



---

# Wisconsin Briefs

*from the Legislative Reference Bureau*

---

Brief 14-2

March 2014

## ONLINE PRIVACY – SOCIAL MEDIA, E-MAIL WARRANT SEARCH, AND CUSTOMER DATA

As many individuals integrate their personal lives with their online presence, privacy remains a priority for those who wish to keep personal data within their control. Recent revelations in the media about the National Security Agency's surveillance have put privacy issues at the top of many legislators' concerns. Such concerns have led to an increased amount of legislation related to privacy.

E-mail, social media, and online databases have quickly opened doors to information that was previously limited in availability. A commonly held belief is that the law has not moved at the same pace as technology, leaving people vulnerable to privacy intrusion. This brief summarizes some of the current issues with Internet privacy and provides a description of what states are doing to address these concerns.

### SOCIAL MEDIA

According to a 2013 poll performed by Pew Research Center, 72% of U.S. adults use social networking sites, which can include sites such as Facebook, LinkedIn, and Twitter. Eight in 10 teens (12-17 years old) who use the Internet use social networking sites. Such sites encourage its users to share information such as where they go to school, their favorite musical artists, and interests. These sites may also serve as a platform for a user to share political or personal beliefs, which other users could find offensive. Despite social media sites having options to delete shared information, the data about that information may be stored indefinitely, which many users do not understand.

Users who share personal opinions may be subject to ridicule or praise from their peers. Users may assume such information is only available to those who are on their approved list of social contacts. However, if a user does not adjust their privacy settings so that only certain people may view their content, the information is public and can be seen by anyone. Sharing personal photos may also pose privacy risks due to the fact that once a person posts an image on the Internet, anyone can save a copy and repost it without permission. For younger users, posts can have an impact as they reach adulthood and they may eventually regret certain posts as they apply for jobs or school.

There have been several reports in media outlets regarding potential employers use of social media information to determine eligibility for employment. For example, if a person posted publicly viewable photos of inappropriate behavior, a potential employer could see the photos and forgo hiring the applicant. Additionally, some cases of potential employers asking for social media passwords have been reported, and many applicants believe they risk losing a chance for employment if they decline to provide them.

Those who are already employed can also feel the effects of social media intrusion. Some employees have been terminated due to photos or posts that were considered to be inappropriate by their employers. Employers argue that they are able to do so if the post goes against company policy, such as making the post while at work. However, terminated employees state that social media posts

fall under free speech and should not be used against them.

In the Virginia federal case *Bland v. Roberts*, a deputy sheriff lost his job when his employer found out that he “liked” the Facebook page of a candidate who was trying to replace his boss, the sheriff. When the sheriff found out about the “like,” he fired the deputy. The plaintiff argued that using the “like” feature on Facebook was protected by the first amendment because it is a form of political speech. The court determined that the “like” feature was not protected by the first amendment and that the plaintiff did not prove his termination was due to political retaliation. However, this decision was recently reversed by the U.S. Court of Appeals 4th Circuit, which determined that “liking” something on Facebook was a form of free speech.

Prospective students applying to some schools have noticed that their social media accounts are scrutinized alongside their applications. University representatives have stated that schools do not have policies that require social media to be taken into consideration for acceptance, but it is not prohibited either. Many question whether it is fair for schools to examine social media posts that occurred several years prior to a prospective student’s application.

Those who argue that employers and schools should not have access to an employee’s or applicant’s social media information include privacy advocacy groups, the American Civil Liberties Union (ACLU), and social media companies. Privacy proponents

believe that allowing employers or schools to view social media information amounts to an invasion of privacy, similar to going through one’s house or mail. They also argue that such access puts the privacy of third parties, such as social media contacts, at risk.

Groups in favor of gaining access to social media sites include employers and some schools. These parties believe that having access to social media profiles helps them to gain a better understanding of whether a person would make a suitable employee or student. Employers say that social media screening allows them to identify applicants whose online behavior might reflect work ethic. It also helps identify if and when workers post photos of inappropriate on-the-job behavior. Some school athletic programs state that such monitoring may help determine whether an athlete has taken part in prohibited behavior such as alcohol or drug use.

In response to privacy concerns, many state legislatures have introduced or passed legislation that prohibits employers and schools from requiring candidates to provide usernames and passwords for employment or acceptance. As of March 2014, 12 states have enacted laws prohibiting employers from requiring job applicants or employees to provide access to their personal social media accounts. Nine states have enacted laws prohibiting higher educational institutions from requiring access to an applicant’s or student’s social media accounts (see Table). Nineteen other states have introduced similar legislation that would prohibit employers or schools from requiring username and passwords for employment or acceptance.\*

---

\*Those states are Florida, Georgia, Hawaii, Indiana, Iowa, Kansas, Maine, Massachusetts, Mississippi, Missouri, Nebraska, New Hampshire, New York, Ohio, Oklahoma, Tennessee, West Virginia, Wisconsin, and Wyoming.

