

WHO SPEWED THAT ABUSE? ANONYMOUS YIK YAK APP ISN'T TELLING

JONATHAN MAHLER

During a brief recess in an honors course at Eastern Michigan University last fall, a teaching assistant approached the class's three female professors. "I think you need to see this," she said, tapping the icon of a furry yak on her iPhone.

The app opened, and the assistant began scrolling through the feed. 2 While the professors had been lecturing about post-apocalyptic culture, some of the 230 or so freshmen in the auditorium had been having a separate conversation about them on a social media site called Yik Yak. There were dozens of posts, most demeaning, many using crude, sexually explicit language and imagery.

After class, one of the professors, Margaret Crouch, sent off a flurry of 3 emails—with screenshots of some of the worst messages attached—to various university officials, urging them to take some sort of action. “I have been defamed, my reputation besmirched. I have been sexually harassed and verbally abused,” she wrote to her union representative. “I am about ready to hire a lawyer.”

In the end, nothing much came of Ms. Crouch’s efforts, for a simple rea- 4 son: Yik Yak is anonymous. There was no way for the school to know who was responsible for the posts.

Eastern Michigan is one of a number of universities whose campuses have 5 been roiled by offensive “yaks.” Since the app was introduced a little more than a year ago, it has been used to issue threats of mass violence on more than a dozen college campuses, including the University of North Carolina, Michigan State University, and Penn State. Racist, homophobic, and misogynist “yaks” have generated controversy at many more, among them Clemson, Emory, Colgate, and the University of Texas. At Kenyon College, a “yakker” proposed a gang rape at the school’s women’s center.

In much the same way that Facebook swept through the dorm rooms of 6 America’s college students a decade ago, Yik Yak is now taking their smartphones by storm. Its enormous popularity on campuses has made it the most frequently downloaded anonymous social app in Apple’s App Store, easily surpassing competitors like Whisper and Secret. At times, it has been one of the store’s 10 most downloaded apps.

Like Facebook or Twitter, Yik Yak is a social media network, only without 7 user profiles. It does not sort messages according to friends or followers but by geographic location or, in many cases, by university. Only posts within a 1.5-mile radius appear, making Yik Yak well suited to college campuses. Think of it as a virtual community bulletin board—or maybe a virtual bathroom wall at the student union. It has become the go-to social feed for college students across the country to commiserate about finals, to find a party, or to crack a joke about a rival school.

Much of the chatter is harmless. Some of it is not. 8

“Yik Yak is the Wild West of anonymous 9 social apps,” said Danielle Keats Citron, a law professor at University of Maryland and the author of *Hate Crimes in Cyberspace*. “It is being increasingly used by young people in a really intimidating and destructive way.”

“Much of the
chatter is harmless.
Some of it is not.”

Colleges are largely powerless to deal with the havoc Yik Yak is wreak- 10 ing. The app’s privacy policy prevents schools from identifying users

without a subpoena, court order, or search warrant, or an emergency request from a law-enforcement official with a compelling claim of imminent harm. Schools can block access to Yik Yak on their Wi-Fi networks, but banning a popular social media network is controversial in its own right, arguably tantamount to curtailing freedom of speech. And as a practical matter, it doesn't work anyway. Students can still use the app on their phones with their cell service.

Yik Yak was created in late 2013 by Tyler Droll and Brooks Buffington, fraternity brothers who had recently graduated from Furman University in South Carolina. Mr. Droll majored in information technology and Mr. Buffington in accounting. Both 24, they came up with the idea after realizing that there were only a handful of popular Twitter accounts at Furman, almost all belonging to prominent students, like athletes. With Yik Yak, they say, they hoped to create a more democratic social media network, one where users didn't need a large number of followers or friends to have their posts read widely.

"We thought, 'Why can't we level the playing field and connect everyone?'" said Mr. Droll, who withdrew from medical school a week before classes started to focus on the app.

"When we made this app, we really made it for the disenfranchised," Mr. Buffington added.

