Who HOLDS THE KEY *to Your* INTERNET PRIVACY?

For those seeking privacy in their daily lives, it's no longer enough just to keep the blinds closed. Our most personal information is now just a "tweet" away from being laid out for the world to see. ~ Sometimes hidden behind flimsy password protection or limited to easily compromised friend networks, details about people's personal lives are floating around in cyberspace. Many fail to stop and think about the loss of privacy that comes with creating an online persona. ~ The consequences of sharing too much too casually about our everyday lives was driven home by the Web site PleaseRobMe.com. The site uses the public information provided by Internet users on services such as Twitter (where people post 140-character "tweets" about what they're doing or thinking) to reveal who is not home and thus easy robbery targets. ~ The site's goal is not to assist actual robbers, but to "raise some awareness on this issue and have people think about how they use services" that allow them to share information that is normally kept private. ~ Think this is only a problem for those who choose to broadcast their personal information to the world? Think again — your online privacy is probably being compromised in ways you don't even know about.

By Brittney Pescatore '07
Illustrations By Harry Campbell

THE WILD, WILD WEB

According to a survey conducted in December 2009 by the Pew Internet and American Life Project, 74 percent of Americans use the Internet. Each time they log on, they find themselves in an online world that Rebecca Hulse, an adjunct professor in media law and privacy at William and Mary School of Law, likens to the "Wild West."

"Initially, the Internet was conceived as an open, free-flowing space, where people weren't confined or constrained by real world barriers," says Hulse. "People's laws weren't supposed to matter."

There is more information flowing on the Web than ever before, but the lawless nature of cyberspace has privacy advocates on edge. The movement to gain more Internet privacy, which most take to mean control over who sees our personal information on the Web and what can be done with that information, has led advocates and consumers to increasingly put pressure on major Web companies to respond to their privacy concerns.

Google is one Web company that has been a major player in discussions of Internet privacy.

Jane Church Horvath '86, Google's global privacy counsel, says the company tries to operate by three bedrock privacy principles: "transparency, choice and security."

Not only does Google have information about what people search, it has e-mails from the more than 100 million people who use Gmail; it has documents from those who do their business via Google Docs; and it even knows the exact location at any given time of a person using its new "Latitude" application for mobile devices, which allows you to share your location with your friends.

William and Mary will be jumping on the Gmail bandwagon soon, abandoning its overburdened student Webmail system for an e-mail program knows as "Google Apps Domain," which is similar to a standard Gmail account but comes with more student-geared features, such as document storage and a calendar.

With so much private information in its servers, it makes sense that Google would have a few people working around the clock to deal with the privacy issues that arise.

Alumna Jane Horvath brings an extensive background in privacy and technology law to the company. After graduating from the University of Virginia Law School, she went on to work for the technology practice at a major Washington, D.C., law firm and then worked in-house for AOL beginning in 1995. For several years she worked at Privacy Laws and Business, a privacy consulting firm.

In 2006, she became the first chief privacy and civil liberties officer for the Department of Justice. At the DOJ, Horvath was tasked with protecting the privacy and civil liberties of the American people by reviewing and overseeing the department's privacy operations and ensuring its privacy compliance. A year later, she went to Google, where she works to ensure that privacy is built into the company's products.

Google recently launched its own social networking feature called "Google Buzz." The application immediately drew criticism from privacy advocates for its built-in network, which revealed users' frequent contacts to the world. Google allows users to hide that information with a click of a button and, in response to complaints, quickly made changes to make its privacy controls easier to find.

"Social networking is all about uploading information and there have been tremendous user controls built in," says Horvath.

Until Buzz landed on the scene, the social networking privacy concerns were focused on sites like Facebook.com.

There are more than 400 million people on Facebook. Thirty-five million of those users update their "status" every day, which allows them to communicate what they're doing or how they're feeling to their friends. There are more than 3 billion photos uploaded to the site each month. While Facebook has made many efforts to keep up with the privacy concerns of its users, often encouraging users to take advantage of the privacy control options on the site, many still have concerns about the massive amount of personal information that the site makes publicly available.

Adam Rosenberg, the new media manager for the Center for Democracy and Technology (CDT), notes that using any of Google's or Facebook's products, or those of any other Web company, is bound to put privacy at risk. The more information we put into the Internet, the more the threat to our privacy grows, he says.

"People put more and more things online without thinking about what they're putting online," says Horvath. "They need to recognize it's up to them to limit who views their information if they can."

