prototype test that detects 15 genetic variants implicated in eight common health conditions, including diabetes, heart disease, high blood pressure, and lung cancer—all of which can be prevented or delayed by changes in lifestyle. But so far, only about 10 percent of those approached have chosen to take it. "We think they don't see themselves as particularly vulnerable," says Colleen McBride, a scientist at the National Human Genome Research Institute and the study's leader.

If healthy people got interested in genetic testing, they would probably be the group to benefit most. If they were found to be at high risk, they could try to prevent even the first signs of disease. "Right now, we can't get on the radar screen of healthy, young individuals because they don't see themselves as susceptible to diseases that occur later in life," says McBride. But new genetic tests "might be the kick start they need to engage them in the process," she says. "The more personal the risk is, the more likely they are to react to it."

When I first learned about my own risk for diabetes, I began exercising religiously and viewed white flour and sugar with suspicion, with the result that I dropped 30 pounds. Since then, my blood sugar tests have all been normal. As a result, my vigilance waned. That's why I decided to order the test, which is almost as easy as buying a book from Amazon: a credit card and the time to answer a quick questionnaire about family history and other risk factors are all it takes. I sent in my DNA-coated swabs a few weeks ago and am awaiting my results. I realize that I'll need to keep exercising and eating right regardless, but I want to know anyway, partly out of curiosity—a positive result could explain my own lengthy family history of diabetes—and partly because I think that for me, a positive result will provide extra motivation. Every little bit counts. TR

Emily Singer is the biotechnology and life sciences editor of Technology Review.

LAW

The Talk of the Town: You

Rethinking privacy in an immodest age.

By Mark Williams Pontin

Earlier this year, *New York* magazine published a long piece called "Say Everything." Subtitled "Kids, the Internet, and the End of Privacy: The Greatest Generation Gap Since Rock and Roll," the piece breathlessly revealed that about 60 percent of modern American youth already have their biographical details and images online at MySpace, Facebook, YouTube, or similar social-networking websites. *New York*'s reporter made a big deal about how "the kids" made her "feel very, very old." Not only did they casually accept that the record of their lives could be Googled by anyone at any time, but they also tended to think of themselves as having an audience. Some even considered their elders' expectations about privacy to be a weird, old-fogey thing—a narcissistic hang-up. One teenage girl was asked about cases in which sexual material featuring girls her own age had been posted on the Internet without the subjects' permission. "It's either documented online for other people to see or it's not, but either way you're still doing it," the girl replied. "So my philosophy is why hide it?"

THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET
By Daniel J. Solove
Yale University Press, 2007, $24.00

Some prominent technologists have arrived at roughly the same conclusion—if a little more reluctantly. As Sun Microsystems chairman Scott McNealy put it in 1999, "You have zero privacy anyway. Get over it." The view that surveillance is already ubiquitous led David Brin to argue, in his 1998 book *The Transparent Society*, that our only real choice is between a society that offers the illusion of privacy, by restricting the power of surveillance to those in power, and one where the masses have it too. Brin prefers the latter.

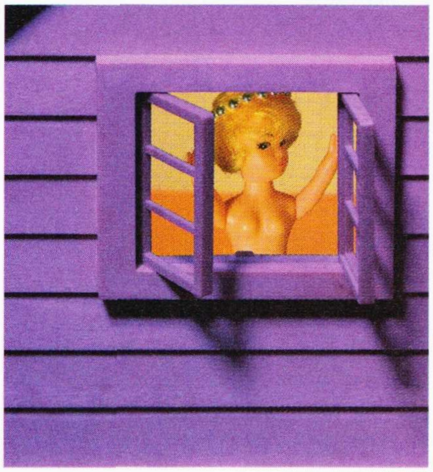
If we don't like that conclusion, we may gravitate to the opposite pole: the absolutism of organizations like the Electronic Privacy Information Center, the Electronic Frontier Foundation, and the ACLU, which tend to construe any collection and analysis of personal data by government agencies (and to a lesser extent by corporations) as potentially violating the U.S. Constitution's Fourth Amendment guarantee of citizens' rights "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

But these two positions may feel, even to their proponents, more theoretical than practicable. Happily, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet*, by Daniel J. Solove, associate professor of law at the George Washington University Law School, offers alternatives.