Just as Mark Zuckerberg and his roommates introduced Facebook at Harvard, Mr. Buffington and Mr. Droll rolled out their app at their alma mater, relying on fraternity brothers and other friends to get the word out.

Within a matter of months, Yik Yak was in use at 40 or so colleges in the South. Then came spring break. Some early adopters shared the app with college students from all over the country at gathering places like Daytona Beach and Panama City. "And we just exploded," Mr. Buffington said.

Mr. Droll and Mr. Buffington started Yik Yak with a loan from Mr. Droll's parents. (His parents also came up with the company's name, which was inspired by the 1958 song, "Yakety Yak.") In November, Yik Yak closed a \$62 million round of financing led by one of Silicon Valley's biggest venture capital firms, Sequoia Capital, valuing the company at hundreds of millions of dollars.

The Yik Yak app is free. Like many tech start-ups, the company, based in Atlanta, doesn't generate any revenue. Attracting advertisers could pose a challenge, given the nature of some of the app's content. For now, though, Mr. Droll and Mr. Buffington are focused on extending Yik Yak's reach by expanding overseas and moving beyond the college market, much as Facebook did.

Yik Yak's popularity among college students is part of a broader reaction against more traditional social media sites like Facebook, which can encourage public posturing at the expense of honesty and authenticity.

"Share your thoughts with people around you while keeping your privacy," Yik Yak's home page says. It is an attractive concept to a generation of smartphone users who grew up in an era of social media—and are thus

inclined to share—but who have also been warned repeatedly about the permanence of their digital footprint.

In a sense, Yik Yak is a descendant of JuicyCampus, an anonymous online college message board that enjoyed a brief period of popularity several years ago. Matt Ivester, who founded JuicyCampus in 2007 and shut it in 2009 after it became a hotbed of gossip and cruelty, is skeptical of the claim that Yik Yak does much more than allow college students to say whatever they want, publicly and with impunity. “You can pretend that it is serving an important role on college campuses, but you can’t pretend that it’s not upsetting a lot of people and doing a lot of damage,” he said. “When I started JuicyCampus, cyberbullying wasn’t even a word in our vernacular. But these guys should know better.”

Yik Yak’s founders say the app’s overnight success left them unprepared for some of the problems that have arisen since its introduction. In response to complaints, they have made some changes to their product, for instance, adding filters to prevent full names from being posted. Certain keywords, like “Jewish,” or “bomb,” prompt this message: “Pump the brakes, this yak may contain threatening language. Now it’s probably nothing and you’re probably an awesome person but just know that Yik Yak and law enforcement take threats seriously. So you tell us, is this yak cool to post?”

In cases involving threats of mass violence, Yik Yak has cooperated with authorities. Most recently, in November, local police traced the source of a yak—“I’m gonna [gun emoji] the school at 12:15 p.m. today”—to a dorm room at Michigan State University. The author, Matthew Mullen, a freshman, was arrested within two hours and pleaded guilty to making a false report or terrorist threat. He was spared jail time but sentenced to two years’ probation and ordered to pay \$800 to cover costs connected to the investigation.

In the absence of a specific, actionable threat, though, Yik Yak zealously protects the identities of its users. The responsibility lies with the app’s various communities to police themselves by “upvoting” or “downvoting” posts. If a yak receives a score of negative 5, it is removed. “Really, what it comes down to is that we try to empower the communities as much as we can,” Mr. Droll said.

When Yik Yak appeared, it quickly spread across high schools and middle schools, too, where the problems were even more rampant. After a rash of complaints last winter at a number of schools in Chicago, Mr. Droll and Mr. Buffington disabled the app throughout the city. They say they have since built virtual fences—or “geo-fences”—around about 90 percent of the nation’s high schools and middle schools. Unlike barring Yik Yak from a Wi-Fi network, which has proved ineffective in limiting its use, these fences actually make it impossible to open the app on school grounds. Mr. Droll and Mr. Buffington also changed Yik Yak’s age rating in the App Store from 12 and over to 17 and over.

Toward the end of last school year, almost every student at Phillips Exeter Academy in New Hampshire had the app on his or her phone and checked it constantly to read the anonymous attacks on fellow students, faculty members, and deans.

