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 underage 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.
EXPRIATION 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.

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