REAL CONCERNS FOR REAL PEOPLE

Internet users may not always have that ability, however. Some of the online activity that we never expect to be shared with anyone can find its way into the public eye.

The issue came into the spotlight in August 2006, when three months' worth of search histories by several hundred thousand America Online users were released to the public. While AOL apologized for the release, saying it was not authorized, the event demonstrated just how much a few months of search history could tell about a person. The *New York Times* provided an example in its August 2006 story about Thelma Arnold, a 62-year-old widow from Georgia who was easily identifiable from her search history, which included queries for landscapers in her hometown and searches for information on a "dog that urinates on everything."

> "People put more and more things online without thinking about what they're putting online. They need to recognize it's up to them to limit who views their information."

The *Times* didn't have to do much investigating to determine that AOL user 4417749 was Ms. Arnold. AOL apologized specifically to Arnold but admitted that there was not much else they could do once the searches had leaked. Whether it's geographic cues or unique interests, most people have search histories that could easily reveal who they are and where they live.

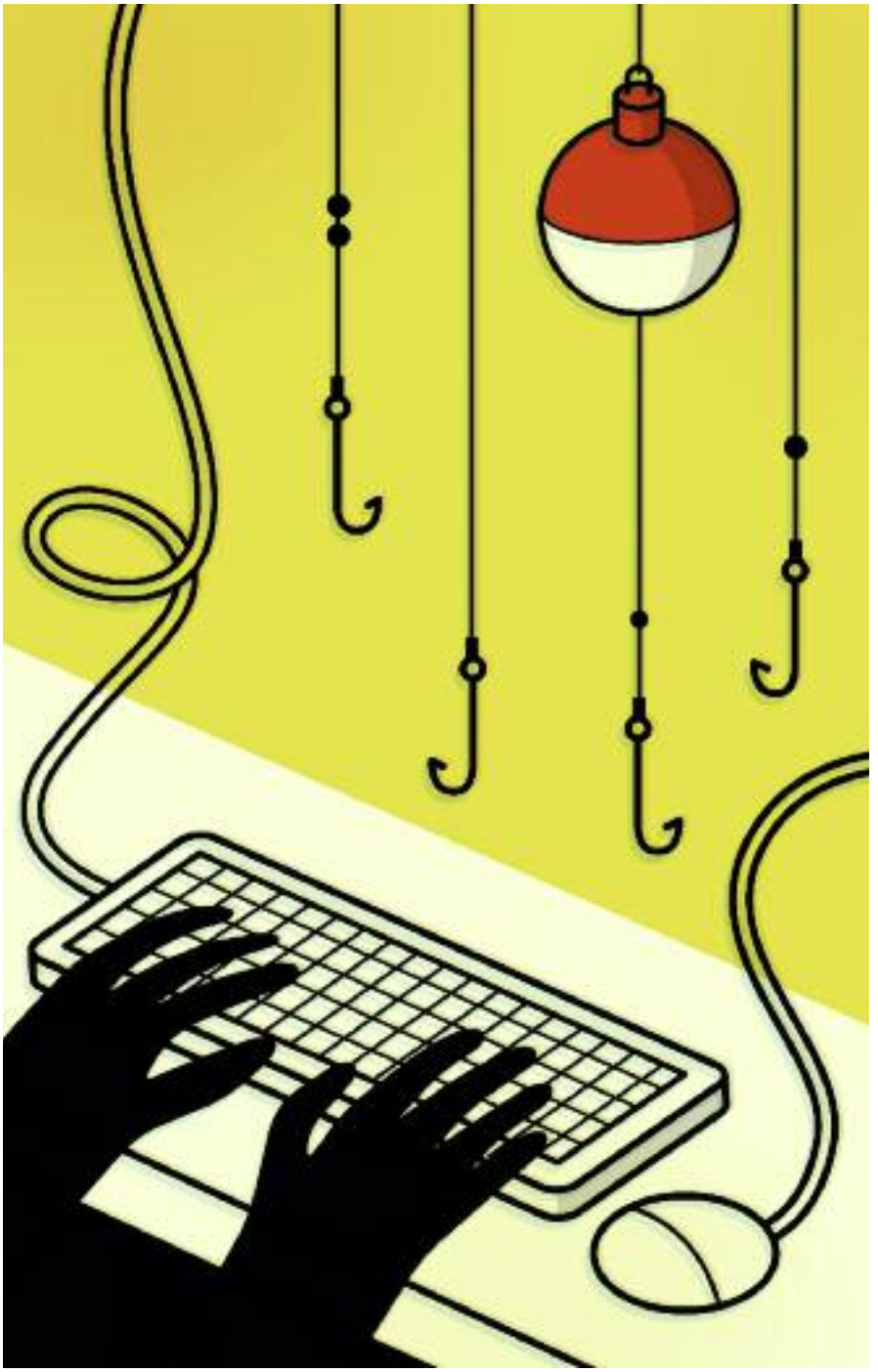
Rebecca Jeschke of the Electronic Frontier Foundation (EFF) notes that it was only recently that Google stopped permanently storing records of every search inquiry ever entered. Storing such data allows Google to improve search quality, but it has raised red flags among privacy advocates. Google now seeks to strike a balance by dumping personal search data after nine months.

