The Web Means the End of Forgetting

Categoría: articulos / Identificación / Identification
Autor: editor
Publicado: 24 Jul, 2010 - 08:30 AM

nytimes.com

July 19, 2010
The Web Means the End of Forgetting
By JEFFREY ROSEN

Four years ago, Stacy Snyder, then a 25-year-old teacher in training at Conestoga Valley High School in Lancaster, Pa., posted a photo on her MySpace page that showed her at a party wearing a pirate hat and drinking from a plastic cup, with the caption "Drunken Pirate." After discovering the page, her supervisor at the high school told her the photo was "unprofessional," and the dean of Millersville University School of Education, where Snyder was enrolled, said she was promoting drinking in virtual view of her under-age students. As a result, days before Snyder's scheduled graduation, the university denied her a teaching degree. Snyder sued, arguing that the university had violated her First Amendment rights by penalizing her for her (perfectly legal) after-hours behavior. But in 2008, a federal district judge rejected the claim, saying that because Snyder was a public employee whose photo didn't relate to matters of public concern, her "Drunken Pirate" post was not protected speech.

When historians of the future look back on the perils of the early digital age, Stacy Snyder may well be an icon. The problem she faced is only one example of a challenge that, in big and small ways, is confronting millions of people around the globe: how best to live our lives in a world where the Internet records everything and forgets nothing — where every online photo, status update, Twitter post and blog entry by and about us can be stored forever. With Web sites like LOL Facebook Moments, which collects and shares embarrassing personal revelations from Facebook users, ill-advised photos and online chatter are coming back to haunt people months or years after the fact. Examples are proliferating daily: there was the 16-year-old British girl who was fired from her office job for complaining on Facebook, "I'm so totally bored!!"; there was the 66-year-old Canadian psychotherapist who tried to enter the United States but was turned away at the border — and barred permanently from visiting the country — after a border guard's Internet search found that the therapist had written an article in a philosophy journal describing his experiments 30 years ago with L.S.D.

According to a recent survey by Microsoft, 75 percent of U.S. recruiters and human-resource professionals report that their companies require them to do online research about candidates, and many use a range of sites when scrutinizing applicants — including search engines, social-networking sites, photo- and video-sharing sites, personal Web sites and blogs, Twitter and online-gaming sites. Seventy percent of U.S. recruiters report that they have rejected candidates because of information found online, like photos and discussion-board conversations and membership in controversial groups.

Technological advances, of course, have often presented new threats to privacy. In 1890, in perhaps the most famous article on privacy ever written, Samuel Warren and Louis Brandeis complained that because of new technology — like the Kodak camera and the tabloid press — "gossip is no longer the resource of the idle and of the vicious but has become a trade." But the mild society gossip of the Gilded Age pales before the volume of revelations contained in the photos, video and chatter on social-media sites and elsewhere across the Internet. Facebook, which surpassed MySpace in 2008 as the largest social-networking site, now has nearly 500 million members, or 22 percent of all Internet users, who spend more than 500 billion minutes a month on the site. Facebook users share more than 25 billion pieces of content each month (including news stories, blog posts and photos), and the average user creates 70 pieces of content a month. There are more than 100 million registered Twitter users, and the Library of Congress recently announced that it will be acquiring — and permanently storing — the entire archive of public Twitter posts since 2006.

In Brandeis's day — and until recently, in ours — you had to be a celebrity to be gossiped about in public: today all of us are learning to expect the scrutiny that used to be reserved for the famous and the infamous. A 26-year-old Manhattan woman told The New York Times that she was afraid of being tagged in online photos because it might reveal that she wears only two outfits when out on the town — a Lynyrd Skynyrd T-shirt or a basic black dress. "You have movie-star issues," she said, "and you're just a person."

We've known for years that the Web allows for unprecedented voyeurism, exhibitionism and inadvertent indiscretion, but we are only beginning to understand the costs of an age in which so much of what we say, and of what others say about us, goes into our permanent — and public — digital files. The fact that the Internet never seems to forget is threatening, at an almost existential level, our ability to control our identities; to preserve the option of reinventing ourselves and starting anew; to overcome our checkered pasts.