"Please stop using Yik Yak immediately," Arthur Cosgrove, the dean of residential life, wrote in an email to the student body. "Remove it from your phones. It is doing us no good."

At Exeter's request, the company built a geo-fence around the school, but it covered only a few buildings. Students continued using the app on different parts of the sprawling campus.

"We made the app for college kids, but we quickly realized it was getting into the hands of high schoolers, and high schoolers were not mature enough to use it," Mr. Droll said.

The widespread abuse of Yik Yak on college campuses, though, suggests that the distinction may be artificial. Last spring, Jordan Seman, then a sophomore at Middlebury College, was scrolling through Yik Yak in the dining hall when she happened across a post comparing her to a "hippo" and making a sexual reference about her. "It's so easy for anyone in any emotional state to post something, whether that person is drunk or depressed or wants to get revenge on someone," she said. "And then there are no consequences."

In this sense, the problem with Yik Yak is a familiar one. Anyone who has browsed the comments of an Internet post is familiar with the sorts of intolerant, impulsive language that the cover of anonymity tends to invite. But Yik Yak's particular design can produce especially harmful consequences.

"It's a problem with the Internet culture in general, but when you add this hyper-local dimension to it, it takes on a more disturbing dimension," says Elias Aboujaoude, a Stanford psychiatrist and the author of *Virtually You*. "You don't know where the aggression is coming from, but you know it's very close to you."

Jim Goetz, a partner at Sequoia Capital who recently joined Yik Yak's board, said the app's history of misuse was a concern when his firm considered investing in the company. But he said he was confident that Mr. Droll and Mr. Buffington were committed to ensuring more positive interactions on Yik Yak, and that over time, the constructive voices would overwhelm the destructive ones.

"It's certainly a challenge to the company," Mr. Goetz said. "It's not going to go away in a couple of months."

Ms. Seman wrote about her experience being harassed on Yik Yak in the school newspaper, the *Middlebury Campus*, prompting a schoolwide debate over what to do about the app. Unable to reach a consensus, the paper's editorial board wrote two editorials, one urging a ban, the other arguing that the problem wasn't Yik Yak but the larger issue of cyberbullying. (Middlebury has not taken any action.)

Similar debates have played out at other schools. At Clemson, a group of African-American students unsuccessfully lobbied the university to ban Yik Yak when some racially offensive posts appeared after a campus march to protest the grand jury's decision not to indict a white police officer in the fatal shooting of an unarmed black teenager in Ferguson, Mo. "We think that in the educational community, First Amendment rights are very important," said

Leon Wiles, the school's chief diversity officer. "It's just problematic because you have young people who use it with no sense of responsibility."

During the fall, Maxwell Zoberman, the sophomore representative to the student government at Emory, started noticing a growing number of yaks singling out various ethnic groups for abuse. "Fave game to play while driving around Emory: not hit an Asian with a truck," read one.

"Guys stop with all this hate. Let's just be thankful we arn't black," read another.

After consulting the university's code, Mr. Zoberman discovered that statements deemed derogatory to any particular group of people were not protected by the school's open expression policy, and were in fact in violation of its discriminatory harassment rules. Just because the statements were made on an anonymous social-media site should not, in his mind, prevent Emory from acting to enforce its own policies. "It didn't seem right that the school took one approach to hate speech in a physical medium and another one in a digital medium," he said.

Mr. Zoberman drafted a resolution to have Yik Yak disabled on the school's Wi-Fi network. He recognized that this would not stop students from using the app, but he nevertheless felt it was important for the school to take a stand.

After Mr. Zoberman formally proposed his resolution to the student government, someone promptly posted about it on Yik Yak. "The reaction was swift and harsh," he said. "I seem to have redirected all of the fury of the anonymous forum. Yik Yak was just dominated with hateful and other aggressive posts specifically about me." One compared him to Hitler.

