The New York Times
nytimes.com

January 25, 2006

A Growing Web of Watchers Builds a Surveillance Society

By DAVID SHENK

IT is strangely fitting that President Bush's no-warrant wiretapping came to light during the season of holiday gift buying, much of which took place online.

As Washington huffed and puffed over a new erosion of privacy, untold millions of us clicked just as fast as our little clickers could click through Google ads and Amazon checkout pages, unwittingly updating our "cookie" ID badges at every new screen. We bought our loved ones cellphones with built-in Global Positioning System and flocked to family gatherings in cars loaded with OnStar and EZ Pass. We paid for mostly everything with credit and debit cards. Out of convenience, we embraced technologies meant to track our every move.

There are important distinctions, of course, between government prying and the emerging web of consumer surveillance. But they share a digital universe that facilitates and rewards watching. Spam, spyware and identity theft are only a taste of how exposed we have all willingly become as we enjoy the benefits of the networked world.

If the American public seems a bit confused about the raging debate of security versus civil liberties - Bush/Cheney versus the A.C.L.U. - it may be because the debate itself has been outpaced by technology. In our post-9/11, protowireless world, democracies and free markets are increasingly saturated with prying eyes from governments, corporations and neighbors. For better and worse, free societies are fast entering the world of total surveillance.

On Thursday, it was reported that Google, the leading search engine, is resisting a Justice Department subpoena seeking millions of its users' search records, and we can all be glad Google chose to stand its ground.

Behind that dramatic headline, though, is the amazing story of how much user information Google actually controls, particularly concerning its registered Gmail users. They have quietly consented to extensive e-mail monitoring in return for free e-mail accounts with virtually unlimited online storage. Google's machines - no employees directly read any e-mail - scan all Gmail messages and then tag them with ads relevant to their content. (The message "John: Want to go fishing this weekend?" may attract a "Click here to buy fishing gear" ad.)

Allowing a computer to read your e-mail may not sound threatening, but with advanced pattern-recognition software, scanning many messages over time could produce a powerful consumer profile. As these machines get smarter and smarter, it may soon be far more worrisome to let a machine "read" your information than to have a human reading it. Further, as the Electronic Privacy Information Center has pointed out, at epic.org/privacy/gmail

/faq.html, Google also has the technical and legal ability to archive and scan registered users' Web searches, to cross-reference that data, and, if it likes, to sell it.

Such broad powers will not, of course, be limited to Google for long. As cellphones become primary devices for e-mail, Internet access and shopping, phone-service providers will be able to amass and analyze the correspondence, curiosities and purchases of each user without listening in on a single phone conversation.

You might not even have to send an e-mail message or click on a Web site to set off a close surveillance. Just last week, Apple Computer added to its iTunes software a new MiniStore, which automatically monitors every song you listen to on your computer, and suggests related songs to buy. But after an uproar from privacy advocates, Apple adjusted the software to allow users to opt out of this service .

In coming years, many other objects of popular consumption will root out and transmit our private data. The retail industry is well on its way to including tiny, virtually invisible radio frequency identification tags with every consumer product from underwear to milk cartons to brake pads.

Such RFID tags - consumer watchdogs call them "spy chips" - will improve shipping, stocking and shelving efficiency, and may offer many new conveniences to consumers. Washing machines, for example, could recognize clothing type and make appropriate adjustments; mechanics could instantly know the age of a car part; refrigerators could issue a warning if food has passed a spoilage date. The potential privacy incursions are also impressive. Retail stores could profile customers according to their clothing purchases and adjust in-store advertising and even pricing and credit policies. Consumers would literally be wearing their shopping tendencies on their sleeves.

These are today's tools. What about tomorrow's? The hallmarks of the new digital tool-building age are machines that are increasingly smart, small, cheap and communicative. We are, without question, headed into a world where - mostly by our choice - the minute details of our bodies, lives and homes will be routinely tracked and shared, with potential for more convenience and safety but also abuse.

On the one hand, most of us will trade in our anonymity and privacy for, yes, increased national security and cleaner, healthier, easier lives. On the other hand, we will be more vulnerable - not only to malicious hackers and identity thieves but also to sophisticated marketers. Our increased exposure will demand a much more nuanced definition of what "privacy" means as well as specific new tools to help us navigate its components. Whether the watcher is the National Security Agency, Verizon or the teenager next door, our increased exposure will also require new and broader vigilance.

Sadly, today's fine-print corporate disclaimers do not even come close to being adequate, and proper disclosure is unlikely to come without government action.

But the good news is that there is a simple and elegant standard for all surveillance minders to adopt: citizens have the right to know - in real time - when and how they are being monitored. Just as some states require "all-party consent" for telephone recordings, so it should be with e-mail, Web surfing, walks in the park or any activity being captured by a distant unseen party.

Such disclosures might look like this:

"Welcome to Shop-Mart. Your shoe size is 9."

"All persons entering City Park are subject to video and audio surveillance by the Metropolitan Police Department."

"Thank you for browsing at BooksOnLine

.com, where page views are recorded and attached to your file. Click here if you prefer to browse anonymously."

Sunshine is the only antidote to surveillance, and openness is inherently democratic. Such disclosures allow consumers to react as they wish. And if the snooping is too embarrassing for companies or public officials to acknowledge, their noses shouldn't be there to begin with.

David Shenk, author of "Data Smog," writes often about the unintended consequences of technology.