In a recent book, "Delete: The Virtue of Forgetting in the Digital Age," the cyberscholar Viktor Mayer-Schönberger cites Stacy Snyder's case as a reminder of the importance of "societal forgetting." By "erasing external memories," he says in the book, "our society accepts that human beings evolve over time, that we have the capacity to learn from past experiences and adjust our behavior." In traditional societies, where missteps are observed but not necessarily recorded, the limits of human memory ensure that people's sins are eventually forgotten. By contrast, Mayer-Schönberger notes, a society in which everything is recorded "will forever tether us to all our past actions, making it impossible, in practice, to escape them." He concludes that "without some form of forgetting, forgiving becomes a difficult undertaking."

It's often said that we live in a permissive era, one with infinite second chances. But the truth is that for a great many people, the permanent memory bank of the Web increasingly means there are no second chances — no opportunities to escape a scarlet letter in your digital past. Now the worst thing you've done is often the first thing everyone knows about you.

THE CRISIS — AND THE SOLUTION?
All this has created something of a collective identity crisis. For most of human history, the idea of reinventing yourself or freely shaping your identity — of presenting different selves in different contexts (at home, at work, at play) — was hard to fathom, because people's identities were fixed by their roles in a rigid social hierarchy. With little geographic or social mobility, you were defined not as an individual but by your village, your class, your job or your guild. But that started to change in the late Middle Ages and the Renaissance, with a growing individualism that came to redefine human identity. As people perceived themselves increasingly as individuals, their status became a function not of inherited categories but of their own efforts and achievements. This new conception of malleable and fluid identity found its fullest and purest expression in the American ideal of the self-made man, a term popularized by Henry Clay in 1832.

From the late 18th to the early 20th century, millions of Europeans moved from the Old World to the New World and then continued to move westward across America, a development that led to what the historian Frederick Jackson Turner called "the significance of the frontier," in which the possibility of constant migration from civilization to the wilderness made Americans distrustful of hierarchy and committed to inventing and reinventing themselves.

In the 20th century, however, the ideal of the self-made man came under siege. The end of the Western frontier led to worries that Americans could no longer seek a fresh start and leave their past behind, a kind of reinvention associated with the phrase "G.T.T.," or "Gone to Texas." But the dawning of the Internet age promised to resurrect the ideal of what the psychiatrist Robert Jay Lifton has called the "protean self." If you couldn't flee to Texas, you could always seek out a new chat room and create a new screen name. For some technology enthusiasts, the Web was supposed to be the second flowering of the open frontier, and the ability to segment our identities with an endless supply of pseudonyms, avatars and categories of friendship was supposed to let people present different sides of their personalities in different contexts. What seemed within our grasp was a power that only Proteus possessed: namely, perfect control over our shifting identities.

But the hope that we could carefully control how others view us in different contexts has proved to be another myth. As social-networking sites expanded, it was no longer quite so easy to have segmented identities: now that so many people use a single platform to post constant status updates and photos about their private and public activities, the idea of a home self, a work self, a family self and a high-school-friends self has become increasingly untenable. In fact, the attempt to maintain different selves often arouses suspicion. Moreover, far from giving us a new sense of control over the face we present to the world, the Internet is shackling us to everything that we have ever said, or that anyone has said about us, making the possibility of digital self-reinvention seem like an ideal from a distant era.

Concern about these developments has intensified this year, as Facebook took steps to make the digital profiles of its users generally more public than private. Last December, the company announced that parts of user profiles that had previously been private — including every user's friends, relationship status and family relations — would become public and accessible to other users. Then in April, Facebook introduced an interactive system called Open Graph that can share your profile information and friends with the Facebook partner sites you visit.

