In my first post on the legal issues, I discussed the public's expectation that their social networking information is private. Here, I will move on to the challenges presented by the lack of legislative or judicial law pertaining to use of social networking information in civil and criminal proceedings. (See Social Networking - Legal and Ethical Issues for Lawyers and Investigators).

There are two primary sources of legal authority to rely on in analyzing the protection of social networking information. The first is the 4th Amendment rights against unreasonable searched and seizures, premised on the doctrine of a person's reasonable expectation of privacy. The second arises from the Electronic Communications Discovery Act of 1986. ECPA was enacted to extend government restrictions on wire taps from telephone calls to include the transmission of electronic data (email), although the restrictions were never extended to stored electronic data that had not yet been read by the recipient. The standard to obtain a warrant under the 4th amendment is probable cause, but under ECPA, the standard is much lower. Originally, the prosecutor need only state that the information sought was "relevant" to a civil or criminal matter without stating any facts to support that claim. Later, the standard was raised to require at least a minimal factual basis for relevance, but is still substantially lower than probable cause.

The protections afforded by ECPA were weakened by the U.S. Patriot Act. Among other things, the Act increased the ability of law enforcement agencies to search telephone, e-mail communications, medical, financial, and other records, eased restrictions on foreign intelligence gathering within the United States and the expanded use of National Security Letters which allows the FBI to search telephone, e-mail, and financial records without a court order. Prosecutors and attorneys have primarily relied on ECPA standards to seek social networking information because of the lower standard to show cause.

At this point, two distinctions should be made. First, it is easier to obtain a warrant to search social networking sites in a criminal investigation than it is to obtain a subpoena in a civil case due to the greater importance of prosecuting crimes over seeking civil remedies. That being said, even in criminal cases, only the prosecution can obtain a warrant. And while the prosecution has the duty to turn over any evidence they obtain to the defense attorney, if they believe they will find exculpatory evidence, it was asserted at the conference that they will simply then not seek to obtain the evidence.

Second, as I discussed previously, there is a difference between "transactional information" and "content." While transactional information generally only requires a subpoena, "content" requires obtaining a warrant, since content carries a higher expectation of privacy. However, as we have seen, the 4th amendment right that protects against searches where there is a reasonable expectation of privacy does not necessarily apply in the electronic information landscape.

So the question remains: what body of law applies, and how does a law intended to regulate telephone and email interception apply to the acquisition of social networking information? The world of online interaction and social membership sites creates a new environment which old legal doctrines,even those directed at email, do not address. This

is true not only of the legal standards required to obtain the information, but also of the unauthorized conduct to do so (to be discussed further in Part 3). For example, computers forensics provides a method to obtain information that was intentionally deleted from a hard drive. Web analytics and other tools aggregate data across many networks that is easily accessible. And then, when all else fails, there are always deceptive practices. The truth is we reveal personal information to an almost endless audience when we participate online through the digital footprint we leave. Neither legislative or judicial decisions have addressed the standards required to obtain admissible evidence in these environments.

As an example of how legal opinions are emerging, there is an excellent discussion of a recent trial court decision in a podcast entitled The Fourth Amendment and Email. Here, the judge ruled that no one can have a reasonable expectation that their emails are private due to the digital footprint they create. Rulings like this must, and will, continue and go up on appeal to begin to create judicial precedent on these issues.

As this is being written, the House Judiciary Committee is considering HR3845, which would amend the Patriot Act. For an up-to-date review of that process, visit the Electronic Frontier Foundation website, or follow them on Twitter @eff. Lawyers and governmental agencies across the country are using social networks as a source of information on a daily basis, as a matter of course. Given that the legal parameters of such use are something akin in justice in the Wild West, this area of law needs to be defined and regulated. Now.