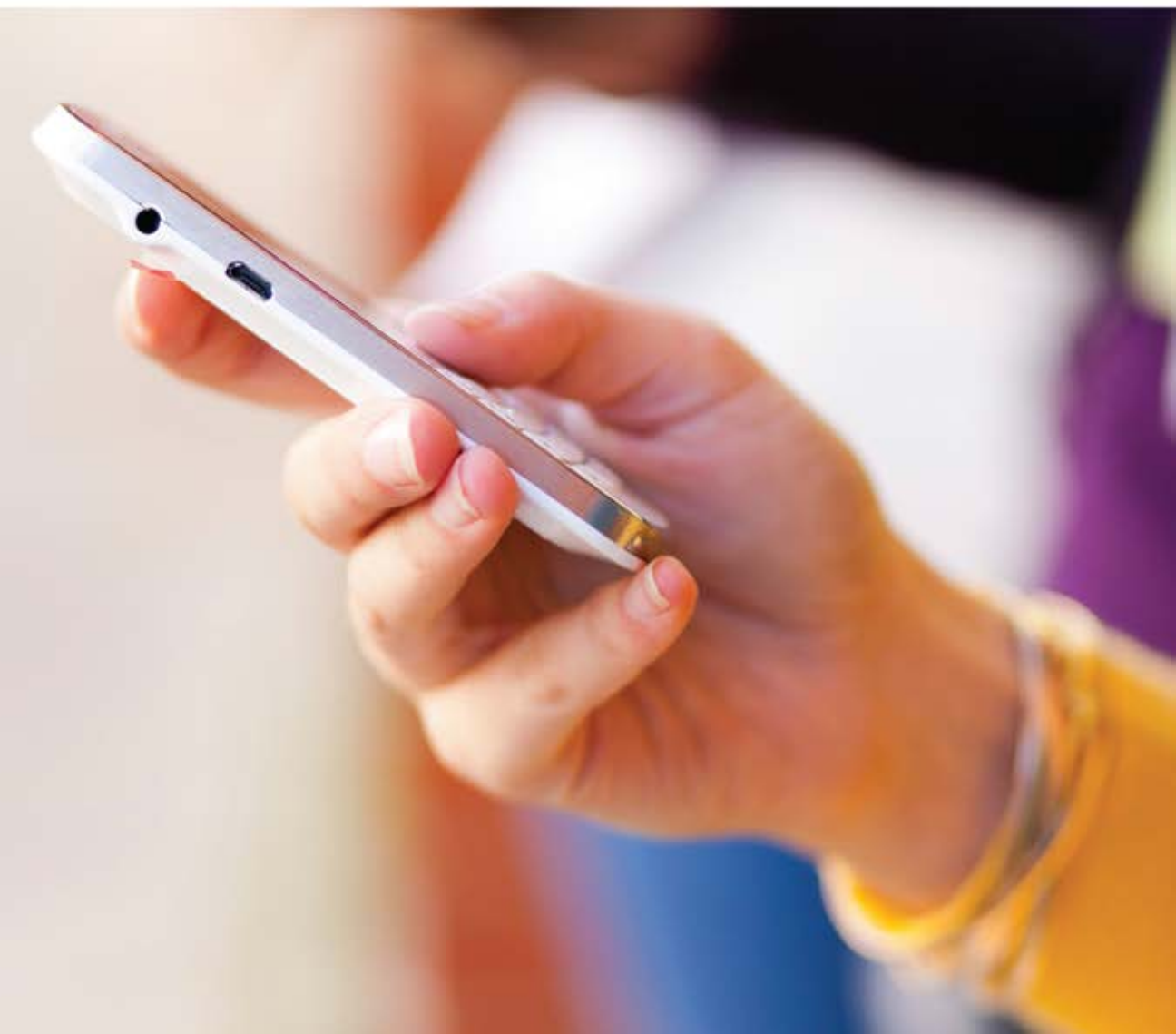
Cell Phones and Society

Cell Phones: Threats to Privacy and Security

Patricia D. Netzley



Contents

Benefits Versus Risks

Introduction

Cell phones have provided society with many benefits. Their portability enables users to talk to friends or call for help from anywhere there is a communication system capable of connecting one phone to another. A type of cell phone called a smartphone also allows individuals to access the Internet while mobile, making business transactions and online entertainment activities just as easy to conduct while traveling as at home. But there are downsides to cell phones as well. All kinds of cell phones can make users vulnerable to invasions of privacy, and smartphones can also expose them to serious financial security threats.

Open to Thieves

Security experts warn that smartphones are never 100 percent private. *Consumer Reports* magazine explains: "When you take your phone into your confidence, so to speak, you're also taking in a host of parties that make all of those wonderful mobile services possible, including app developers, your wireless carrier and phone manufacturer, mobile advertisers, and the maker of your phone's operating system."[1] All of these entities can collect data, such as a phone's location or unique ID, that allow the user's online and physical movements to be tracked.