What followed was an avalanche of criticism from users, privacy regulators and advocates around the world. Four Democratic senators — Charles Schumer of New York, Michael Bennet of Colorado, Mark Begich of Alaska and Al Franken of Minnesota — wrote to the chief executive of Facebook, Mark Zuckerberg, expressing concern about the "instant personalization" feature and the new privacy settings. The reaction to Facebook's changes was such that when four N.Y.U. students announced plans in April to build a free social-networking site called Diaspora, which wouldn't compel users to compromise their privacy, they raised more than $20,000 from more than 700 backers in a matter of weeks. In May, Facebook responded to all the criticism by introducing a new set of privacy controls that the company said would make it easier for users to understand what kind of information they were sharing in various contexts.

Facebook's partial retreat has not quieted the desire to do something about an urgent problem. All around the world, political leaders, scholars and citizens are searching for responses to the challenge of preserving control of our identities in a digital world that never forgets. Are the most promising solutions going to be technological? Legislative? Judicial? Ethical? A result of shifting social norms and cultural expectations? Or some mix of the above? Alex Türk, the French data-protection commissioner, has called for a "constitutional right to oblivion" that would allow citizens to maintain a greater degree of anonymity online and in public

places. In Argentina, the writers Alejandro Tortolini and Enrique Quagliano have started a campaign to "reinvent forgetting on the Internet," exploring a range of political and technological ways of making data disappear. In February, the European Union helped finance a campaign called "Think B4 U post!" that urges young people to consider the "potential consequences" of publishing photos of themselves or their friends without "thinking carefully" and asking permission. And in the United States, a group of technologists, legal scholars and cyberthinkers are exploring ways of recreating the possibility of digital forgetting. These approaches share the common goal of reconstructing a form of control over our identities: the ability to reinvent ourselves, to escape our pasts and to improve the selves that we present to the world.

REPUTATION BANKRUPTCY AND TWITTERGATION

A few years ago, at the giddy dawn of the Web 2.0 era — so called to mark the rise of user-generated online content — many technological theorists assumed that self-governing communities could ensure, through the self-correcting wisdom of the crowd, that all participants enjoyed the online identities they deserved. Wikipedia is one embodiment of the faith that the wisdom of the crowd can correct most mistakes — that a Wikipedia entry for a small-town mayor, for example, will reflect the reputation he deserves. And if the crowd fails — perhaps by turning into a digital mob — Wikipedia offers other forms of redress. Those who think their Wikipedia entries lack context, because they overemphasize a single personal or professional mistake, can petition a group of select editors that decides whether a particular event in someone's past has been given "undue weight." For example, if the small-town mayor had an exemplary career but then was arrested for drunken driving, which came to dominate his Wikipedia entry, he can petition to have the event put in context or made less prominent.

In practice, however, self-governing communities like Wikipedia — or algorithmically self-correcting systems like Google — often leave people feeling misrepresented and burned. Those who think that their online reputations have been unfairly tarnished by an isolated incident or two now have a practical option: consulting a firm like ReputationDefender, which promises to clean up your online image. ReputationDefender was founded by Michael Fertik, a Harvard Law School graduate who was troubled by the idea of young people being forever tainted online by their youthful indiscretions. "I was seeing articles about the 'Lord of the Flies' behavior that all of us engage in at that age," he told me, "and it felt un-American that when the conduct was online, it could have permanent effects on the speaker and the victim. The right to new beginnings and the right to self-definition have always been among the most beautiful American ideals."

ReputationDefender, which has customers in more than 100 countries, is the most successful of the handful of reputation-related start-ups that have been growing rapidly after the privacy concerns raised by Facebook and Google. (ReputationDefender recently raised $15 million in new venture capital.) For a fee, the company will monitor your online reputation, contacting Web sites individually and asking them to take down offending items. In addition, with the help of the kind of search-optimization technology that businesses use to raise their Google profiles, ReputationDefender can bombard the Web with positive or neutral information about its customers, either creating new Web pages or by multiplying links to existing ones to ensure they show up at the top of any Google search. (Services begin from $10 a month to $1,000 a year; for challenging cases, the price can rise into the tens of thousands.) By automatically raising the Google ranks of the positive links, ReputationDefender pushes the negative links to the back pages of a Google search, where they're harder to find. "We're hearing stories of employers increasingly asking candidates to open up Facebook pages in front of them during job interviews," Fertik told me. "Our customers include parents whose kids have talked about them on the Internet — 'Mom didn't get the raise'; 'Dad got fired'; 'Mom and Dad are fighting a lot, and I'm worried they'll get a divorce.' "