A few colleges have taken the almost purely symbolic step of barring Yik Yak from their servers. John Brown University, a Christian college in Arkansas, did so after its Yik Yak feed was overrun with racist commentary during a march connected to the school's World Awareness Week. Administrators at Utica College in upstate New York blocked the app in December in response to a growing number of sexually graphic posts aimed at the school's transgender community.

In December, a group of 50 professors at Colgate University—which had experienced a rash of racist comments on the app earlier in the fall—tried a different approach, flooding the app with positive posts.

Generally speaking, though, the options are limited. A student who felt that he or she had been the target of an attack on Yik Yak could theoretically pursue defamation charges and subpoena the company to find out who had written the post. But it is a difficult situation to imagine, given the cost and murky legal issues involved. Schools will probably just stand back and hope that respect and civility prevail, that their communities really will learn to police themselves.

Yik Yak's founders say their start-up is just experiencing some growing pains. "It's definitely still a learning process for us," Mr. Buffington said, "and we're definitely still learning how to make the community more constructive."

"Yik Yak's founders say their start-up is just experiencing some growing pains."

ALL EYES ON YOU

JENNIFER GOLBECK

Every day, nearly everywhere I go, I'm being followed. That's not paranoia. It's a fact. Consider:

On my local Washington, D.C., streets, I am constantly watched. The city government alone has hundreds of traffic and surveillance cameras. And then there are the cameras in parks, office buildings, ATM lobbies, and, of course, around every federal building and landmark. On an average day, my image is captured by well over 100 cameras.

When I'm online and using social media, a wealth of information about my interests and routines is collected behind the scenes. I employ an add-on on my browser that blocks companies from tracking my searches and visits. In just one recent month, it reported blocking nearly 16,000 separate attempts to access my data online.

I'm monitored offline, too. Anytime I use a reward card at a supermarket, department store, or other retail outlet, my purchase is recorded, and the data either sold to other marketers or used to predict my future purchases and guide me to make them in that store. Department store tracking based on purchase records can even conclude that a woman is pregnant and roughly when she is due.

My own devices report on me. I carry an iPhone, which tracks and records my every movement. This will help me find my phone if I ever lose it (I haven't yet), but it also provides Apple with a treasure trove of data about my daily habits.

Data on any call I place or email I send may be collected by the National Security Agency. Recent news reports have revealed that the federal intelligence arm may be collecting metadata on phone and Internet traffic—when Americans communicate and with whom, if not the actual content of those communications. As Barton Gellman, Pulitzer Prize-winning intelligence reporter for the *Washington Post*, said during a recent panel discussion, it's not that the NSA knows everything about everyone, but that "it *wants* to be able to know anything about anybody."

Thirty years after 1984, Big Brother is here. He's everywhere. In many cases, we've invited him in. So the question we have to ask now is, How does this constant surveillance affect us and what, if anything, can we do about it?

"Get Over It."

There's no question our privacy has been eroded with the help of technology. There's also little question that those most responsible aren't much inclined to retreat. As Scott McNealy, cofounder of Sun Microsystems, famously said: "You have zero privacy anyway. Get over it."

Privacy is an intangible asset. If we never think about it, we may not realize it's gone.

Does it still matter? Elias Aboujaoude, a professor of psychiatry at Stanford University and the author of *Virtually You: The Dangerous Powers of the E-Personality*, insists that it does. "We cannot afford to just 'get over it,' for nothing short of our self-custody seems to be at stake," he says. "At its heart, this is about our psychological autonomy and the maintenance of some semblance of control over the various little details that make us us."

In the modern surveillance environment, with so much personal information accessible by others—especially those with whom we have not chosen to share that information—our sense of self is threatened, as is our ability to manage the impression others have of us, says Ian Brown, senior research fellow at the Oxford Internet Institute.

If people treat us differently based on what they have discovered online, if the volume of data available about us eradicates our ability to make a first impression on a date or a job interview, the result, Brown believes, is reduced trust, increased conformity, and even diminished civic participation. The impact can be especially powerful when we know that our information was collected and shared without our consent.

