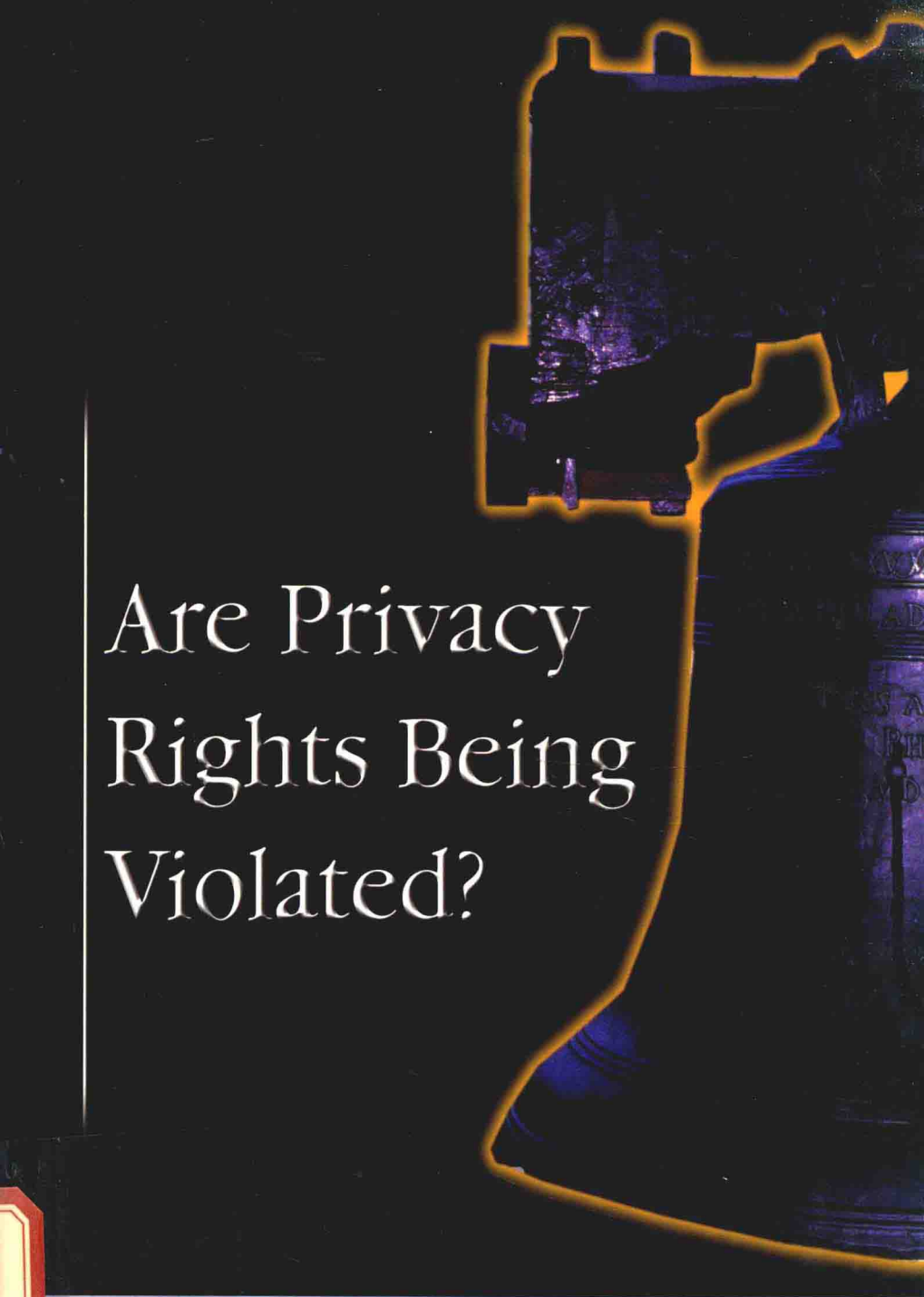

Are Privacy Rights Being Violated?