2014 State Statutes Related to Social Media Privacy Protection		
State	Employer	Educational Institutions
AR	Ark. Stat., Secs. 6-60-104 and 11-2-124	Ark. Stat., Sec. 6-60-104
CA	Cal. Lab Code, Sec. 980	Cal. Ed. Code, Sec. 99121
CO	Col. Rev. Stat., Sec. 8-2-127	
DE		Del. Code, tit. 14 Sec. 8103
IL	820 ILCS 55/10	105 ILCS 75/10
MD	Md. Labor and Employment Code, Sec. 3-712	
MI	Mich. Comp. Laws, Sec. 37.273	Mich. Comp. Laws, Sec. 37.274
NJ	N.J. Stat. Ann. Sec., 34:6B-6	N.J. Stat. Ann. Sec., 18A:3-30
NM	N.M. Stat., Sec. 50-4-34	N.M. Stat., Sec. 21-1-46
NV	Nev. Rev. Stat., Sec. 613.135	
OR	Ore. Rev. Stat., Sec. 659A.330	Ore. Rev. Stat., Sec. 326.551
UT	Utah Code Ann. 34-48-201	Utah Code Ann. 53B-25-201
WA	Wash. Rev. Code, Sec. 49.44.200	

## E-MAIL SEARCHES

The federal Electronic Communications Privacy Act (ECPA) of 1986 requires federal and state agencies to obtain a warrant in order to access e-mails that are less than 180 days old (18 U.S.C. § 2703 (a)). However, when the ECPA was written, Internet users were not perpetually logged on to servers due to the high costs associated with being online. Additionally, the high cost for online storage caused most users to download their e-mails directly onto their computers and delete those e-mails from the e-mail service provider's server, rather than store them indefinitely online.

Today, the majority of Internet users store their e-mails indefinitely using cloud-based storage, known as the Cloud, rather than downloading them to their computers. Authorities need a warrant to read e-mails less than 180 days old, however e-mails that are more than 180 days old can be accessed with a warrant, subpoena, or court order (18 U.S.C. § 2703 (a) and (b)). Privacy advocates argue that there should be no distinction between e-mails that are less or more than 180 days old, and that the ECPA needs to be updated to reflect the technological changes that

have occurred since 1986. Some congressional lawmakers have expressed concerns about e-mail searches, but no changes to the ECPA have been made.

Advocates for stronger e-mail privacy protections argue that e-mail searches without a warrant violates a person's Fourth Amendment rights against unreasonable search and seizure. Since many users do not delete e-mails, advocates state that the ECPA leaves users' privacy open to intrusion.

Those who wish to maintain the current language of the ECPA state that searching e-mails is a matter of national security that does not violate the Fourth Amendment. Some court cases have determined that individuals have limited privacy rights when they decide to share information through a third party, which includes e-mail service providers. Others assert that accessing e-mails could prevent future terrorist acts if authorities were able to obtain information that revealed potential threats.

Texas recently became the first state to require a warrant for e-mail searches. 2013 Texas House Bill 2268 was signed into law in June 2013.

## DATA PRIVACY

Consumers who visit a company's web-page provide data to the company about their interests simply by clicking on links or purchasing items. The data is stored and can eventually be used to determine what a consumer may be interested in purchasing in the future. For example, a consumer who navigates to a page that contains information about running shoes may later see advertisements about other running gear. The sharing of personal information allows companies to sell data to third parties, which may in turn use the data to determine advertisements that a person may find of interest.

Privacy advocates say the data may be used to make unmerited assumptions about individuals, and that consumers have a right to know what kind of data is being collected. In addition to knowing what data is collected, advocates believe that consumers should also be able to know which companies purchase it.

From the standpoint of organizations that analyze collected data, such information can provide insights into things such as consumer trends and preferences. Using analytics, gathering data on social media posts has been shown to predict flu outbreaks and voter trends. Groups in favor of such data collection also believe that society has reached a point where Internet privacy should no longer be an expectation.

Legislation on browser data collection has been very limited, mostly because the issue still appears to be new to most lawmakers. California became the first state to introduce so-called "right-to-know" legislation during their 2013 session. Although the bill recently died, 2013 California Assembly Bill 1291 would have required any business that retains a customer's data, or provides that information to a third party, to provide a copy of that information to the customer within 30 days of the customer's request.

