Written by **Raven Clabough** on January 12, 2011

Privacy Laws at Risk for Internet Users

Telecommunications and Internet companies are increasingly finding themselves in uncomfortable positions, caught between privacy laws that protect their consumers and law enforcement efforts that necessitate privacy invasion. As Internet and telecommunications services grow in popularity, law enforcement agencies have utilized them as a means to find information about individuals that would otherwise be difficult to obtain.

However, there are specific laws, enacted in 1986, that govern communication privacy. The 1986 Electronic Communications Privacy Act established rules for information access, but they are contingent upon the type of information sought and how old it is. Unfortunately, views of the sanctity of those laws are beginning to evolve.

The *New York Times* reports:

> Many Internet companies and consumer advocates say the main law governing communication privacy — enacted in 1986, before cell phone and e-mail use was widespread, and before social networking was even conceived — is outdated, affording more protection to letters in a file cabinet than e-mail on a server.
>
> They acknowledge that access to information is important for fighting crime and terrorism, but say they are dealing with a patchwork of confusing standards that have been interpreted inconsistently by the courts, creating uncertainty.

Google and Verizon are among a number of companies that have been flooded by requests for information. According to Google, the requests "are valid and the information needed is for legitimate criminal investigations." Google's privacy policy, similar to that of Facebook, indicates that it will comply "with valid legal processes seeking account information." Twitter's policy, however, is different in that they "notify users of requests for their information prior to disclosure unless we are prohibited from doing so by statute or court order."

Susan Freiwald, professor at the University of San Francisco School of Law and an expert in electronic surveillance law, indicated,

> Some people think Congress did a pretty good job in 1986 seeing the future, but that was before the World Wide Web. The law can't be expected to keep up without amendments.

She added that the government does not typically notify people that their online information is being accessed, nor does it feel the need to prove probable cause before doing so. What's worse is that even when the government violates privacy laws, the accessed information is often still permitted as

evidence in trial.

Law enforcement agents assert that they require access to important information. For example, the U.S. Justice Department made the argument in court last year that cell phone users gave up their expectation of privacy when they voluntarily gave that information to carriers. Later in the year, a federal court argued in Colorado that it was permissible for federal agents to gain access to emails without a warrant. The *New York Times* adds, "And federal law enforcement officials, citing technology advances, plan to ask for new regulations that would smooth their ability to perform legal wiretaps of various Internet communications."

Ryan Calo, director of the consumer privacy project at the Center for Internet & Society at Stanford Law school, explains:

> When your job is to protect us by fighting and prosecuting crime, you want every tool available. No one thinks D.O.J. and other investigative agencies are sitting there twisting their mustache trying to violate civil liberties. They're trying to do their job.

Internet companies have shown some discomfort in violating privacy laws, asserting that email should be treated in the same way as a home. Some companies are asking law enforcement agencies to secure search warrants from a judge rather than what is called a simple subpoena — one obtained from a prosecutor.

Likewise, as information requests have increased, Internet companies have responded in a variety of ways. Again, the *New York Times*:

> In the Wikileaks case, Twitter took the unusual step of seeking to unseal the court order so it could follow its own internal policies and notify its customers, the Wikileaks members, that the government wanted information about them. Privacy experts praised Twitter for this.

Twitter informed its consumers, who were part of the government investigation for Wikileaks, that it would disclose individual information after 10 days unless the individuals being investigated were willing to go to court to block the release of their data. Twitter's actions taught a valuable lesson about the limits of the law.

As tensions continue to grow between Internet companies and law enforcement agencies, it seems likely that further regulations will be issued in order to address the disputes.