At Issue

CIVIL LIBERTIES

At Issue

Are Privacy Rights Being Violated?

Stuart A. Kallen, *Book Editor*

Bruce Glassman, *Vice President*
Bonnie Szumski, *Publisher*
Helen Cothran, *Managing Editor*

GREENHAVEN PRESS
An imprint of Thomson Gale, a part of The Thomson Corporation

THOMSON
GALE

Detroit • New York • San Francisco • San Diego • New Haven, Conn.
Waterville, Maine • London • Munich

For more information, contact
Greenhaven Press
27500 Drake Rd.
Farmington Hills, MI 48331-3535
Or you can visit our Internet site at http://www.gale.com

LIBRARY OF CONGRESS CATALOGING-IN-PUBLICATION DATA

Are privacy rights being violated? / Stuart A. Kallen, book editor.
p. cm. — (At issue)
Includes bibliographical references and index.
ISBN 0-7377-2360-2 (lib. : alk. paper) — ISBN 0-7377-2361-0 (pbk. : alk. paper)
1. Privacy, Right of—United States. I. Kallen, Stuart A., 1955– . II. At issue (San Diego, Calif.)
KF1262.A97 2006
342.7308'58—dc22 2005045117

Printed in the United States of America

Contents

At Issue

Are Privacy Rights Being Violated?

Stuart A. Kallen, *Book Editor*

Bruce Glassman, *Vice President*
Bonnie Szumski, *Publisher*
Helen Cothran, *Managing Editor*

GREENHAVEN PRESS
An imprint of Thomson Gale, a part of The Thomson Corporation

THOMSON
GALE

Detroit • New York • San Francisco • San Diego • New Haven, Conn.
Waterville, Maine • London • Munich

For more information, contact
Greenhaven Press
27500 Drake Rd.
Farmington Hills, MI 48331-3535
Or you can visit our Internet site at http://www.gale.com

LIBRARY OF CONGRESS CATALOGING-IN-PUBLICATION DATA

Are privacy rights being violated? / Stuart A. Kallen, book editor.
p. cm. — (At issue)
Includes bibliographical references and index.
ISBN 0-7377-2360-2 (lib. : alk. paper) — ISBN 0-7377-2361-0 (pbk. : alk. paper)
1. Privacy, Right of—United States. I. Kallen, Stuart A., 1955– . II. At issue (San Diego, Calif.)
KF1262.A97 2006
342.7308'58—dc22 2005045117

Printed in the United States of America

Contents

Introduction

English author George Orwell wrote his novel *1984* in the years following World War II. The book envisions a society dominated by a totalitarian government, known as "Big Brother," that monitors peoples' every move through television-like screens in homes, offices, and businesses. Citizens have no privacy and expect none as ubiquitous posters remind them that "Big Brother is watching you."

When Orwell published his novel in 1949, technology was much less advanced than it is today. There were no surveillance cameras on street corners or supercomputers analyzing billions of credit card transactions. More than fifty-five years later, however, some privacy rights advocates argue that the world depicted in *1984* has come to pass. As author Richard A. Glenn explains in *The Right to Privacy: Rights and Liberties Under the Law:*

> Closed-circuit TVs scrutinize activities in supermarkets, shopping malls, workplaces, and along city streets. Traffic monitoring systems record the whereabouts of automobiles. Wireless communications technology can pinpoint the location of cellular phones. Electronic communications systems generate information about an individual's credit-card purchases and Internet browsing habits. Computer technology provides the means for central storage of and easy accessibility to massive amounts of data, making information collection much easier. And the Internet . . . facilitates the unprecedented and rapid dissemination of stored information.

The development of technologies such as those described above has led to many limitations on privacy in the United States. Police can use video cameras to monitor people walking down a city street—or record the actions of people protesting at a demonstration. Banks, convenience stores, and other businesses have the right to use video surveillance cameras to record the comings and goings of customers. Businesses can also collect credit information, records of purchases, Social Se-

curity numbers, and other financial data about customers. Furthermore, there are few restrictions on the rights of businesses to monitor their employees in the workplace. A 2000 study of human resources professionals at more than seven hundred companies revealed that 74 percent of employers monitor workers' Internet use at work; 72 percent check their employees' e-mails; and 51 percent review employees' phone calls.