Companies like ReputationDefender offer a promising short-term solution for those who can afford it; but tweaking your Google profile may not be enough for reputation management in the near future, as Web 2.0 swiftly gives way to Web. 3.0 — a world in which user-generated content is combined with a new layer of data aggregation and analysis and live video. For example, the Facebook application Photo Finder, by Face.com, uses facial-recognition and social-connections software to allow you to locate any photo of yourself or a friend on Facebook, regardless of whether the photo was "tagged" — that is, the individual in the photo was identified by name. At the moment, Photo Finder allows you to identify only people on your contact list, but as facial-recognition technology becomes more widespread and sophisticated, it will almost certainly challenge our expectation of anonymity in public. People will be able to snap a cellphone picture (or video) of a stranger, plug the images into Google and pull up all tagged and untagged photos of that person that exist on the Web.

In the nearer future, Internet searches for images are likely to be combined with social-network aggregator search engines, like today's Spokeo and Pipl, which combine data from online sources — including political contributions, blog posts, YouTube videos, Web comments, real estate listings and photo albums. Increasingly these aggregator sites will rank people's public and private reputations, like the new Web site Unvarnished, a reputation marketplace where people can write anonymous reviews about anyone. In the Web 3.0 world, Fertik predicts, people will be rated, assessed and scored based not on their creditworthiness but on their trustworthiness as good parents, good dates, good employees, good baby sitters or good insurance risks.

Anticipating these challenges, some legal scholars have begun imagining new laws that could allow people to correct, or escape from, the reputation scores that may govern our personal and professional interactions in the future. Jonathan Zittrain, who teaches cyberlaw at Harvard Law School, supports an idea he calls "reputation bankruptcy," which would give people a chance to wipe their reputation slates clean and start over. To illustrate the problem, Zittrain showed me an iPhone app called Date Check, by Intelius, that offers a "sleaze detector" to let you investigate people you're thinking about dating — it reports their criminal histories, address histories and summaries of their social-networking profiles. Services like Date Check, Zittrain said, could soon become even more sophisticated, rating a person's social desirability based on minute social measurements — like how often he or she was approached or avoided by others at parties (a ranking that would be easy to calibrate under existing technology using cellphones and Bluetooth). Zittrain also speculated that, over time, more and more reputation queries will be processed by a handful of de facto reputation brokers — like the existing consumer-reporting agencies Experian and Equifax, for example — which will provide ratings for people based on their sociability, trustworthiness and employability.

To allow people to escape from negative scores generated by these services, Zittrain says that people should be allowed to declare "reputation bankruptcy" every 10 years or so, wiping out certain categories of ratings or sensitive information. His model is the Fair Credit Reporting Act, which requires consumer-reporting agencies to provide you with one free credit report a year — so you can dispute negative or inaccurate information — and prohibits the agencies from retaining negative information about bankruptcies, late payments or tax liens for more than 10 years. "Like personal financial bankruptcy, or the way in which a state often seals a juvenile criminal record and gives a child a ‘fresh start' as an adult," Zittrain writes in his book "The Future of the Internet and How to Stop It," "we ought to consider how to implement the idea of a second or third chance into our digital spaces."

Another proposal, offered by Paul Ohm, a law professor at the University of Colorado, would make it illegal for employers to fire or refuse to hire anyone on the basis of legal off-duty conduct revealed in Facebook postings or Google profiles. "Is it really fair for employers to know what you've put in your Facebook status updates?" Ohm asks. "We could say that Facebook status updates have taken the place of water-cooler chat,

which employers were never supposed to overhear, and we could pass a prohibition on the sorts of information employers can and can't consider when they hire someone."

Ohm became interested in this problem in the course of researching the ease with which we can learn the identities of people from supposedly anonymous personal data like movie preferences and health information. When Netflix, for example, released 100 million purportedly anonymous records revealing how almost 500,000 users had rated movies from 1999 to 2005, researchers were able to identify people in the database by name with a high degree of accuracy if they knew even only a little bit about their movie-watching preferences, obtained from public data posted on other ratings sites.