To be sure, we are responsible for much of this. We're active participants in creating our surveillance record. Along with all of the personal information we voluntarily, often eagerly, share on social networks and shopping sites—and few of us take advantage of software or strategies to limit our digital footprint—we collectively upload 144,000 hours of video footage a day to YouTube. And with tech enthusiasts trumpeting personal drones as the next hot item, we may soon be equipped to photograph ourselves and, just as easily, our neighbors, from above.

Most of us try to curate the public identities we broadcast—not only through the way we dress and speak in public, but also in how we portray ourselves on social-media platforms. The problem arises when we become conscious that uninvited observers are also tuning in. "The most fundamental impact surveillance has on identity," Brown says, "is that it reduces individuals' control over the information they disclose about their attributes in different social contexts, often to such powerful actors as the state or multinational corporations." When we discover that such entities—and third parties to which our information may be sold or shared—make decisions about us based on that data, our sense of self can be altered.

The Right to Be Forgotten

There are existential threats to our psyches in a world where nothing we do can be forgotten, believes Viktor Mayer-Schönberger, professor of Internet governance and regulation at the Oxford Internet Institute. His book, *Delete: The Virtue of Forgetting in the Digital Age*, relates the experiences of people whose lives were negatively affected because of information available about them online.

"Does it still matter?"

9

10

11

12

13

14

In 2006, for example, psychotherapist Andrew Feldmar drove from his Vancouver home to pick up a friend flying in to Seattle. At the United States border, which Feldmar had crossed scores of times, a guard decided to do an Internet search on him. The query returned an article Feldmar had written for an academic journal five years earlier, in which he revealed that he'd taken LSD in the 1960s. The guard held Feldmar for four hours, fingerprinted him, and asked him to sign a statement that he had taken drugs almost 40 years earlier. He was barred from entry into the U.S.

Aboujaoude relates the story of "Rob," a nurse in a public hospital emergency room chronically short on staff. His willingness to fill in when the ER needed extra hands led to significant overtime pay. When a website published an "exposé" of seemingly overpaid public employees, Rob's name and salary were posted as an example. He was then hounded by hate mail—both paper and electronic. People called his house, and his daughter was harassed at school. Eventually the stress and constant criticism made him feel as if he were becoming paranoid and led him to Aboujaoude as a therapy patient.

The ability to forget past events, Mayer-Schönberger says, or at least to let them recede in our minds, is critical for decision making. Psychologists often note that our ability to forget is a valuable safety valve. As we naturally forget things over time, we can move on and make future choices without difficult or embarrassing episodes clouding our outlook. But when our decisions are tangled up in the perfect memory of the Internet—when we must factor in the effect of our online footprint before every new step—"we may lose a fundamental human capacity: to live and act firmly in the present," he says.

The result can be demoralizing and even paranoia-inducing. Lacking the power to control what, when, and with whom we share, Mayer-Schönberger explains, our sense of self may be diminished, leading to self-doubt internally and self-censorship externally, as we begin to fixate on what others will think about every potentially public action and thought, now and in the future.

Under normal circumstances, the passage of time allows us to shape our narrative, cutting out or minimizing less important (or more embarrassing) details to form a more positive impression. When we can't put the past behind us, it can affect our behavior and intrude on our judgment. Instead of making decisions fully in the present, we make them while weighed down by every detail of our past.

The effects are not trivial. A range of people, from a long-reformed criminal seeking a fresh slate to a sober former college party girl in the job market, can find that the omnipresence of public records and posted photos permanently holds them back. At its worst, these weights can inhibit one's desire to change. If we can never erase the record of one mistake we made long ago, if we're convinced it will only continue to hinder our progress, what motivation do we have to become anyone different from the person who made that mistake? For that matter, why bother moving

"With easily accessible digital reminders, bygones cannot be bygones."

beyond conflicts with others if the sources of those disputes remain current online? With easily accessible digital reminders, bygones cannot be bygones. It's no accident that the most successful legal campaign yet against permanent digital records hinges on "the right to be forgotten."