Thieves can use apps to access phone data as well, typically to steal personal information related to financial transactions. A study by *Consumer Reports* suggests that in 2013 roughly 1.6 million smartphone users were tricked into installing a malicious app—made to look like a legitimate one—that allowed a thief to intercept credit card information during online transactions and/or steal banking passwords or other sensitive information. Thieves can also install harmful software in a phone by sending an e-mail or message that tricks a phone user

into visiting a malicious website and unknowingly downloading the software.

In addition, security experts warn that smartphones can be hacked (accessed by someone without authorization to do so) just as a computer can. This is because whenever a smartphone is on, it is usually connected to the Internet. Moreover, as cybersecurity expert John Hale notes, "Your cell phone really is a small computer."[2]

Millions of Users

No one knows just how many people have had their cell phones hacked. However, the number of potential victims is growing because of the rise in smartphone use. *Consumer Reports* estimates that in 2013 more than half of all American adults used such a device, and more than 100 million relied on their smartphone to conduct business transactions using either the Internet or an app. However, security experts say that there are ways to protect a phone from invasion by thieves. These include installing apps cautiously and not accessing the Internet via unsecure wi-fi connections, such as ones provided at hotels and airports. In regard to the latter, David Jacobs of the Electronic Privacy Information Center, a consumer advocacy group, says, "Most consumers don't realize when they're transmitting info over an open Wi-Fi network that it can be intercepted."[3]

> "Your cell phone really is a small computer."[2]
>
> *—Cybersecurity expert John Hale.*

Security experts add that it is important to have safety features on a phone in case the device is stolen. Without these, thieves can easily access the phone's personal data. One such security measure is a screen lock with a strong password that blocks anyone without the password from using the phone. Another is an app that allows the phone's owner to erase all of its data from a remote location upon realizing the phone has been lost or stolen. Although smartphone users are typically connected to the Internet for long periods, experts say that taking such precautions can make smartphones as safe as home computers.

Smartphones benefit users of all ages, but privacy and security vulnerabilities are a growing concern. Tracking features, malicious apps, and hacking all pose threats to users.

a court order to do so can monitor any phone a suspected criminal might have access to, not only phones ordinarily used by the suspect. This means that if a suspected terrorist visits the home of an innocent person, the phone in that home might be subjected to a wiretap. The 9/11 attacks also triggered the creation of a classified government surveillance program whereby certain kinds of information can be gathered without first getting a court order. As details about this program have leaked out, many Americans have become concerned about the privacy of their cell phone conversations.

Security experts counter that since most law-abiding Americans are unlikely to be the target of a government wiretap, the greater concern should be the risk that criminals, friends, or relatives might compromise cell phone security or privacy. New technologies are making

Related Organizations and Websites

American Civil Liberties Union (ACLU)

125 Broad St., 18th Floor
New York, NY 10004
phone: (212) 549-2500
website: www.aclu.org

The ACLU works to protect the rights and liberties established by the US Constitution and US laws, including the right to privacy.

CTIA-The Wireless Association

1400 Sixteenth St. NW, Suite 600
Washington, DC 20036
phone: (202) 736-3200
website: www.ctia.org

Previously known as the Cellular Telecommunications Industry Association, this international nonprofit membership organization supports the wireless communications industry and provides information on cell phone–related issues and laws.

Internet Crime Complaint Center (IC3)

website: www.ic3.gov

Established by the FBI and the National White Collar Crime Center, this agency receives Internet-related criminal complaints and refers them to the appropriate agencies for investigation. These complaints include crimes associated with smartphone access to the Internet.

For Further Research

Books

Dale-Marie Bryan, *Smartphone Safety and Privacy*. New York: Rosen, 2013.

Brian X. Chen, *Always On: How the iPhone Unlocked the Anything-Anytime-Anywhere Future—and Locked Us In*. Cambridge, MA: Da Capo, 2011.

Ronald J. Diebert, *Black Code: Surveillance, Privacy, and the Dark Side of the Internet*. Toronto: McClelland & Stewart, 2013.

Richard Guerry, *Public and Permanent: The Golden Rule of the 21st Century; Straight Talk About Digital Safety; The Real Consequences of Digital Abuse*. Bloomington, IN: Balboa Press, 2011.

Sheran Gunasekera, *Android Apps Security*. New York: Springer Science+Business Media, 2012.

Richard Hantula, *How Do Cell Phones Work?* New York: Chelsea Clubhouse, 2009.

Daniel V. Hoffman, *Blackjacking: Security Threats to BlackBerry Devices, PDAs, and Cell Phones in the Enterprise*. Indianapolis: Wiley, 2007.

Anmol Misra, *Android Security: Attacks and Defenses*. Boca Raton, FL: CRC, 2013.

Kevin D. Murray, *Is My Cell Phone Bugged?* Austin, TX: Emerald, 2011.

Index

Note: Boldface page numbers indicate illustrations.