Ohm says he worries that employers would be able to use social-network-aggregator services to identify people's book and movie preferences and even Internet-search terms, and then fire or refuse to hire them on that basis. A handful of states — including New York, California, Colorado and North Dakota — broadly prohibit employers from discriminating against employees for legal off-duty conduct like smoking. Ohm suggests that these laws could be extended to prevent certain categories of employers from refusing to hire people based on Facebook pictures, status updates and other legal but embarrassing personal information. (In practice, these laws might be hard to enforce, since employers might not disclose the real reason for their hiring decisions, so employers, like credit-reporting agents, might also be required by law to disclose to job candidates the negative information in their digital files.)

Another legal option for responding to online setbacks to your reputation is to sue under current law. There's already a sharp rise in lawsuits known as Twittergation — that is, suits to force Web sites to remove slanderous or false posts. Last year, Courtney Love was sued for libel by the fashion designer Boudoir Queen for supposedly slanderous comments posted on Twitter, on Love's MySpace page and on the designer's online marketplace-feedback page. But even if you win a U.S. libel lawsuit, the Web site doesn't have to take the offending material down any more than a newspaper that has lost a libel suit has to remove the offending content from its archive.

Some scholars, therefore, have proposed creating new legal rights to force Web sites to remove false or slanderous statements. Cass Sunstein, the Obama administration's regulatory czar, suggests in his new book, "On Rumors," that there might be "a general right to demand retraction after a clear demonstration that a statement is both false and damaging." (If a newspaper or blogger refuses to post a retraction, they might be liable for damages.) Sunstein adds that Web sites might be required to take down false postings after receiving notice that they are false — an approach modeled on the Digital Millennium Copyright Act, which requires Web sites to remove content that supposedly infringes intellectual property rights after receiving a complaint.

As Stacy Snyder's "Drunken Pirate" photo suggests, however, many people aren't worried about false information posted by others — they're worried about true information they've posted about themselves when it is taken out of context or given undue weight. And defamation law doesn't apply to true information or statements of opinion. Some legal scholars want to expand the ability to sue over true but embarrassing violations of privacy — although it appears to be a quixotic goal.

Daniel Solove, a George Washington University law professor and author of the book "The Future of Reputation," says that laws forbidding people to breach confidences could be expanded to allow you to sue your Facebook friends if they share your embarrassing photos or posts in violation of your privacy settings. Expanding legal rights in this way, however, would run up against the First Amendment rights of others. Invoking the right to free speech, the U.S. Supreme Court has already held that the media can't be prohibited

from publishing the name of a rape victim that they obtained from public records. Generally, American judges hold that if you disclose something to a few people, you can't stop them from sharing the information with the rest of the world.

That's one reason that the most promising solutions to the problem of embarrassing but true information online may be not legal but technological ones. Instead of suing after the damage is done (or hiring a firm to clean up our messes), we need to explore ways of pre-emptively making the offending words or pictures disappear.

EXPIRATION DATES
Jorge Luis Borges, in his short story "Funes, the Memorious," describes a young man who, as a result of a riding accident, has lost his ability to forget. Funes has a tremendous memory, but he is so lost in the details of everything he knows that he is unable to convert the information into knowledge and unable, as a result, to grow in wisdom. Viktor Mayer-Schönberger, in "Delete," uses the Borges story as an emblem for the personal and social costs of being so shackled by our digital past that we are unable to evolve and learn from our mistakes. After reviewing the various possible legal solutions to this problem, Mayer-Schönberger says he is more convinced by a technological fix: namely, mimicking human forgetting with built-in expiration dates for data. He imagines a world in which digital-storage devices could be programmed to delete photos or blog posts or other data that have reached their expiration dates, and he suggests that users could be prompted to select an expiration date before saving any data.

