The Downfall of Privacy

"Privacy" has always been a somewhat ephemeral concept. We do not protect privacy as such in the Constitution of the United States. However, the courts see privacy as a penumbra of several constitutional protections. What the courts have done is to create a metaphor between privacy and a solar eclipse. During a total solar eclipse, there is the appearance of a ring of fire seen around the moon. That ring is something that scientists call the penumbra. Therefore, while privacy is not explicitly mentioned in the Constitution, we can see it as a ring around the Bill of Rights.

Putting aside the question as to whether the courts have gone too far in finding a constitutional right to privacy, most Americans believe that they are entitled to that protection. Perhaps the most alarming case that I have seen in my career on the subject was when a healthcare worker, employed for some years, was asked to sign a form waiving her rights to privacy concerning her credit history. The employer wanted to snoop into all of its employees' credit history, regardless of whether they worked in the financial sector of the company. One brave woman refused and was fired. The United States Court of Appeals for the Third Circuit affirmed that the woman had no right to object to her employer's demand and she could be fired for refusing to provide the waiver of her confidential financial information.

Privacy is not a static concept and has morphed into a variety of other real-life situations. Most Americans have come to accept hacking into their computers as part of modern life. "Hacking" is stealing, plain and simple. The hacker is a thief who can be criminally prosecuted under federal and state law.

What happens when someone receives stolen goods? If Mary J. Citizen has reason to know she is receiving stolen goods, she will be prosecuted in every jurisdiction in the United States.

What does this mean for newspapers, political operatives and others who receive stolen emails and other information from computers or servers? Is WikiLeaks committing a crime if it hacks or receives information it has good reason to know has been hacked from computers? The answer is, without question, "yes." How about the newspapers that sometimes receive the information that has been hacked and publish it? Are they committing a crime?

More importantly and to the point is whether we are going to have a different standard for the receipt and publication of hacked material which is terribly interesting or concerns a person of public character. The defamation laws in this country have been bent and tweaked to protect those who publish defamatory material about those with a public presence.

It once was the law that if some bigshot was the subject of untruthful reporting, that person could sue for defamation and receive such damages as could be proven. The Supreme Court decided that newspapers needed greater protection, and therefore the standard for recovering in a defamation action should be higher. Today, those in the public have to prove actual malice, and not merely that somebody lied about them through neglect or carelessness.

The “actual malice” standard is great protection for the liars but awful for those who may be completely innocent.

It is important to step back from the current controversy as to who WikiLeaks is intending to help or hurt. As a wise old sage once said to me, “It all depends on whose ox is being gored.” Today it is Hillary Clinton who may be suffering at the hands of the Russians, WikiLeaks or who knows whom, but tomorrow it could be some highly placed Republican.

The big question that we will have to decide, when the smoke and fire of the current Presidential election clears, is whether we are going to enforce the laws we have or pass stronger laws to punish computer hacking and those who receive and use the hacked materials. Is there going to be a different standard if the information concerns public policy or public officials? The voters and legislators will have to make that decision. Clearly, our elected officials are nervous about strengthening laws against the theft of material from computers and the sale or transfer of that material because the public often revels in salacious and gory news. While I was driving on Route 80 the other day, it was annoying to notice how many people slow down to look at the car wreck on the side of the road during a heavy downpour. There is something about the human psyche that is thrilled by dramatic career-ending stories of hate, greed and lust.

The legal issues will not go away. The next generation of legislators will have to deal with a world where privacy does not exist and data of every kind for every person is on sale.

The time has come for us to squarely face this problem, both through technology protection and enforcement of the law. Unfortunately, some of the laws protect the computer manufacturers and internet providers. Legislation limiting the liability of software companies and web providers take the cop off the beat. They, too, should have culpability to the extent they permit or even encourage the facilitation of data stolen from one location and transferred, sold, or otherwise delivered to another. There is much the geniuses in Silicon Valley can do to prevent the unseemly trading in personal computer information, but there is no legal disincentive for those megacorporations to protect personal privacy.

So, what will it be; open season on personal information or protection for some of us or all of us?

Clifford A. Rieders, Esquire
Rieders, Travis, Humphrey,
Waters & Dohrmann
161 West Third Street
Williamsport, PA 17701
(570) 323-8711 (telephone)
(570) 323-4192 (facsimile)

Cliff Rieders, who practices law in Williamsport, is Past President of the Pennsylvania Trial Lawyers Association and a member of the Pennsylvania Patient Safety Authority. None of the opinions expressed necessarily represent the views of these organizations.