## WISCONSIN INTERNET PRIVACY LAWS AND LEGISLATION

Currently, the Wisconsin Statutes contain provisions that address court ordered interception of electronic communications and the process that allows for subpoenas and warrants for certain electronic communications. The statutes, however, do not contain any provisions about social media accounts or data collection with respect to Internet browsing. Some bills have recently been introduced on social media and passwords.

Section 968.28, Wisconsin Statutes, states that an investigative or law enforcement officer may receive approval from the attorney general and the district attorney from any county to obtain an order authorizing the interception of electronic communications. An authorization may only be granted if the interception will provide evidence in cases involving certain serious crimes such as homicide, kidnapping, and child sex trafficking. If an officer is authorized to intercept electronic communications, he or she may only disclose information derived therefrom where it is appropriate to the investigation [s. 968.29].

The application for authorization must include the applicant's identity; a complete, factual statement about the investigation and the justification for obtaining the order; a description of what other investigative procedures have taken place and why they were unsuccessful, or why they would be unsuccessful if tried; the period of time for which the interception will be sustained; and a statement about any other requests or approvals for interceptions. If the application is for an extension of an order, then the officer must provide a statement describing the results thus far or provide a reason why results have not been achieved. Furthermore, an authorization may not last longer than 30 days unless an extension is approved [s. 968.30]. If a person intentionally intercepts, uses, alters, discloses, or attempts to disclose information

found in electronic communications, he or she will be guilty of a Class H felony [s. 968.31].

2009 Wisconsin Act 349 created Sections 968.375, Wisconsin Statutes, which addresses the disclosure of electronic communications. The statute allows the attorney general or a district attorney, upon probable cause, to request a judge to issue a subpoena, which would require an electronic communication service provider to provide certain information about a customer. Such information can include a customer's name, address, telephone connection records, duration of service, and source of payment for the service.

Section 968.375 also permits the attorney general or a district attorney to obtain a warrant from a judge. If a warrant is obtained, an electronic communication service provider must provide the contents of electronic communications stored in a communications system. The requirement for a subpoena or warrant does not apply if the customer consents to the search, or in cases of emergencies involving death or serious injury if the records are not obtained.

2013 Senate Bill 223 and its companion bill, Assembly Bill 218, would make it unlawful for employers, educational institutions, and landlords to request an employee, applicant for employment, student, prospective student, tenant, or prospective tenant to provide access to his or her personal Internet accounts. The bills would also prohibit those entities from disciplining or penalizing individuals who do not provide access to their Internet accounts. SB-223 passed the Senate and Assembly Bill 218 is awaiting the governor's signature.

## SOURCES

Dame, Jonathan. "Will Employers Still Ask For Facebook Passwords in 2014?," *USA Today College*, January 6, 2014, <http://www.usatoday.com/story/money/business/2014/01/10/facebook-passwords-employers/4327739/>.

Doyle, Charles. *Privacy: An Overview of the Electronic Communications Privacy Act*. Washington, DC: Library of Congress, Congressional Research Service, 2012. <http://www.fas.org/sgp/crs/misc/R41733.pdf>.

Madden, Mary, et al. *Teens, Social Media, and Privacy*. Washington, DC: Pew Research Center, May 21, 2013: [http://www.pewinternet.org/files/2013/05/PIP\\_TeensSocialMediaandPrivacy\\_PDF.pdf](http://www.pewinternet.org/files/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf).

Pew Research Internet Project. "Social Networking Use," Accessed December 1, 2013. <http://www.pewresearch.org/data-trend/media-and-technology/social-networking-use/>.

Schoenberg, Tom. "Facebook 'Like' Is Protected Speech, Appeals Court Says." *Bloomberg*, September 18, 2013, <http://www.bloomberg.com/news/2013-09-18/facebook-like-is-protected-speech-appeals-court-says.html>.

Sengupta, Somini. "No U.S. Action, So States Move on Privacy Law," *New York Times*, October 30, 2013, <http://www.nytimes.com/2013/10/31/technology/no-us-action-so-states-move-on-privacy-law.html>.

Singer, Natasha. "They Loved Your G.P.A. Then They Saw Your Tweets," *New York Times*, November 9, 2013, [http://www.nytimes.com/2013/11/10/business/they-loved-your-gpa-then-they-saw-your-tweets.html?\\_r=2&](http://www.nytimes.com/2013/11/10/business/they-loved-your-gpa-then-they-saw-your-tweets.html?_r=2&).