Google and other Web companies also seek to balance privacy concerns with innovation opportunities in advertising.

"I don't think most people realize that if they sign up for a Gmail

account, their e-mails are mined for possible advertising uses," says Professor Hulse. She asserts that "behavioral advertising" is "a huge and misunderstood problem."

Behavioral advertising refers to the process of targeting ads to specific consumers based on their online behavior. For instance, someone who recently visited a lot of Web sites about the Bahamas might later find an advertisement for hotels in the Caribbean while on a Web site for something completely unrelated. The benefit of this kind of advertising technology is obvious; it ensures that advertisers are reaching relevant audiences and thus makes advertising more effective. Privacy advocates are concerned, however, about information collected on browsing histories and search queries.



But William and Mary students won't be as susceptible to these same privacy risks because their accounts won't have advertising.

"One of the deals that we make with Google as part of this process is that there will be no advertising for students," says Chris Ward, the director of systems and support for the information technology department (IT) at the College.

While W&M students won't have to worry about their e-mail content influencing what advertisements they see, they still deal with a host of privacy concerns related to their everyday Internet usage.

Maya Horowitz '10 got a glimpse of how easily personal data can be misappropriated in cyberspace when she discovered an innocent picture of high school friends, taken at her 16th birthday party, being used to promote a pornographic Web site.

"The nature of the picture — two of my friends on my bed making mock kissy faces with their tongues out — was pretty tame," says Horowitz. "It wasn't 'Girls Gone Wild' or anything."

Horowitz says she suspects the porn site got hold of the pictures through a public album on an online photo sharing Web site, Webshots.

"I was not aware that this sort of thing could happen, but in retrospect, I should have been," she says. She recalled that several of her classmates in high school had been suspended for drug- or alcohol-related pictures being brought to the attention of school administrators.

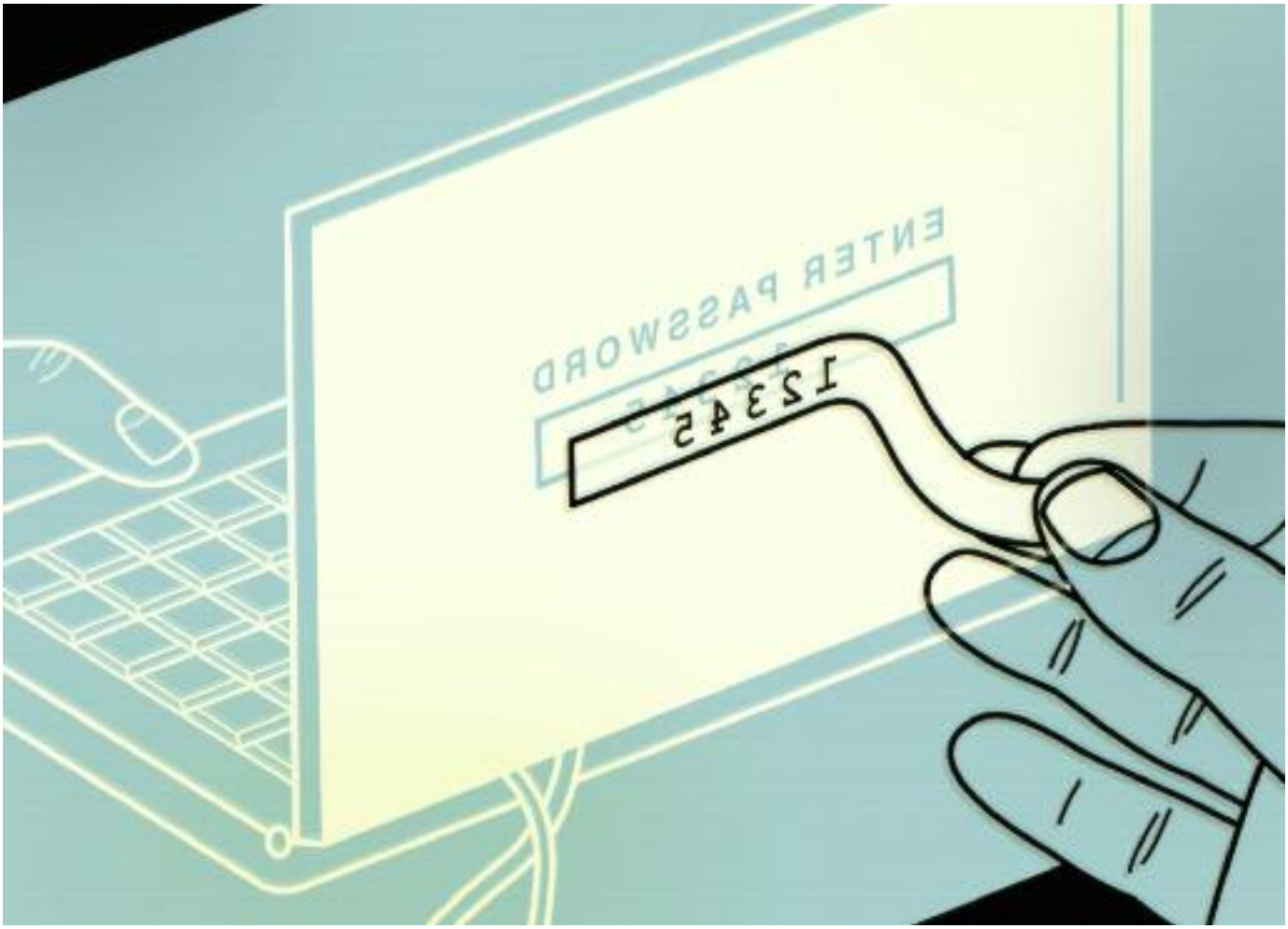
Her experience finding her friends' photos being used without their knowledge has stuck with her. She says she keeps careful watch on her privacy settings, but it's not something she constantly worries about.