Even as modern technologies encroach on personal privacy in dozens of ways, many Americans still value their right to be left alone. According to an August 2002 survey by the First Amendment Center, 81 percent of those polled reported that the right to privacy was "essential." People are particularly concerned about protecting their privacy because of the rise of identity theft, in which a criminal steals personal identification information—such as an individual's Social Security number or credit card account codes—in order to commit a crime such as obtaining a loan or mortgage or even filing a bankruptcy claim in that person's name. CBSNews.com reported that in 2005 alone, more than five hundred thousand Americans would become the victims of identity theft and that more than $4 billion would be stolen in their names. According to experts it can take anywhere from six months to two years for victims to sort out the financial havoc created by identity thieves.

Given the risks of identity theft, some Americans are wary of even legitimate businesses violating their privacy rights. For example, in a 2002 report to Congress the Federal Trade Commission (FTC) cited a poll showing that 92 percent of respondents from households with Internet access stated that they do not trust online companies to keep their personal information confidential. This lack of trust is estimated by the FTC to cost online retailers as much as $18 billion in lost sales annually.

While many Americans are highly concerned about invasions of privacy, some argue that reports that privacy is dying are highly exaggerated. Amitai Etzioni, the author of *The Limits of Privacy*, writes that although it is not difficult to find U.S. opinion polls that support the argument that Americans fear their privacy rights are in grave danger, these polls ask "cost-free" questions such as whether or not people would like stronger laws to protect their privacy. Etzioni argues that such questions are "like asking if you want more fresh air, good movies, or better government—with no additional effort or expenditure on your part. The only surprise here is that anybody demurs." He states that Americans reveal the true extent of their

concern about privacy rights when they are asked to make an effort to protect them. For example, he notes that when people were asked whether they checked the privacy policy of the health and medical Web sites they visited, only one in four claimed they did "despite the fact that medical privacy concerns the most personal information of all." Further, he found that about 80 percent of Americans polled said they were willing to reveal personal information in order to obtain a small discount.

Privacy researcher Alan Westin has also found that the majority of Americans are not deeply worried about the possibility of their privacy rights being violated. He divides the American public into three categories: privacy advocates, who possess very high privacy concerns; privacy pragmatists, who are willing to forgo some privacy for shopping convenience; and the privacy unconcerned, who have little to no concern about privacy issues. According to Westin's research, 125 million Americans make up the privacy pragmatist category, and another 45 million comprises the privacy unconcerned group. The number of people in these two groups combined is nearly three times the 57 million Americans in the privacy advocate group.

Some researchers believe that people who are apparently unconcerned about privacy violations feel this way because they do not understand the extent of the legal rights enjoyed by the government and businesses to gather information about citizens. Communications expert Oscar Gandy has found that the more people read or hear about the potential use and abuse of computerized information, the more worried they become about privacy violations and the less they trust organizations that collect information about consumers.

Although it may be difficult to gauge the extent of people's concern and knowledge about privacy rights, it is certain that as technology continues to develop, new products will be devised that could make Americans more vulnerable to privacy violations. On the other hand, many new devices that protect privacy, such as sophisticated encryption systems for computers, are also being developed. In addition, more laws and regulations are being put in place to protect privacy. It is therefore unclear whether the future will bring greater protection of people's personal information or an erosion of privacy rights. The authors in *At Issue: Are Privacy Rights Being Violated?* explore the current debate over privacy rights and some of the trends that will affect future debate.

1

Companies Use Computer Spyware to Steal Personal Data

Matthew Callan

Matthew Callan writes for the online magazines, or "zines," Scratchbomb.com and Freezerbox.com. He is currently working on his first novel, Breaking My Shoes.

