



## INTERNET PRIVACY

Lexile Measure: 1220L

### FIELDS OF STUDY

Computer Science; Privacy; Security

### ABSTRACT

Internet privacy is an issue of concern in the early twenty-first century. With increasing Internet use for work, socializing, and daily tasks comes a corresponding increase in potential breaches of privacy. To address this issue, individuals may use a variety of technologies and techniques to ensure the security of their personal information and online communications.

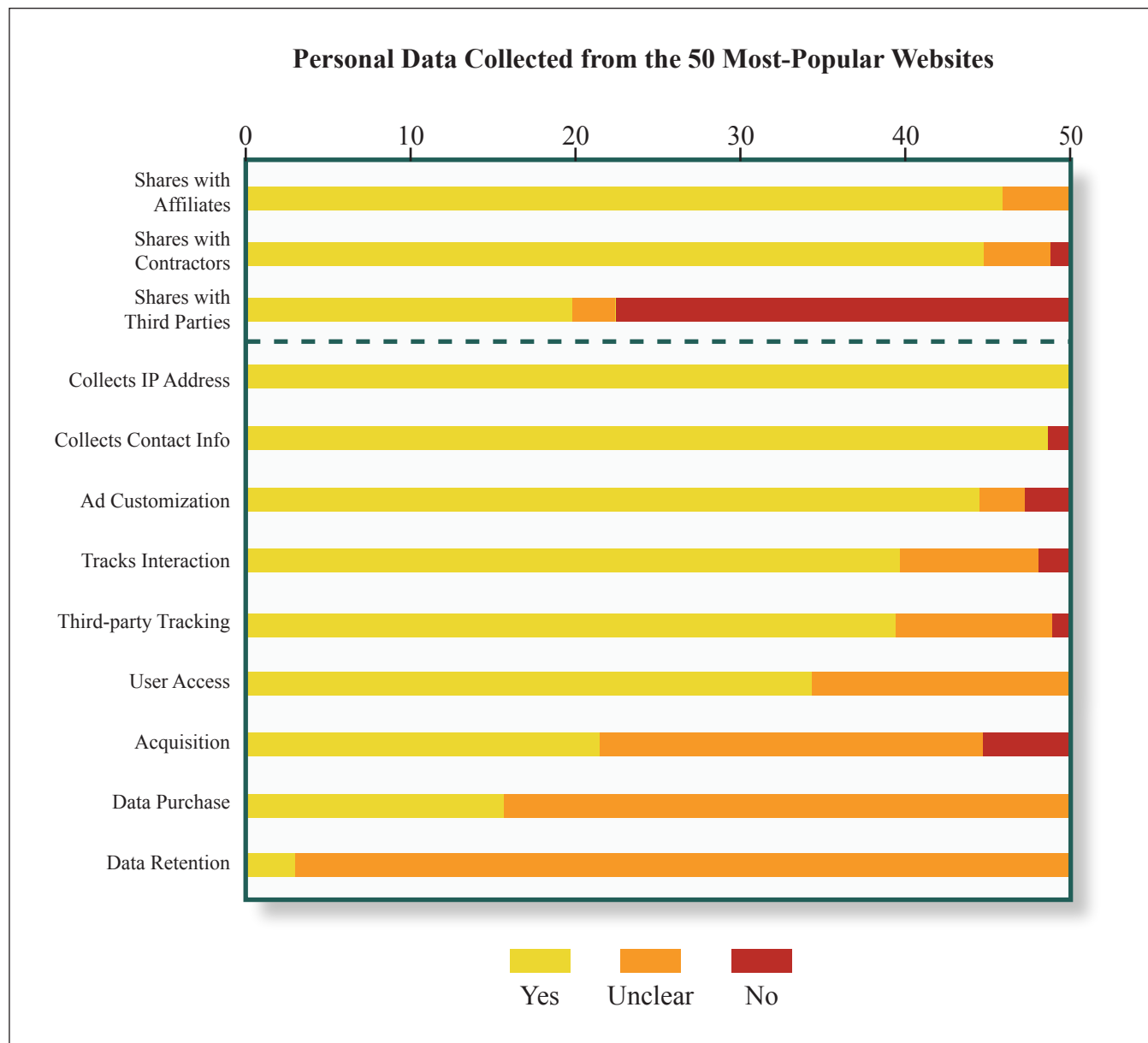
### PRINCIPAL TERMS

- **behavioral marketing:** advertising to users based on their habits and previous purchases.
- **cookies:** small data files that allow websites to track users.
- **digital legacy (digital remains):** the online accounts and information left behind by a deceased person.
- **device fingerprinting:** the practice of collecting identifying information about a computer or other web-enabled device.
- **personally identifiable information (PII):** information that can be used to identify a specific individual.
- **Privacy Incorporated Software Agents (PISA):** a project that sought to identify and resolve privacy problems related to intelligent software agents.

### Internet Privacy Concerns

The Internet has enabled individuals the world over to communicate with one another and share information. Internet users can socialize, shop, conduct financial transactions, and carry out other tasks online. The privacy of their online actions and the data they share have become increasingly at risk, however. Breaches of online privacy can take many forms. It can be the inadvertent sharing of **personally identifiable information (PII)** through lax social media security settings. Or it can be the theft of banking or credit card information. Insufficient privacy practices can make it possible for criminals to gain access to individuals' contact details, health data, financial information, or government identification information such as Social Security numbers. Such access can lead to identity theft or fraud.