Horowitz and her friends had no idea when they were posting photos online that there was the risk those photos could be misappropriated in that way. Thelma Arnold certainly didn't know when she was typing queries into a search engine that she was risking revealing that information to the rest of the world. The question facing Internet users like Horowitz and Arnold is, what can they do about it?

THE KEY HOLDERS

"Private businesses hold the key," according to Professor Hulse. Online privacy reform is most likely to come not from Congress or the Federal Trade Commission, but from the companies that have the ability to exploit our private information. Major Web companies like Google, Facebook, Amazon.com, eBay and others are where privacy advocates are currently moving to focus their energy.

Rosenberg, from the CDT, agrees that the future of privacy protection is in the hands of these private companies, but warns that change won't come on its own.



"They're not going to do anything if people don't stand up and get angry," he says.

Horvath recognizes that the burden is on companies like Google.

"It's up to us companies to provide the tools with which users can do that and the transparency so that users can see what they do with their information," she says.

Horvath emphasizes the importance of companies having readable and meaningful privacy policies.

"The privacy policy is a very, very important document," she says, adding that Google has taken the extra step of creating videos that explain the company's privacy policy. She also points to Facebook's efforts on this front, noting that they posted open letters on their homepage to inform users of recent privacy policy changes. Jeschke, of the EFF, also notes Facebook's recent change of its privacy settings as an example of how some companies are becoming more open about the privacy risks that users face when using their sites.

"That sparked a nationwide debate, whether in blogs or newspapers, about what privacy is and what is important and what people need to do to protect themselves," Jeschke says.

Rosenberg thinks that increasing awareness about privacy policies is the first step to real change.

"If people really knew how much of their information could easily be exposed, they'd be really upset," says Rosenberg. "The issue is that people should know about this and they don't."

For example, people may not be aware of the opt-out nature of many sites' privacy settings, which have the more open and invasive settings as default options.

The CDT has also launched a bookmarklet tool as part of its "Take Back Your Privacy" campaign, which allows Internet users to file a consumer privacy complaint with the FTC just by clicking on the button and reporting your concern whenever you are concerned that the Web site you are visiting does not have adequate privacy protections.

While there are increasingly more protective security settings available, there is still some risk that the content people introduce to the Internet will find its way to unwanted eyes. Ultimately, the best defense against privacy invasion is to keep private content off of the Internet altogether.

"It's important to know that if you post something on the Internet for the world to see, you shouldn't be surprised if the world sees it," warns Jeschke.