A Spanish lawyer, Mario Costeja González, sued Google over search results that prominently returned a long-ago news article detailing a government order that he sell his home to cover unpaid debts. The European Court of Justice ruled in his favor, asserting, based on an older legal concept allowing ex-convicts to object to the publication of information related to their crimes, that each of us has the right to be forgotten. Even if the information about the man's foreclosure is true, the court ruled, it is "irrelevant, or no longer relevant," and should be blocked from Google's (and other browsers') searches.

Google is now working to implement a means for European users to request that certain information be removed from their searches, a process it is finding to be more complicated than many observers had imagined. No similar verdict has been handed down in the U.S., and privacy experts believe that Congress is unlikely to take up the issue anytime soon.

Do Cameras Make Us More Honorable, or Just Paranoid?

Trust is perennially strained in our workplaces, where more employees than ever are being overseen via cameras, recorded phone calls, location tracking, and email monitoring. Studies dating back two decades have consistently found that employees who were aware that they were being surveilled found their working conditions more stressful and reported higher levels of anxiety, anger, and depression. More recent research indicates that, whatever productivity benefits management hopes to realize, increased surveillance on the office floor leads to poorer performance, tied to a feeling of loss of control as well as to lower job satisfaction.

Outside the workplace, we expect more freedom and wider opportunity to defend our privacy. But even as we become more savvy about online tracking, we're beginning to realize just how little we can do about so-called "passive" surveillance—the cameras recording our movements as we go about our business—especially because so much of this observation is covert. The visual range of surveillance cameras has expanded even as their physical size has shrunk, and as satellites and drones become more accurate from increasing distances, social scientists have begun to explore how near-constant surveillance, at least in the public sphere, affects our behavior. The research so far identifies both concerns and potential benefits. We tend, for example, to be more cooperative and generous when we suspect someone is watching—a recent Dutch study found that people were more likely to intervene when witnessing a (staged) crime if they knew they were being watched, either by others or by a camera. But we don't become more generous of spirit. Pierrick Bourrat, a graduate student at the University of Sydney, and cognitive scientist Nicolas Baumard of the École Normale Supérieure in Paris, recently published a study on how we judge other people's bad behavior. They found that when subjects believed they were being watched, they rated others' actions more severely. A possible

explanation: When we think we're being observed, we adjust our behavior to project an image of moral uprightness through harsher-than-usual judgment of others.

But adjusting our behavior in the presence of cameras to project an image aligned with presumed social norms can have a downside. The Oxford Internet Institute's Brown sees a cooling effect on public discourse, because when people think they're being watched, they may behave, consciously or not, in ways that comply with what they presume governmental or other observers want. That doesn't mean we trust the watchers. A recent Gallup poll found that only 12 percent of Americans have "a lot of trust" that the government will keep their personal information secure; we trust banks three times as much.

When Users Strike Back

What would happen if we really tried to root out all of the surveillance in our life and took action to erase ourselves from it? We think such knowledge would equal power, but it may just bring on paranoia. Pulitzer Prize-winning investigative journalist Julia Angwin tried for a year to prevent her life from being monitored. She used a disposable cell phone. She installed encryption software on her email accounts. She even developed a fake identity ("Ida Tarbell") to prevent her online and commercial activities from being tied to her true self.

Angwin detailed these efforts in her book, *Dragnet Nation*, which, while ultimately hopeful, relates a draining journey during which she lost trust in nearly every institution that holds her data. Even with her resources and single-mindedness, Angwin could achieve only partial success: Her past personal data, after all, were stored in bits and pieces by hundreds of brokers that traffic in information, and she had no means of turning back the clock.

The efforts also affected her worldview: "I wasn't happy with the toll that my countersurveillance techniques had taken on my psyche. The more I learned about who was watching me, the more paranoid I became. By the end of my experiment, I was refusing to have digital conversations with my close friends without encryption. I began using my fake name for increasingly trivial transactions; a friend was shocked when we took a yoga class together and I casually registered as Ida Tarbell."