Cybercrime is one of the major causes of concern in regard to Internet privacy. Privacy breaches by corporations and marketers are also major concerns. Tracking technologies



Graph showing privacy policy practices of the 50 most visited websites, adapted from KnowPrivacy ([knowprivacy.org](http://knowprivacy.org)) research conducted by UC Berkeley School of Information, 2009. Users' personal data is often collected and shared with affiliates or contractors that the site does not consider "third party," making them exempt from privacy policies stating the site does not share users' information. In many cases, it is unclear what information is being collected.

enable advertisers to market to individuals based on their browsing habits and previous purchases. Some users enjoy being served ads relevant to their shopping patterns, but others view that it as an invasion of privacy. Protecting one's online activity from government surveillance is likewise of concern to some Internet users. Their concern increased after the secret US National Security Agency (NSA) Internet surveillance program PRISM was revealed in 2013.

## Research

A number of government and public-sector organizations have researched the privacy needs of Internet users. One such research initiative, the European-run **Privacy Incorporated Software Agents (PISA)**, sought to identify and resolve privacy problems associated with intelligent software agents. These agents are computer systems that act on the behalf of the user in a semiautonomous manner. The researchers also examined existing privacy laws and best practices. They created a prototype interface designed to meet usability requirements of users. The interface was also designed to gain users' trust, so that they would feel comfortable entering their personal information. The researchers found that even when privacy options were provided, as in a settings or control panel interface, many users had difficulty understanding how to use those options to meet their privacy needs. The users also found it hard to understand how the privacy options were connected to the personal information they had entered.

## Threats to Internet Privacy

Potential threats to Internet privacy take a number of forms. Perhaps the most high-profile threat is that of hackers who seek to steal individuals' personal data. In some cases, criminals may steal data such as credit card numbers by hacking into the servers of online retailers. In other cases, a criminal may use phishing e-mails to trick an individual into revealing personal information. Some criminals use surveillance programs such as keyloggers. Keyloggers can record all keystrokes made on a computer and transmit that data to another user. Most threats to Internet privacy are digital in nature, but the consequences of weak Internet privacy can also extend past the computer screen. A lack of privacy protections on social media can reveal an individual's address and the dates they will be on vacation to potential burglars, for instance.

Privacy concerns likewise extend to online marketing. Many marketers use **cookies**, small data files that track individual users on the Internet. Cookies allow marketers to send individuals targeted ads based on prior purchases and browsing habits. For example, an individual may view a pair of shoes online but not immediately buy them. The shoe seller may use cookies to send ads for the shoes to the user as they keep browsing online. This process is called **behavioral marketing**.

In addition to criminals and ads, the government is sometimes perceived as a threat to online privacy. In the United States, government surveillance of online activity greatly increased following the terrorist attacks of September 11, 2001, and the subsequent passage of the controversial PATRIOT Act. In 2013 the US government confirmed the existence of the Internet surveillance program PRISM. The National Security Agency used PRISM to access data from companies such as Google and Microsoft. The government stated it needed this access to protect national security.

## Digital Remains

Among the more unusual Internet privacy dilemmas is that of an individual's **digital legacy**, or **digital remains**. These are the online information, records of communication, and personal websites or profiles of a deceased person. Digital remains may continue to exist on the Internet long after the person has died. In certain cases, the deceased's next of kin may leave online remains in place as a digital memorial. Or, if allowed, they may delete them to protect the deceased person's privacy. Some online services, such as the social network Facebook, offer users the option to name a contact who can gain access to the

account after the user's death. The contact can then determine whether to delete or preserve profile information. Many legal issues remain around who can access and control an individual's digital remains and to what extent this information may be controlled.

## Protecting Internet Privacy

Those concerned about Internet privacy can make their personal data more secure. To obtain a basic level of privacy, individuals should observe standard online security procedures. These include using strong, unique passwords and two-factor authentication, in which a password is paired with another form of authentication, when available. Running antivirus or firewall software allows individuals to identify and remove programs such as keyloggers or prevent them from infecting the computer in the first place. Individuals can also protect the privacy of credit card or Social Security numbers by entering them only on trusted websites that encrypt such data. Most standard web browsers offer users the ability to delete cookies, which temporarily prevents such tracking from taking place. However, it is sometimes possible to track devices without the use of cookies through **device fingerprinting**. Thus, deleting cookies can provide only a limited level of privacy.

— Joy Crelin

## Bibliography

- Bernal, Paul. *Internet Privacy Rights: Rights to Protect Autonomy*. New York: Cambridge UP, 2014. Print.
- "Internet Privacy." *ACLU*. American Civil Liberties Union, 2015. Web. 28 Feb. 2016.
- "Online Privacy: Using the Internet Safely." *Privacy Rights Clearinghouse*. Privacy Rights Clearinghouse, Jan. 2016. Web. 28 Feb. 2016.
- "Protect Your Privacy on the Internet." *Safety and Security Center*. Microsoft, n. d. Web. 28 Feb. 2016.
- "A Short History of US Internet Legislation: Privacy on the Internet." *ServInt*. ServInt, 17 Sept. 2013. Web. 28 Feb. 2016.
- "What Is Personally Identifiable Information (PII)?" *U Health*. U of Miami Health System, n.d. Web. 28 Feb. 2016.