PRIVACY VERSUS SECURITY

Concerns about controlling our information online merge with concerns about Internet security. Professor Haining Wang, of the William and Mary computer science department, works in the area of network security. When people talk about a Web site's "security," says Wang, they are referring to how well that site is maintained and what sort of security mechanism is being employed. What is required of a site to be deemed "secure" varies depending on the nature of that site.

"If a site is being used for e-commerce, then it should have a strong security protocol," says Wang. But more general-purpose sites, such as the William and Mary Web site, don't require as much because there's no money involved.

Students at the College face many Internet security threats, primarily phishing, which refers to fraudulent attempts to secure private information, such as passwords and credit card numbers, by posing as a legitimate and trustworthy organization. Think of e-mails from a Nigerian prince asking for money so that he can reclaim his throne.

According to IT's Ward, phishing is the biggest security problem his department deals with. Every so often, students will be spammed (sent unsolicited mass e-mails) by someone seeking their account information.

"Invariably, we have one or two people who will respond, and then those people take over their account to spam other people," says Ward.

The IT office keeps careful watch for such phishing problems.

"The risk is that then William and Mary has the potential to be blacklisted by other networks and Internet service providers as a spammer, so it's a real chore for us," says Ward.

This past fall, the dangers of phishing were driven home for thousands of Hotmail e-mail users, whose passwords were leaked to the Internet as the result of a phishing scheme. The experience not only highlighted how private information might be vulnerable to security threats, it also revealed what a poor job some people were doing of guarding their online security. The leak demonstrated that the most popular password was the highly unoriginal "12345." The second most popular password? "123456789."

Ultimately, privacy and security risks have something important in common.

"The main risk is the human being itself," says Professor Wang. "Even if you provide a really good security mechanism, people might not be using it right."

Internet privacy, unlikely security, doesn't always involve the fraudulent acquisition of personal information. When we talk about privacy, we're talking about controlling our audience. The danger of the Internet is that what we think is being presented for the eyes of a few may instead be laid before the eyes of many.

ON THE HORIZON

It is hard to tell how protected our privacy will be as we enter the next digital era.

"As new services come up — the next Twitter, the next Facebook — hopefully privacy protective technologies will be engineered in," says the EFF's Jeschke. She suggested that companies' desire to get a competitive advantage in the market will motivate such action.

Nonetheless, she noted that we are in a "critical time," where we must start thinking about what aspects of our privacy we are willing to sacrifice in the name of innovation, and what we aren't.

While technology may provide increased ways to protect consumer security, Professor Wang warns that as protections increase, so do the ways companies seeking to exploit your information can use to get around those protections.

"I think there have been some terrific innovations within the last two years in privacy," says Horvath, "and companies are building tools that allow consumers to avail themselves of privacy."

"It comes down to consumer preferences and how much people actually care about privacy online," says Professor Hulse. If Internet users want more privacy, they're going to have to ask for it first. ■

ONLINE SAFETY TIPS

CHECK YOUR DEFAULT PRIVACY SETTINGS.

On social networking sites like Facebook, your default settings may not be as private as you want them to be. Look at your settings and opt out of any public sharing that you are uncomfortable with. "Sites like Facebook now have groups so you can decide what information goes to what person," says Rebecca Jeschke of the Electronic Frontier Foundation. Under the privacy or settings sections of Web sites like Facebook and Gmail, there is usually a drop-down bar somewhere where users can select the audience for certain information, such as their photo albums or their chat availability.

LOOK AT YOUR BROWSER CONTROLS.

Your browser is the service you use to view the Internet — Internet Explorer, Mozilla Firefox, Safari and Chrome are examples of some of the more popular ones. "Chrome allows you to go off the record when you're searching," says Google's Jane Horvath of her company's recently launched Internet browser. Mozilla also lets you enable private browsing, which stops the browser from retaining visited pages, search bar entries, passwords and cookies.

WATCH OUT FOR COOKIES.

Horvath and Hulse both caution that users should be on the lookout for "cookies," which are messages sent from your Web server to your Web browser with certain information such as passwords, addresses, viewing preferences, etc. These can be great in that they provide for a more personalized browsing experience, but there are concerns that some sites might abuse that information. To protect against it, go to the security or privacy settings on your Internet browser and decide if you want to allow certain cookies, all cookies, or no cookies. Adam Rosenberg, from the Center for Democracy and Technology, suggests looking into the "add-ons" available for enhanced privacy and security. These are tools you download to your browser that can do things like track where your information is being sent, block advertisements or automatically delete cookies.