The Next Level

Modern surveillance does have some clear benefits. Cameras in public spaces help the authorities detect crime and catch perpetrators, though they catch us in the dragnet as well. Cell phone tracking and networked late-model cars allow us to be found if we become lost or injured, and mapping apps are incredibly useful for directing us where we want to go. These features save lives—but all of them constantly transmit our location and generate a precisely detailed record of our movements. Our social media history helps providers put the people and content we prefer front and center when we log on, and our online searches and purchase records allow marketers to offer us discounts at the places we shop most, all the while collecting data on our personal

preferences and quirks. Given the difficulty of completely avoiding the monitoring, it may be somewhat reassuring to acknowledge this tradeoff.

Laura Brandimarte of Carnegie Mellon University and her colleagues have studied people's willingness to disclose personal information. They found that when entities give people more control over the publication of their information, people disclose more about themselves—even if it is also clear that the information will be accessed and seen by others more often than it currently is.

Their work demonstrates the concept of illusion of control. In many situations, we tend to overestimate the control we have over events, especially when we get cues that our actions matter. The risk to our private information comes not just from what we've shared but from how much of it is sold or made available to others. And yet when we feel that we have been given more control over our information's dissemination, our privacy concerns decrease and our disclosure increases, even though that apparent control does not actually diminish the possibility that our data will be shared. "The control people perceive over the publication of personal information makes them pay less attention to the lack of control they have over access by others," Brandimarte says.

In other words, we are simply not very sophisticated when it comes to making choices about what to share.

When it comes to privacy-protection, the first issue for social-media users to grapple with is inertia: According to a range of surveys of U.S. Facebook users, for example, as many as 25 percent have never checked or adjusted their privacy settings to impose even the most basic restriction on their postings: not making them public.

There is a growing availability of privacy fixes for homes, cell phones, and computers. Whether they will be able to keep up with tracking mechanisms is unclear. But evidence suggests that even if they work as advertised, we may not be savvy enough to use them.

So we have limited options to protect our privacy, and few of us take advantage even of those. What's the ultimate cost? Aboujaoude argues that our need for privacy and true autonomy is rooted in the concept of individuation, the process by which we develop and maintain an independent identity. It's a crucial journey that begins in childhood, as we learn to separate our own identity from that of our parents, and continues through adulthood.

Many psychologists emphasize that maintaining self-identity requires a separation from others, and Aboujaoude believes that, in today's environment, control over personal information is a critical piece of the process. "You are a psychologically autonomous individual," he says, "if you have the option to keep your person to yourself and dole out the pieces as you see fit."

And who do we become if we don't have that option? We may soon find out.

I Married a P.I.

When we worry about who might be watching us, we tend to focus our concern on Facebook, the NSA, or marketers. But we may want to consider our own partners as well.

Sue Simring, an associate professor at Columbia University's School of Social Work and a psychotherapist with four decades of experience working primarily with couples, says the ease with which people can now monitor each other has radically changed her work. "It used to be that, unless you literally discovered them [in flagrante], there was no way to know for sure that people were having an affair," she says.

No more.

When spouses stray today, their digital trail inevitably provides clues for the amateur sleuth with whom they share a bed. Simring describes one case in which a man had carried on an affair for years while traveling for work. He managed to keep it secret until a technical glitch started sending copies of his text messages to his wife's iPad.

But the easy availability of tools to track a partner can cut both ways. In the case of another couple that Simring worked with, the husband was convinced that his wife was having an affair. Determined to catch her, he undertook increasingly complex and invasive surveillance efforts, eventually monitoring all of her communications and installing spy cameras in their home to catch her in the act. The more he surveilled, the more his paranoia grew. It turned out that the wife was not having an affair, but because of the trauma the husband's surveillance caused her, she ended the marriage.

s posted to the online newspaper *The Start* on February 27, 2015.

MY CREEPY INSTAGRAM MAP KNOWS WHERE I LIVE

CRAIG DESSON

U.S. Congressman Aaron Schock's reputation took a hit this week when the Associated Press used geo-location data from his Instagram account to show how he was flying on private jets provided by campaign donors, expensed massages, and bought Katy Perry tickets for his interns.

The reporters involved explained that "the AP extracted location data associated with each image, then correlated it with flight records showing airport stopovers and expenses later billed for air travel against Schock's office and campaign records."

