeaks is a publisher of documents that people can submit anonymously. After WikiLeaks released a trove of classified government diplomatic cables last year, U.S. Attorney General Eric Holder said the U.S. was pursuing an "active criminal investigation" of WikiLeaks.

Passed in 1986, the Electronic Communications Privacy Act is older than the World Wide Web, which was dreamed up in 1989. A coalition of technology companies—including Google, Microsoft Corp. and AT&T Corp. —is lobbying Congress to update the law to require search warrants in more digital investigations.

The law was designed to give the same protections to electronic communications that were already in place for phone calls and regular mail. But it didn't envision a time when cellphones transmitted locations and people stored important documents on remote services, such as Gmail, rather than on their own computers.

Law enforcement uses the law to obtain some emails, cellphone-location records and other digital documents without getting a search warrant or showing probable cause that a crime has been committed. Instead the law sets a lower bar: The government must show only "reasonable grounds" that the records would be "relevant and material" to an investigation.

As a result, it can be easier for law-enforcement officers to see a person's email information than it is to see their postal mail.

Another significant difference: A person whose email is inspected this way often never knows a search was conducted. That's because court orders under the 1986 law are almost always sealed, and the Internet provider is generally prohibited from notifying the customer whose data is searched. By contrast, search warrants are generally delivered to people whose property is being searched.

The secrecy makes it difficult to determine how often such court orders are used. Anecdotal data suggest that digital searches are becoming common.

In 2009, Google began disclosing the volume of requests for user data it received from the U.S. government. In the six months ending Dec. 31, Google said it received 4,601 requests and complied with 94% of them. The data include all types of requests, including search warrants, subpoenas and requests under the 1986 law.

At a Senate hearing in April on whether the 1986 law needs updating, Associate Deputy Attorney General James A. Baker cautioned Congress "that raising the standard for obtaining information under ECPA may substantially slow criminal and national security investigations."

In May, the ECPA's author, U.S. Sen. Patrick Leahy (D., Vt.), said the original law is "significantly outdated and outpaced by rapid changes in technology." He introduced a bill adopting many of the recommendations of the technology coalition lobbying for changes to the law.

Some federal courts have questioned the law's constitutionality. In a landmark case in December, the U.S. Court of Appeals for the Sixth Circuit ruled that the government violated the Fourth Amendment when it obtained 27,000 emails without a search warrant.

"The police may not storm the post office and intercept a letter, and they are likewise forbidden from using the phone system to make a clandestine recording of a telephone call—unless they get a warrant," Judge Danny Boggs wrote in the 98-page opinion. "It only stands to reason that, if government agents compel an [Internet service provider] to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search."

In August, the U.S. District Court of the Eastern District of New York over-ruled a government request to obtain cellphone location records without a warrant, calling it "Orwellian." Judge Nicholas Garaufis wrote: "It is time that the courts begin to address whether revolutionary changes in technology require changes to existing Fourth Amendment doctrine." The government has appealed.

The WikiLeaks case became a test bed for the law's interpretation earlier this year when Twitter fought a court order to turn over records from the accounts of WikiLeaks supporters including Mr. Appelbaum.

Mr. Applebaum is a developer for the Tor Project Inc., a Walpole, Mass., nonprofit that provides free tools that help people maintain their anonymity online. Tor's tools are often used by people living in countries where Internet traffic is monitored by the government. Tor obtains some of its funding from the U.S. government.

Mr. Appelbaum has also volunteered for WikiLeaks, which recommends people use Tor's tools to protect their identities when submitting documents to its website. In April 2010, Mr. Appelbaum's involvement in WikiLeaks was inadvertently disclosed publicly in a blog post on the website of the Committee to Protect Journalists. The reporter, Danny O'Brien, said Mr. Appelbaum had thought he was speaking anonymously. Mr. O'Brien said he later offered to remove Mr. Appelbaum's name from the post.

After the blog post appeared, Mr. Appelbaum became a public advocate for WikiLeaks. In June, he gave a speech at a Northern California technology camp where he called WikiLeaks founder Julian Assange one of the "biggest inspirations in my life."

On Dec. 14, the U.S. Department of Justice obtained a court order for information from the Twitter account of people including Mr. Appelbaum and WikiLeaks supporters Birgitta Jonsdottir, a member of the Icelandic parliament, and Rop Gonggrijp, a Dutch computer programmer. Neither has been charged with wrongdoing.

The order sought the "Internet protocol," or IP, addresses of the devices from which people logged into their accounts. An IP address is a unique number assigned to a device connected to the Internet.

The order also sought the email addresses of the people with whom those accounts communicated. The order was filed under seal, but Twitter successfully won from the court the right to notify the subscribers whose information was sought.

On Jan. 26, attorneys for Mr. Appelbaum, Mr. Gonggrijp and Ms. Jonsdottir jointly filed a motion to vacate the court order. They argued, among other things, that because IP addresses can be used to locate a person in "specific geographic destinations," it constituted a search under the Fourth Amendment and thus required a warrant.

The government argued that IP addresses don't reveal precise location and are more akin to phone numbers. At a Feb. 15 hearing, Assistant U.S. Attorney John S. Davis said, "this is a standard… investigative measure that is used in criminal investigations every day of the year all over this country."

On March 11, U.S. Magistrate Judge Theresa Carroll Buchanan denied the WikiLeaks supporters' motion. They have appealed.

Twitter hasn't turned over information from the accounts of Mr. Appelbaum, Ms. Jonsdottir and Mr. Gonggrijp, according to people familiar with the investigation.

The court orders reviewed by the Journal seek the same type of information that Twitter was asked to turn over. The secret Google order is dated Jan. 4 and directs the search giant to hand over the IP address from which Mr. Appelbaum logged into his gmail.com account and the email and IP addresses of the users with whom he communicated dating back to Nov. 1, 2009. It isn't clear whether Google fought the order or turned over documents.

The secret Sonic order is dated April 15 and directs Sonic to turn over the same type of information from Mr. Appelbaum's email account dating back to Nov. 1, 2009.

On Aug. 31, the court agreed to lift the seal on the Sonic order to provide Mr. Appelbaum a copy of it. Sonic Chief Executive Mr. Jasper said the company also sought to unseal the rest of its legal filings but that request "came back virtually entirely denied."