This is not an entirely fanciful vision. Google not long ago decided to render all search queries anonymous after nine months (by deleting part of each Internet protocol address), and the upstart search engine Cuil has announced that it won't keep any personally identifiable information at all, a privacy feature that distinguishes it from Google. And there are already small-scale privacy apps that offer disappearing data. An app called TigerText allows text-message senders to set a time limit from one minute to 30 days after which the text disappears from the company's servers on which it is stored and therefore from the senders' and recipients' phones. (The founder of TigerText, Jeffrey Evans, has said he chose the name before the scandal involving Tiger Woods's supposed texts to a mistress.)

Expiration dates could be implemented more broadly in various ways. Researchers at the University of Washington, for example, are developing a technology called Vanish that makes electronic data "self-destruct" after a specified period of time. Instead of relying on Google, Facebook or Hotmail to delete the data that is stored "in the cloud" — in other words, on their distributed servers — Vanish encrypts the data and then "shatters" the encryption key. To read the data, your computer has to put the pieces of the key back together, but they "erode" or "rust" as time passes, and after a certain point the document can no longer be read. Tadayoshi Kohno, a designer of Vanish, told me that the system could provide expiration dates not only for e-mail but also for any data stored in the cloud, including photos or text or anything posted on Facebook, Google or blogs. The technology doesn't promise perfect control — you can't stop someone from copying your photos or Facebook chats during the period in which they are not encrypted. But as Vanish improves, it could bring us much closer to a world where our data didn't linger forever.

Kohno told me that Facebook, if it wanted to, could implement expiration dates on its own platform, making our data disappear after, say, three days or three months unless a user specified that he wanted it to linger forever. It might be a more welcome option for Facebook to encourage the development of Vanish-style apps that would allow individual users who are concerned about privacy to make their own data disappear without imposing the default on all Facebook users.

So far, however, Zuckerberg, Facebook's C.E.O., has been moving in the opposite direction — toward transparency rather than privacy. In defending Facebook's recent decision to make the default for profile information about friends and relationship status public rather than private, Zuckerberg said in January to the founder of the publication TechCrunch that Facebook had an obligation to reflect "current social norms" that favored exposure over privacy. "People have really gotten comfortable not only sharing more information and different kinds but more openly and with more people, and that social norm is just something that has evolved over time," he said.

PRIVACY'S NEW NORMAL

But not all Facebook users agree with Zuckerberg. Plenty of anecdotal evidence suggests that young people, having been burned by Facebook (and frustrated by its privacy policy, which at more than 5,000 words is longer than the U.S. Constitution), are savvier than older users about cleaning up their tagged photos and being careful about what they post. And two recent studies challenge the conventional wisdom that young people have no qualms about having their entire lives shared and preserved online forever. A University of California, Berkeley, study released in April found that large majorities of people between 18 and 22 said there should be laws that require Web sites to delete all stored information about individuals (88 percent) and that give people the right to know all the information Web sites know about them (62 percent) — percentages that mirrored the privacy views of older adults. A recent Pew study found that 18-to-29-year-olds are actually more concerned about their online profiles than older people are, vigilantly deleting unwanted posts, removing their names from tagged photos and censoring themselves as they share personal information, because they are coming to understand the dangers of oversharing.

Still, Zuckerberg is on to something when he recognizes that the future of our online identities and reputations will ultimately be shaped not just by laws and technologies but also by changing social norms. And norms are already developing to recreate off-the-record spaces in public, with no photos, Twitter posts or blogging allowed. Milk and Honey, an exclusive bar on Manhattan's Lower East Side, requires potential members to sign an agreement promising not to blog about the bar's goings on or to post photos on social-networking sites, and other bars and nightclubs are adopting similar policies. I've been at dinners recently where someone has requested, in all seriousness, "Please don't tweet this" — a custom that is likely to spread.

But what happens when people transgress those norms, using Twitter or tagging photos in ways that cause us serious embarrassment? Can we imagine a world in which new norms develop that make it easier for people to forgive and forget one another's digital sins?

