

Protecting Our Privacy In a Digital World by MARCIA J. WEISS

In this high-technology era of smartphones, all kinds of computers and social media, what we communicate, search for and store can be used for unwanted interference into our private lives. Privacy and data security issues are a growing concern of Americans, especially as the internet and technology have made personal information more accessible and easier to collect and manipulate.

Security cameras monitor traffic and our movements in public and private places. Mobile tracking devices that anyone can buy can trace your location via GPS. Smart (or internet-connected) televisions have snooping devices, and tracking cookies on our computers routinely divulge our shopping and other habits. Even when we've taken precautions to ensure privacy — eliminating spyware in our computers, regularly changing passwords, deleting cookies and using encryption — we are still at risk.

A recent Karlstad University (Sweden) study found that few people even know how their data are accessed, collected, used and shared.

New technologies are advancing our freedoms, but they are also enabling unprecedented invasions of privacy. National laws have yet to catch up with the changing needs for privacy that come with new digital technologies.

The Fourth Amendment guarantees that “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated and no warrants shall issue, but upon probable causes supported by oath or affirmation and particularly describing the place to be searched.” Now more than 200 years later, however,

the websites we visit and what we read and buy in cyberspace help to establish personal patterns that can be monitored, disclosed and manipulated.

The right of privacy is not expressly guaranteed in the Constitution. Instead, privacy has been inferred within the “liberty” guarantee of the Fourteenth Amendment to encompass decisions about procreation, marriage, abortion, child rearing and termination of medical treatment. It is also referred to in the Ninth Amendment’s “enumeration clause,” stating that the Bill of Rights “shall not be construed to deny or disparage other rights retained by the people.”

What is our expectation of privacy? In 1890, the future Supreme Court Justice Louis D. Brandeis and his law partner Samuel D. Warren published the influential essay “The Right to Privacy.” They reasoned that privacy encompasses the often quoted phrase “the right to be let alone.” Author Gabriel Garcia Marquez noted, “All human beings have three lives: public, private and secret.” Statistics have demonstrated older generations are concerned with maintaining information away from watchful eyes, while younger generations are less fearful of revealing certain data about themselves and their likes and dislikes.

In a 2012 issue of the *Stanford Law Review*, authors Omer Tene and Jules Polonetsky write that there are ways in which data collection can help promote the common good, for example, enabling researchers to determine adverse side effects of drugs that might otherwise go unnoticed and to track and respond to the exposure and spread of diseases. Balancing the various interests in

health information and upholding confidentiality, privacy and security present major challenges within our healthcare and legal systems.

Insights into various aspects of human behavior may also be beneficial but violate personal rights. Invasion of privacy might be justified in allowing law enforcement agencies to collect and use certain information when investigating crimes and in permitting the military to uncover terrorists through personal information.

The scope of privacy issues extends far beyond the limits of this article, but here are some thoughts on educating ourselves and taking action.

There are ways to protect our privacy. Consider the inherent risks and make efforts to control the amount of personal information that you provide online. Educate friends and family about the importance of online privacy and the steps they can take to protect themselves. Change passwords frequently and make them strong; use different passwords for different sites. Refrain from opening emails from unrecognized sources.

You can contact your internet service provider (ISP) and opt out of data sharing on your internet use. You can use encryption to hide the content of your communications from an ISP or other parties. You can use a VPN (Virtual Private Network). Unfortunately, these options have limitations and might be difficult to set up.

Electronic health information can also be compromised. If health information privacy has been violated, the Office of Civil Rights of the Department of Health and Human Services should be notified and a complaint filed.

Forty-nine states have created databases to track prescription drugs. Law enforcement agencies need a warrant to access the content of the database. Since records of prescription medications can reveal sensitive personal information, some states give legal protection to drug databases. But protection does not go unchallenged. Although Oregon requires probable cause to issue a warrant for law enforcement access, the federal Drug Enforcement Administration has tried to obtain the data without a warrant. An ACLU lawsuit resulted in a judicial ruling that patients have a reasonable expectation of privacy in their drug prescription records within a state database. Failure to obtain a warrant is illegal under the Fourth Amendment.

Monitoring and advocating for privacy laws are essential. Look at a headline from this past April: "Trump Signs Bill Repealing U.S. Internet Privacy Rules." These Obama administration rules would have required wireless and broadband providers to get your permission before packaging and selling your private information, including your Social Security number, financial and health data, web browsing history, app usage history and the content of communications. In terms of rights, the new rules violate our freedom of speech and our right to associate. It also violates our First Amendment rights, making it more difficult to understand how personal information is being shared and used.

The April 26, 2017, issue of *Science News* addressed the need for new human rights laws to protect against advances in neurotechnology that may put the "freedom of the mind" at risk. Brain imaging can be used by consumer companies for neuromarketing. Advanced brain imaging might be used some day in

criminal courts to assess criminal responsibility or the risk of reoffending. The field of neurolaw raises some fascinating and frightening questions. Will advanced neurotechnology violate the terms of the Constitution? Should a warrant be required to look inside someone's brain? Even if technologies don't violate constitutionality, ethical questions remain.

Americans are speaking with a unified, nonpartisan voice on these matters: A 2016 poll showed that 90 percent of Americans wanted the next president to prioritize "protecting privacy so [Americans] have more control over our personal information."

State legislators throughout this nation have heard their call. The message from these collective state actions is clear: If Congress is unwilling or unable to act to adequately protect Americans' privacy, the states are more than willing to step up and fill the void. All states except Alabama and South Dakota have security breach laws. They require the government and private companies that collect data and compile information to notify individuals of a security break of personally identifiable information. Twenty-five states have passed social media privacy laws preventing employers and educational institutions from obtaining passwords for personal internet access.

For more information, visit the National Conference of State Legislatures (ncsl.org), a comprehensive, bipartisan source of state laws.

As the internet and new technologies continue to raise new policy questions about privacy, we need to keep up-to-date and to advocate to protect ourselves.

Marcia J. Weiss, JD, is NA'AMAT USA national vice president of advocacy and education.