One of the newest tools that advertisers can use to violate a person's privacy rights is known as spyware. This software is secretly bundled with freeware available on the Internet. When users download the freeware, they also unknowingly download spyware that records users' Web browsing habits and software preferences. The information is transmitted to advertisers who then bombard the victims with an endless array of annoying pop-up ads. Only the most competent computer users can detect and delete spyware once it finds its way onto a hard drive. With few legal limits on this activity, the privacy of computer users is under attack by unprincipled advertisers who will stop at nothing to steal personal information to make a profit.

Though we have been firmly entrenched in the information age for almost 20 years now, the Internet still retains a Wild West atmosphere, without a Wyatt Earp to tame it. Rules are made and discarded at will, virtue a dead end, pimping a virtue. You must get yours before the next guy grabs it, any way you can, and there are plenty of sharpies promising an edge, bottles

Matthew Callan, "Spyware: How Your Personal Data Gets Stolen Online," *Alternet*, February 8, 2002.

of snake oil in hand labeled DRINK ME.

Witness the latest con, spyware, software that is able to swipe personal data from your computer and sell it to the highest bidder. All this is done under the guise of collecting general demographics and providing users with exciting offers, but its potential is far too frightening to ignore.

Spyware usually comes to your computer in the form of a simple data-collection program, bundled along with a piece of freeware (an application that the developer offers to the public gratis) that contains embedded banner ads. As you use the application, the spyware takes the personal information you provided when registering and adds to it other appliction-related data; what you are using the application for, how long you use it, etc. This information is sent to a server that interprets the data in order to target you with very specific advertising.

> *"A program you never wanted squats in your computer's hard drive, sending personal information to a company with whom you never had any direct contact and never agreed to give such access."*

Rotating banner ads are like airport surveys: If you want to ignore them, you can. And since most freeware relies on advertising dollars to pay the bills, this may seem a fair price to pay for a programmer's labor (and the reason why these programs are often referred to more benignly as adware). However, there are troubling aspects to this practice; some potential, some already in play.

First of all, users are rarely notified of the presence of any spyware when they download; if so, only in the glaucoma-inducing lines of tiny text that make up a User Agreement. More often than not, spyware is not administered by the company from which users receive the application, but by a third party that markets the spyware. So while you may have agreed to the terms and conditions set forth by the application's developers, you did not specifically agree to anything the spyware's administrator has in store for you. Under current laws, this is all perfectly kosher. Software providers are under no legal obligation to inform the public of their purpose in gather-

ing personal information, let alone how they do it and with whom. Most sites do disclose some information about what software you receive and what it does, merely to give lip service to privacy concerns, knowing full well that their security policies have the same judicial weight as handshake agreements.

Pop-Ups Appear Incessantly

So it was only a matter of time until a program such as VX2 would hit the Web, and hit it hard. VX2 takes spyware to a new level by pulling information, not just from use of an application, but from the use of a computer. When freeware that includes VX2 is installed on a computer, the program saves itself to a directory on the hard drive. Once firmly in place, it keeps track of the user's Web browsing (current and historical), information entered into forms, and configuration of the user's hardware and software. Based on all this information, pop-up ads begin to appear incessantly in the user's Web browser, giving the false impression that the Web page being viewed is responsible for the constant annoyances.

In order to discover that VX2 is on your computer, you would have to determine the IP [identifier number of the computer] of the pop-up ads plaguing your browser, a task that less technically-inclined Web surfers are not able to do. Even harder to determine is how VX2 got on your computer, and where it is stored. To top it all off, VX2 is an incredibly difficult program to completely remove from a hard drive, and doing so often disables the freeware that let it in.