That kind of social norm may be harder to develop. Alessandro Acquisti, a scholar at Carnegie Mellon University, studies the behavioral economics of privacy — that is, the conscious and unconscious mental trade-offs we make in deciding whether to reveal or conceal information, balancing the benefits of sharing with the dangers of disclosure. He is conducting experiments about the "decay time" and the relative weight of good and bad information — in other words, whether people discount positive information about you more quickly and heavily than they discount negative information about you. His research group's preliminary results suggest that if rumors spread about something good you did 10 years ago, like winning a prize, they will be discounted; but if rumors spread about something bad that you did 10 years ago, like driving drunk, that information has staying power. Research in behavioral psychology confirms that people pay more attention to bad rather than good information, and Acquisti says he fears that "20 years from now, if all of us have a skeleton on Facebook, people may not discount it because it was an error in our youth."

On the assumption that strangers may not make it easy for us to escape our pasts, Acquisti is also studying technologies and strategies of "privacy nudges" that might prompt people to think twice before sharing

sensitive photos or information in the first place. Gmail, for example, has introduced a feature that forces you to think twice before sending drunken e-mail messages. When you enable the feature, called Mail Goggles, it prompts you to solve simple math problems before sending e-mail messages at times you're likely to regret. (By default, Mail Goggles is active only late on weekend nights.) Acquisti is investigating similar strategies of "soft paternalism" that might nudge people to hesitate before posting, say, drunken photos from Cancún. "We could easily think about a system, when you are uploading certain photos, that immediately detects how sensitive the photo will be."

 A silly but surprisingly effective alternative might be to have an anthropomorphic icon — a stern version of Microsoft's Clippy — that could give you a reproachful look before you hit the send button. According to M. Ryan Calo, who runs the consumer-privacy project at Stanford Law School, experimenters studying strategies of "visceral notice" have found that when people navigate a Web site in the presence of a human-looking online character who seems to be actively following the cursor, they disclose less personal information than people who browse with no character or one who appears not to be paying attention. As people continue to experience the drawbacks of living in a world that never forgets, they may well learn to hesitate before posting information, with or without humanoid Clippys.

 FORGIVENESS
 In addition to exposing less for the Web to forget, it might be helpful for us to explore new ways of living in a world that is slow to forgive. It's sobering, now that we live in a world misleadingly called a "global village," to think about privacy in actual, small villages long ago. In the villages described in the Babylonian Talmud, for example, any kind of gossip or tale-bearing about other people — oral or written, true or false, friendly or mean — was considered a terrible sin because small communities have long memories and every word spoken about other people was thought to ascend to the heavenly cloud. (The digital cloud has made this metaphor literal.) But the Talmudic villages were, in fact, far more humane and forgiving than our brutal global village, where much of the content on the Internet would meet the Talmudic definition of gossip: although the Talmudic sages believed that God reads our thoughts and records them in the book of life, they also believed that God erases the book for those who atone for their sins by asking forgiveness of those they have wronged. In the Talmud, people have an obligation not to remind others of their past misdeeds, on the assumption they may have atoned and grown spiritually from their mistakes. "If a man was a repentant [sinner]," the Talmud says, "one must not say to him, ‘Remember your former deeds.' "

 Unlike God, however, the digital cloud rarely wipes our slates clean, and the keepers of the cloud today are sometimes less forgiving than their all-powerful divine predecessor. In an interview with Charlie Rose on PBS, Eric Schmidt, the C.E.O. of Google, said that "the next generation is infinitely more social online" — and less private — "as evidenced by their Facebook pictures," which "will be around when they're running for president years from now." Schmidt added: "As long as the answer is that I chose to make a mess of myself with this picture, then it's fine. The issue is when somebody else does it." If people chose to expose themselves for 15 minutes of fame, Schmidt says, "that's their choice, and they have to live with it."

 Schmidt added that the "notion of control is fundamental to the evolution of these privacy-based solutions," pointing to Google Latitude, which allows people to broadcast their locations in real time.

 This idea of privacy as a form of control is echoed by many privacy scholars, but it seems too harsh to say that if people like Stacy Snyder don't use their privacy settings responsibly, they have to live forever with the consequences. Privacy protects us from being unfairly judged out of context on the basis of snippets of private information that have been exposed against our will; but we can be just as unfairly judged out of context on the basis of snippets of public information that we have unwisely chosen to reveal to the wrong audience.

