

# THE PLAYBOY FORUM

## IS JOHN DOE DEAD?

WITH THE LOSS OF OUR ANONYMITY COMES  
THE LOSS OF OUR FREEDOM

BY DANIEL J. SOLOVE

**D**o Americans still have the right to privacy? Some people don't think so. "In our interconnected and wireless world," says Donald Kerr, director of the National Reconnaissance Office, "anonymity is quickly becoming a thing of the past." Kerr, one of the nation's highest-ranking security officials, made this comment in a speech at an intelligence conference in San Antonio this past October. "Protecting anonymity isn't a fight that can be won," he said. "Anyone who's typed in their name on Google understands that. Younger generations have a very different idea of what is essential privacy, what they would wish to protect about their lives and affairs."

We have long cherished the ability to go about our life without anyone monitoring our activities. But Kerr wants us to be realistic: Technology is eroding privacy, and we should accept that we now live in a fishbowl. There are more than 30 million surveillance cameras in the U.S. Businesses collect torrents of personal information about what we buy, where we travel, what movies and TV shows we watch and which books we read. The government sweeps up this data, feeds it into gigantic databases and analyzes it for patterns of behavior it deems suspicious.

Members of the generation growing up today expose intimate details about every facet of their life on blogs and social-networking websites. They don't seem to expect privacy anymore. They expect to be watched, recorded, tracked and profiled. They expect details of their life to be posted online for the world to see. "You already have zero privacy," Scott McNealy, chairman of Sun Microsystems, once declared. "Get over it."

But this is wrong. If you accept these defeatist views, you play into the hands of those who aim to encroach upon our privacy. The government and businesses want us to give up the fight. This is precisely why we have to strive harder to protect our privacy. We should do so not because people expect to have privacy but because they



may not. As technology makes it easier to capture and spread information, people will, of course, expect less privacy. The important question is not whether we expect privacy but whether we desire it. We protect it because it is something we want, not because it is something we already expect.

Kerr recommends we protect privacy with oversight committees and privacy boards, but we already have many of both within government agencies that purportedly safeguard our privacy and civil liberties. These committees and boards have little power. Many don't even report to the public, so they rarely bring greater openness to government. They act as little more than advisors.

Can we protect our privacy today in a meaningful way? Yes, but first we must stop blaming technology. Technology alone

doesn't destroy privacy; those who use technology do. Those who collect and use our personal information don't want to be regulated. They don't want to be limited, and they sure don't want to be held accountable. Arguments that we have to sacrifice privacy in the name of security or economic efficiency are often attempts to be allowed to gather and use our personal information with even less oversight and accountability.

We can regulate how our information is collected, used and disclosed. Despite the rapidly growing number of surveillance cameras, we have hardly any rules about how they may be used, how long the information should be stored and with whom the video footage can be shared. The laws intended to control the government's increasing access to our personal information held by businesses are weak and riddled with gaps and loopholes.

When it comes to companies collecting and using our information, the law is also ineffective. In only a few contexts does the law provide protection. Federal law prohibits video stores from disclosing your rental information, but bookstores, websites and countless other businesses are not

# PROFILING FOR PROFIT

IT'S NO SURPRISE FACEBOOK IS  
SELLING YOUR SECRETS

limited at all. They can do virtually anything they want with your information.

One problem holding back the law today is that it labors under impoverished understandings of privacy. Many view the concept in a binary way: Information is either private or public. Under this standard, if something occurs in public or is no longer hidden, it cannot be private. But this understanding of privacy is wrong. One of the most important dimensions of our privacy is anonymity, which Kerr claims is a thing of the past. We often take our anonymity for granted in daily life. The people we encounter in many public places will often not know us, not care about what we're doing or remember who we are.

But if our photograph can be taken at any time, if we're tracked and monitored by the surveillance cameras watching over us, if computers constantly collect and analyze our personal data, then our anonymity disappears. And with it goes a large dimension of our freedom. We won't be able to act without fearing how our information may be judged by a government bureaucrat or how new pieces of data may affect our profiles in large databases.

Gone too will be the ability to have a second chance and a fresh start. America has always been a place of new opportunities, where people can escape the errors of their past and start anew. But if all our mistakes and minor transgressions are preserved forever online or in dossiers maintained by companies and the government, we will remain chained to our past. We will become less free.

The current state of affairs is avoidable. Government and businesses can use our information with little oversight or limitation not because of technology but because the law doesn't regulate them sufficiently. We can restrict the information businesses and the government gather about us. We can limit how they use it, and we can require them to delete it after a period of time. When facing growing threats to our privacy, we should not react by throwing up our hands and saying we must get used to living in a fishbowl. Instead, we should vigorously work to achieve the privacy we want.

The loss of privacy is not inevitable. We have a choice. We can protect our privacy, or we can give it up. If we lose it, we should blame ourselves. We will have lost our privacy because we made no effort to protect it.

*Daniel J. Solove is associate professor at the George Washington University Law School and author of *The Future of Reputation: Gossip, Rumor and Privacy on the Internet*.*



By Andrew Hultkrans

**T**his past November Facebook founder Mark Zuckerberg (pictured above) regaled an audience of New York City advertising execs with bold visions of a marketing revolution. He called it Social Ads, and its battle standard was displayed on a screen behind him: **TARGET EXACTLY THE AUDIENCE YOU WANT.**

Barely out of the Clearasil demographic at the age of 23, Zuckerberg made the type of paradigm-smashing claims familiar to anyone who has attended a Silicon Valley launch. Before Facebook Social Ads, he implied, marketers were hapless Cro-Magnons, blindly rooting around in darkened caves for a stray piece of flint. Now they would be advanced anthropologists, surfing Facebook's "social graph," as he put it, receiving "trusted referrals" from Facebook users and gaining "valuable metrics"—"the exact mind share" their brand is getting, no less—in the form of "data on activity, fan demographics, ad performance and trends."

"This is some really powerful stuff," Zuckerberg said, "and nothing

like this has ever been seen before."

What a difference a month makes on the Internet. By December Zuckerberg and Facebook were reeling after a barrage of editorials, blog rants, a 70,000-strong MoveOn.org petition and the cybersleuthing of Stefan Berteau, a Computer Associates antispyware researcher—all objecting to the deceptive privacy violations of Beacon, a crucial subset of the Social Ads platform.

Beacon was designed to track and report to Facebook the activities of its members on 44 third-party partner websites, including those of Sony, Blockbuster, eBay and *The New York Times*. If users did not notice or prop-

erly click a briefly flashed opt-out window on the third-party site or on Facebook, their activities—from making a purchase to writing a review—were automatically broadcast to their entire Facebook friends network through the already controversial News Feed feature, which had previously transmitted only internal Facebook information. The ostensible "trusted referral"

**IT'S A PARAECONOMY THAT GENERATES MONEY BY GATHERING PERSONAL INFORMATION.**