> *"Many companies offering freeware attach [spyware] to their software willy-nilly, presumably under the spell of sleazy marketers."*

Even more disturbing information can be culled from the VX2's Privacy Policy, as featured on its Web site. Although VX2 insists that it does not collect any truly damaging data (i.e., credit card information), it does concede that "the operation of certain third party websites may result in some personal information being included in URL data. . . . Such instances are rare and are the result of poor security practices by these third party

websites." Thereby, the buck is passed when some mysterious charges suddenly appear on your Visa bill. VX2 also reserves the right to update its software at any time, saying that "upgrades may include third party applications. . . . They will be done automatically in the background while you are surfing the web in order to cause the least amount of inconvenience to our users as possible." Its stated reason for capturing data that the user enters into forms (which includes even secure, encrypted forms) goes past disingenuousness and straight into Orwell country: "This information is automatically sent to VX2 in order to save you the time and trouble of submitting such information to us yourself."

What VX2 boils down to is this: A program you never wanted squats in your computer's hard drive, sending personal information to a company with whom you never had any direct contact and never agreed to give such access; a program that, furthermore, can upgrade itself and add any other program to your computer that it sees fit. It is the kind of application that would make the CIA drool, but once again, private industry has beaten the public sector to the punch.

Guilty Firms Deny Responsibility

It is difficult to determine which applications are or have been bundled with VX2, due to the frequency of freeware updates and the program's inherently insidious nature. Companies that use VX2 are obviously tight lipped about it; companies who no longer use it, but once did, are in no rush to inform users that they were being spied on. Because of the nature of VX2's operation, however, these once-guilty firms still have a responsibility to inform their users. This spyware embeds itself into a user's hard drive; therefore, the application once bundled with VX2 does not even have to be running for it to gather information and send it to an ad server. Even if a company no longer maintains a relationship with VX2, unless it alerts its users to VX2's existence, and how to effectively delete it from their hard drive, the program will continue to do its dirty work. By keeping quiet, under the guise of not alarming their users, these firms remain co-conspirators in VX2's quest to snoop on the Web-browsing public.

The most popular application known to have used VX2 is the Audio Galaxy Satellite, a music-downloading application similar to Napster. Portal of Evil, a Web site that collects pages

"from the margins of society," and one of the first sites to break the whole sordid VX2 story, has attempted to make Audio Galaxy accountable for bundling VX2 along with their Satellite freeware. In responses to both Portal of Evil and Wired.com, Audio Galaxy merely stated that VX2 was no longer included with their freeware, refusing to state when it was and for how long. The company said it had little knowledge of the program's use and blamed its presence in their software on Onflow, a software company that supplied Audio Galaxy with advertising graphics enhancers. Onflow maintains that it had never heard of VX2 until it was alerted by Portal of Evil.

Ignorance is a poor excuse for what companies such as Audio Galaxy have unleashed on the Web. What is now crystal clear is this: many companies offering freeware attach add-ons to their software willy-nilly, presumably under the spell of sleazy marketers, not knowing or not caring what this software will do to its users. . . . (Audio Galaxy did not respond to this writer's request for comment.)

The origins of the program are incredibly murky, and fraught with . . . secrecy. . . . No one has ever taken responsibility for writing the code (or funding such). As is often the case with such spyware, the program was probably developed and tested by a third-party tech department far removed from whoever wields it now, and then funneled through several different subsidiaries of a large parent company, in order to throw any curious bloodhounds off the scent. . . .

Thanks to the venal efforts of these people, the Web remains a lawless place huddled on the edge of civilization, full of mustache twirling barkers who cruise for those easy marks just off the stagecoach. And since times are tighter these days, the stakes are higher, the con jobs meaner, the medicine show a lot less funny. In the current political climate, anything that threatens our privacy deserves a long hard look, and a long hard fight. Until a sheriff finally arrives—until everyone realizes how much we stand to lose and how soon it will happen—we must get used to the hustler's hello: one hand slapping us in the back and the other one reaching into our pockets.

Incidentally, VX2 happens to share a name with a component of a variety of nerve agent. This brand of biological weapon is ten times more powerful than other nerve agents, and is characterized by its oily texture and long half-life. Whether the spyware's nomenclature was a loving tribute or a dark coincidence remains to be seen.