Moreover, the narrow focus on privacy as a form of control misses what really worries people on the Internet today. What people seem to want is not simply control over their privacy settings; they want control over their online reputations. But the idea that any of us can control our reputations is, of course, an unrealistic fantasy. The truth is we can't possibly control what others say or know or think about us in a world of Facebook and Google, nor can we realistically demand that others give us the deference and respect to which we think we're entitled. On the Internet, it turns out, we're not entitled to demand any particular respect at all, and if others don't have the empathy necessary to forgive our missteps, or the attention spans necessary to judge us in context, there's nothing we can do about it.

But if we can't control what others think or say or view about us, we can control our own reaction to photos, videos, blogs and Twitter posts that we feel unfairly represent us. A recent study suggests that people on Facebook and other social-networking sites express their real personalities, despite the widely held assumption that people try online to express an enhanced or idealized impression of themselves. Samuel Gosling, the University of Texas, Austin, psychology professor who conducted the study, told the Facebook blog, "We found that judgments of people based on nothing but their Facebook profiles correlate pretty strongly with our measure of what that person is really like, and that measure consists of both how the profile owner sees him or herself and how that profile owner's friends see the profile owner."

By comparing the online profiles of college-aged people in the United States and Germany with their actual personalities and their idealized personalities, or how they wanted to see themselves, Gosling found that the online profiles conveyed "rather accurate images of the profile owners, either because people aren't trying to look good or because they are trying and failing to pull it off." (Personality impressions based on the online profiles were most accurate for extroverted people and least accurate for neurotic people, who cling tenaciously to an idealized self-image.)

Gosling is optimistic about the implications of his study for the possibility of digital forgiveness. He acknowledged that social technologies are forcing us to merge identities that used to be separate — we can no longer have segmented selves like "a home or family self, a friend self, a leisure self, a work self." But although he told Facebook, "I have to find a way to reconcile my professor self with my having-a-few-drinks self," he also suggested that as all of us have to merge our public and private identities, photos showing us having a few drinks on Facebook will no longer seem so scandalous. "You see your accountant going out on weekends and attending clown conventions, that no longer makes you think that he's not a good accountant. We're coming to terms and reconciling with that merging of identities."

Perhaps society will become more forgiving of drunken Facebook pictures in the way Gosling says he expects it might. And some may welcome the end of the segmented self, on the grounds that it will discourage bad behavior and hypocrisy: it's harder to have clandestine affairs when you're broadcasting your every move on Facebook, Twitter and Foursquare. But a humane society values privacy, because it allows people to cultivate different aspects of their personalities in different contexts; and at the moment, the enforced merging of identities that used to be separate is leaving many casualties in its wake. Stacy Snyder couldn't reconcile her "aspiring-teacher self" with her "having-a-few-drinks self": even the impression, correct or not, that she had a drink in a pirate hat at an off-campus party was enough to derail her teaching career.

That doesn't mean, however, that it had to derail her life. After taking down her MySpace profile, Snyder is understandably trying to maintain her privacy: her lawyer told me in a recent interview that she is now working in human resources; she did not respond to a request for comment. But her success as a human being who can change and evolve, learning from her mistakes and growing in wisdom, has nothing to do with the

digital file she can never entirely escape. Our character, ultimately, can't be judged by strangers on the basis of our Facebook or Google profiles; it can be judged by only those who know us and have time to evaluate our strengths and weaknesses, face to face and in context, with insight and understanding. In the meantime, as all of us stumble over the challenges of living in a world without forgetting, we need to learn new forms of empathy, new ways of defining ourselves without reference to what others say about us and new ways of forgiving one another for the digital trails that will follow us forever.

 Jeffrey Rosen, a law professor at George Washington University, is a frequent contributor to the magazine. He is writing a book about Louis Brandeis.

Este artículo viene de culturas de archivo
http://culturasdearchivo.org/

La URL de esta historia es:
http://culturasdearchivo.org/modules.php?op=modload&name=News&file=article&sid=799