The book isn't much concerned with privacy advocates' usual bête noire, the surveillance state. Instead, Solove focuses on a more down-to-earth set of concerns. Nowadays, thanks to Marshall McLuhan, we're accustomed to talking about the "global village." But traditionally, in villages, everybody knew everybody else's business; personal privacy and anonymity are social constructs that achieved their current legitimacy when increasing numbers of people started moving to cities in the 18th and 19th centuries. Nonetheless, privacy remains simply, as Columbia University professor emeritus of public law Alan F. Westin has phrased it, "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." That claim had far less authority in the smaller communities in which most people once lived, and those communities had greater power to enforce social norms by enhancing or destroying reputations. In 1910, writer John Jay Chapman testified eloquently to the extent of that power: "If a man can resist the influences of his townsfolk, if he can cut free from the tyranny of neighborhood gossip, the world has no terrors for him; there is no second inquisition."

And yet, as Solove points out, the current state of the Internet allows townsfolk to be nearly lethal. For one example of the inquisitorial possibilities presented by the digital global village, he suggests, consider the young woman who let her small dog crap on the floor of a South Korean subway train in 2005 and then ignored other passengers who told her to clean up the mess. Somebody took pictures and posted them on a blog. Within hours, the photos were on dozens of other blogs; within days, the young woman had been identified, the story had reached Korea's mainstream media, and millions knew her as gae-ttong-nyue, or "dog poop girl." In response, she dropped out of her university.

Or take the case of Jessica Cutler, a junior staffer for a U.S. senator, who began blogging in 2004 as the Washingtonienne. According to Solove, Cutler's blog "described daily adventures ... which consisted of a lot of partying with various men." The blog featured a revolving cast of a half-dozen of these, and Cutler wrote sexually graphic commentary about her exploits with them. A much-read Beltway gossip blog called Wonkette soon linked to Cutler. The resulting notoriety got Cutler fired, but it also attracted the likes of the *Washington Post*, the *New York Times*, and CNN, and earned her a $300,000 book contract and a *Playboy* photo shoot. Things went less swimmingly, Solove observes, for one of Cutler's former boyfriends, a DC lawyer, who'd had no idea that her accounts of their trysts had been appearing on the Internet. Cutler had used his initials and mentioned that he worked for the same senator that she did, making his identity–and his spanking fetish–quite clear. "RS" left his job and launched suits against Cutler for invasion of privacy. The wrangling is being watched by privacy groups for the precedents it may establish about whether bloggers are obligated to protect the privacy of those they discuss. Solove points out that balancing the right to privacy against the First Amendment's guarantee of free speech has always been problematic; Cutler's case, however amusing, shows that the Internet has made that dilemma even more acute.



ROBERT JONES/ARCANGEL IMAGES

Solove describes the spectrum of sites set up to tarnish reputations. At the lighter end is Bitterwaitress.com, with its searchable "Shitty Tipper Database," which contains alleged culprits' names and their rankings as cheapskates. Sites such as Don't Date Him Girl have greater potential to harm the people they profile. And on the dark end of the spectrum are fringe sites like the Nuremberg Files, which profiles doctors who perform abortions. Until it was forced to stop doing so, it listed those wounded by antiabortion activists in gray type and put a line through the names of those who'd been killed.

Solove sees an expanded role for law here, but he disapproves of authoritarian legislation that attempts to ban specific kinds of speech or activity. He also thinks that although people who feel abused online can and should have recourse to tort, defamation, and privacy law, each of these areas needs reconsideration. Before being allowed to proceed with litigation, he suggests, plaintiffs could be compelled to prove, first, that they sought redress outside court, and second, either that the defendants refused to remove harmful material or that the damage done was severe and irreparable.

Beneath Solove's legal suggestions rests a keen insight about the extent to which the Internet changes basic questions about privacy. Traditionally, Solove reminds us, the law's view of privacy has been binary: if somebody is filmed in public, that person is deemed to have had no reasonable expectation of privacy; anyone who really wanted privacy, the law generally says, should have stayed home. Similarly, if somebody communicates confidential information–that he's HIV-positive, say–to a trusted circle of 50-odd acquaintances, and one of them then conveys the facts beyond that circle, the law makes it difficult to sue for breach of confidentiality. Solove believes it should be harder for someone to betray trust in that kind of situation, and he proposes using social-network theory, which analyzes social relationships in terms of nodes (individual actors within a network) and ties (the relationships between those actors), to determine when a reasonable expectation of privacy exists.

Solove's proposals in *The Future of Reputation*, if tried, might work or fail. They have the virtue, at least, of giving us something to think about beyond the old binary view of privacy, which is too blunt and dysfunctional to address privacy in the Internet era. TR

Mark Williams is a Technology Review *contributing editor.*