To track somebody on Instagram the way AP did for the Schock story isn't difficult. There is a program called Creepy that will create a Google map showing where you've been, based on what you've shared on Instagram, Twitter, and Flickr.

I ran Creepy on my own Instagram account and found it wouldn't be hard for a stranger to figure out where I live in the Annex.



This is the map the program made about my account, and with a bit of 5 deductive logic it's clear I live just north of Bloor and Spadina.

The photos taken around Front St. are all interiors of offices, because that's 6 where I've worked for the past two and a half years. The photos taken along major streets such as King and Bloor portray me hanging out with friends.

Then there is the funny collection of dots north of Bloor in the Annex 7 that link to Instagram photos of an apartment's interior.

You don't need to be Sherlock Holmes to guess that's my home. 8

It's true that 20 years ago, a phonebook might have led a stranger to my 9 home address. But I would at least know that I had a listed number. The trouble with Instagram tracking is that most users have no idea their photo-sharing app is also building a detailed history of where they work and live.

If Aaron Schock, a congressman with paid communications people, 10 couldn't figure this out, then it's likely most members of the public have no idea this is going on.

USA Today posted this article to its website on March 27, 2014.



IS ONLINE DATING SAFE?

SHARON JAYSON

Change may be coming to the rapidly growing dating industry as concern 1 mounts about the privacy and safety of all online and mobile users.

Sen. Al Franken, D-Minn., introduced legislation Thursday requiring 2 companies to get customers' permission before collecting location data off their mobile devices and sharing it with others.

It's a move that would greatly affect dating websites and apps. As mobile dating proliferates, the focus no longer is just on daters leery of scams or sexual predators, but on keeping their locations confidential.

"This stuff is advancing at a faster and faster rate, and we've got to try and catch up," Franken says. "This is about Americans' right to privacy and one of the most private things is your location."

Illinois, New York, New Jersey, and Texas have laws that require Internet dating sites to disclose whether they conduct criminal background checks on users and to offer advice on keeping safe.

"I see more regulation about companies stating what kind of information they actually use and more about their specific operation(s)," says analyst Jeremy Edwards, who authored a report on the industry last fall for IBIS-World, a Santa Monica, Calif.-based market research company. "I expect them to have to be more explicit in what they do with their data and what they require of users."

According to a Pew Research Center report in October, 11% of American adults—and 38% of those currently "single and looking" for a partner—say they've used online dating sites or mobile dating apps.

"We entrust some incredibly sensitive information to online dating sites," says Rainey Reitman of the San Francisco, Calif.-based Electronic Frontier Foundation, a nonprofit that advocates for user privacy amid technology development. "People don't realize how much information they're exposing even by doing something as slight as uploading a photograph."

He adds, "Many online apps are very cavalier about collecting that information and perhaps exposing it in a way that would make you uncomfortable."

Dating services eHarmony, Match.com, and Spark Networks and ChristianMingle signed an agreement in 2012 with the California attorney general's office to protect customers with online safety tools. These include companies checking subscribers against national sex offender registries and providing a rapid abuse reporting system for members.

However, cyberdating expert Julie Spira of Los Angeles says such reports are sometimes little more than revenge.

"When people get reported, sometimes it's because they got jilted," she says. "How do you quantify when someone feels rejected and pushes the report button, and when somebody really feels scared?"

Match.com, which has 1.9 million paid subscribers, has been screening all subscribers against sexual offender registries since the summer of 2011,

"As mobile dating proliferates, the focus no longer is just on daters leery of scams or sexual predators, but on keeping their locations confidential."

according to spokesman Matthew Traub. Earlier that year, a woman sued the dating site saying she was assaulted by someone she met through it.

Edwards believes dating sites are doing what they can to help users 14 be safe.

“It’s difficult for these companies to do much else than provide information 15 and tips,” he says. “Meeting someone through one of these websites does not present any greater risk than meeting someone in a bar or any other setting. There’s no real added risk because you don’t know who anyone is when you meet them for the first time.”