



Privacy – The Next “Big” Thing

By P. Blake Keating
Assistant Vice President, Media Claims
Content, Technology, and Services Liability Division
OneBeacon Professional Insurance

A German consumer recently went to court to compel disclosure of how much information his cell phone company had on his whereabouts. He was stunned to learn that Deutsche Telecom had recorded and saved his GPS coordinates 35,000 times during a prior six month period, or about once every seven minutes. Technology companies and firms that compile data are currently matching people's television viewing preferences with other personal data including prescription drug records in a sophisticated attempt to help advertisers buy advertisements that are targeted to shows watched by certain demographic groups, according to a recent report in [The Wall Street Journal](#).

In the United States, Facebook recently announced that one-half of all Americans age twelve or older now have a Facebook account, one of the highest national participation rates for the company in the world. Such widespread usage is evidence that most Americans are generally less concerned with their personal privacy being diminished than are persons in other parts of the world. Americans “voluntarily” and pragmatically give up certain rights such as privacy in exchange for things they see as benefits, such as discounts for having their shopping habits tracked by stores. But concern over diminished personal privacy is growing rapidly, even in the United States.

Privacy refers both to the right of the individual from oversight and monitoring as to the individual's activities, and increasingly, to the protection of stored data concerning, and owned by, individuals. Both concepts are undergoing significant change globally, generally in a manner of expanding individuals' rights.

In late January, the European Union announced that it had revised its fifteen year-old data protection law and indicated that its new standards might set precedents for the globally utilized, but borderless, Internet. Officials for companies over the world have surprisingly accepted the idea of new standards which would clarify rules about [which](#) legal standards apply [where](#) as to privacy issues. Differing national and cultural standards across the world, and a resulting decrease in rules of legal certainty, have previously proven problematic for companies such as Microsoft, Google and Facebook.

In Japan, Facebook has had limited growth because the Japanese typically use pseudonyms and nicknames online and Facebook requires that members use their real names. In Germany, Facebook has recently agreed to let users better shield their email contacts from unwanted advertisements and solicitations it sends. Google has recently been fined in France for violation of data protection laws in the collection of data for its online mapping service. In Switzerland, strict privacy laws have resulted in restrictions on updating Google's Street View photo service.

Over the past year, [The Wall Street Journal](#) and others have reported on the explosive growth of hundreds of companies that collect personal details about Internet users and their online activities including those related to personal data on health, finance, political leanings and shopping habits, among others. Many persons in the United States are surprised to learn that numerous companies harvest data on Internet users and assemble detailed profiles which are sold to advertisers and others without the knowledge of the Internet users. In response, heightened concerns about the erosion of personal privacy and companies and products which help persons manage the way companies track their information online have grown greatly.

In February, the Federal Trade Commission (FTC) proposed for the first time a “do not track” system that would help individuals prevent their online habits from being monitored as extensively as at present. One month later, Microsoft announced a new version of its Internet Explorer web browser that would assist users of its products in controlling their privacy. Consumer awareness of online privacy risks has resulted in other proposed changes enhancing privacy. Facebook has also recently adopted a more “plain English” privacy policy for consumers. The advertising industry seeks to counter the momentum for greater privacy by arguing that any restrictions would undermine the concept of free information on the Internet by depriving advertisers of revenue by curtailing their ability to reach specific customers.

Much of the exasperation of the American public that there is no general right to privacy has been exacerbated by the use of social media and the surprise that what many believe is “private”, is in fact, “public”. Facebook has declared all posts by members to be public, for example. Google saves for a period of time all searches made by users, which could be utilized to identify the searchers. Additionally, many consumers are dismayed to learn that they can be subjected to targeted advertisements that are intended to match their specific interests, based on websites they have visited. When using their computer at home, many Americans have a sense of being “in private”, when in reality, much of what they’re doing is “in public”.

Many Americans are genuinely surprised at how limited their privacy rights are in fact. There is no general federal right of privacy either constitutionally or by statute. Instead, there are a variety of laws on a variety of subjects that place limits on the use of information in a variety of contexts. Examples of federal statutory enactments include the Fair Credit Reporting Act, the Electronic Communications Privacy Act, and the Health Insurance Portability and Accountability ACT (HIPAA). Another federal law which affects the media online is the Children’s Online Privacy Protection Act (COPPA). It requires commercial websites oriented towards children and certain general interest websites to obtain parental permission before collecting information from children under age 13. About a dozen states have their own privacy statutes.

At common law over the past two hundred plus years, various states have recognized some parts of rights of privacy. These may be generally described as: (1) false light (a misleading mischaracterization); (2) disclosure of private facts; (3) intrusion upon seclusion; and (4) commercial misappropriation of the name or likeness of an individual for advertising or financial gain. California has recognized all four types of invasion of privacy, treating false light like libel. It has also enacted a statute preventing appropriation of a name or likeness. New York has recognized none of the four general rights at common law, but has, like California, enacted a statute against the use of an individual name or likeness for purposes of advertising. Other states recognize various combinations of these four types of privacy rights.

The current piecemeal approach to privacy in the U.S. is confusing for consumers and businesses. It is also expensive for businesses to comply with all the various laws. In response, the Obama administration in March announced a proposed “privacy bill of rights” to protect Americans from intrusive means of data gathering, citing the growing concern about the tracking and targeting of Internet users. As proposed, the bill might prohibit companies’ use of personal information for a purpose other than that for which it was collected. A new law would give consumers the right to access information about themselves and a right to have that information stored securely.

Privacy law throughout the world is currently in a state of amazing, rapid change and remains an emerging concept, particularly in the United States. The media and businesses need to be aware of such changes throughout both the political and technological worlds and to anticipate further similar changes. Risk management and media insurance should apply globally to all activities of an organization whether at any given time it is engaged in news gathering, dissemination of content or storage of data. As the amount of information continues to grow exponentially, along with means of access, it is more and more likely that privacy breaches will occur. OneBeacon Professional Insurance Company can work with you to implement risk management and damage control procedures in advance designed to limit your liability and related damages.