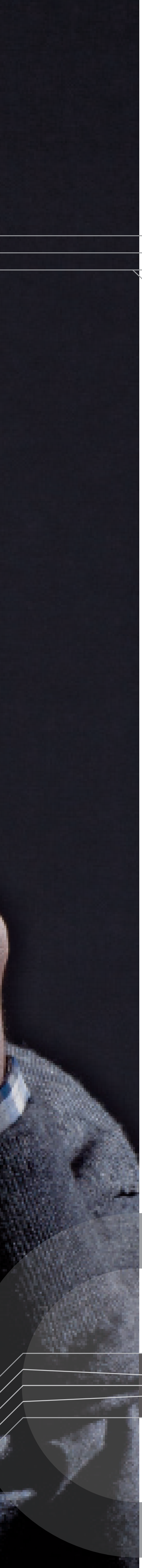
Hidden in Plain Sight

How online privacy tools are changing Internet security and driving the (probably quixotic) quest for anonymity in the digital age.



for many of us, the Internet is like a puppy—lovable by design and fun to play with, but prone to biting. We suspect that our digital footprint is being tracked and recorded (true), mined and sold (super true), but we tolerate these teeth marks because, for many of us, the Internet is irresistible, its rewards greater than its risks. In a 2011 Gallup poll, more than half of those surveyed said they worried about privacy issues with Google, yet 60 percent paid weekly visits to the search giant. As long as we clear our search terms, block cookies, use antivirus software and see that our social media presence isn't too social, we'll be OK. Right?

Increasingly, this sense of security is an illusion. "I don't trust anything on the Internet," says digital whistleblower John Young. "Cybersecurity is a fiction." He would know: Young was a seminal member of WikiLeaks and runs Cryptome, a website that posts "documents prohibited by governments worldwide"—think FBI files and manuals detailing how Microsoft spies on us. He argues that the tenuous architecture of the Internet prevents it from being truly secure.

Case in point: Mat Honan, the wired.com writer whose entire digital existence was destroyed by hackers within the span of an hour last August. The cyberbaddies broke into Honan's Gmail, accessed his Apple ID account and deleted data on his MacBook, iPhone and iPad, including photos of his family. The scariest part of this privacy breach—aside from the fact that its victim is a tech writer (ahem)—is that the hackers hijacked his online world using nothing more than his billing address and the last four digits of his credit card, information that's relatively easy to obtain online if you know the right tricks. Honan's story served as yet another reminder that THE INTERNET IS NOT SAFE, PEOPLE.

So is it time to go off the grid? That's one option. Another is to ditch the puppy analogy and view the Internet the way those who demand higher than average levels of security do: as a giant tracking device that can be outsmarted. Countless tools exist to cloak your digital identity: email encryption services, "meta search engines" that promise private browsing and networks and software that offer a degree of anonymity and, in some cases, entry to previously inaccessible websites. Sounds like the stuff of spy novels, but these tools are available to

BY CHRIS CLAYTON | PHOTOGRAPHY BY RICHARD FLEISCHMAN

> “Anonymity felt great . . . but then social media arrived. Suddenly, we decided it was important to tell the Internet our real name and what we had for breakfast.”

anyone with an Internet connection.

Of course, the idea of online anonymity clashes with the prevailing "share everything" approach to the Internet—and the moneymaking opportunities therein—which makes it a fascinating and complicated topic. Its opponents say it fosters hate and crime (Mark Zuckerberg's sister, Randi Zuckerberg, who used to head up marketing at Facebook, famously called for the end of online anonymity earlier this year, stating that "People behave a lot better when they have their real names down"), while privacy champions argue that anonymity grants greater security and freedom of expression. The John Youngs of the world will tell you that being truly unidentifiable online is a fairy tale. But every fairy tale has a lesson, and even if you get hives thinking about trading your identity for a more armored online existence, there's plenty to learn from the heroes, villains and everyday secret-keepers attempting to go John Doe in the digital realm.

There's a famous *New Yorker* cartoon from 1993 that shows two dogs in front of a computer, one saying to the other, "On the Internet, nobody knows you're a dog." This was a novel proposition in the Web's early days. Liberated from our actual identity, we chatted in forums using ridiculous pseudonyms such as "beaniebabyaddict47" and posted comments as "Anonymous," our snarky alter ego. Anonymity felt great, even if technically it was just a state of mind. But then social media arrived, and with it the idea that transparency is power. Suddenly, we decided it was important to tell the Internet our real name and what we had for breakfast.

For those who want to keep their breakfast habits a secret, the rise of transparency created new security risks. Enter the digital cloaking device. In 2002, the U.S. Naval Research Lab debuted Tor, one of the more effective "anonymizers" to date. A group of M.I.T. grads developed it with the goal of masking one's IP address, the string of numbers that reveals a given computer's physical location (snoops and hacks love your IP because it brings them one step closer to determining the real you).

At the heart of Tor is a concept called "onion routing," which sends the "packets" of info needed to get from points A to B online on a winding route through a network of randomly selected servers, each one knowing only the packet's previous and next stops in the chain, thereby hiding the user's IP and allowing a degree of anonymous Web browsing. Confused? In the simplest terms, Tor separates the origin and destination of your online communication, essentially tunneling you through the Web.

The U.S. Navy financed this tunnel to protect government communications, but its code was released to the public because, as Karen Reilly, development director for the nonprofit Tor Project, puts it, "A Navy anonymity network wouldn't work. The idea is to have many diverse users so that you can't tell who somebody is just by virtue of them using Tor." Using seed money from the Electronic Frontier Foundation, a digital rights advocacy group, the Tor Project formed a decade ago to grow Tor's user base and maintain and improve its network. Today, Reilly estimates that Tor has about half a million daily users and 3,000 to 4,000 "nodes," volunteer servers that hopscotch you through the network.

Tor is available as a free download on torproject.org. This software includes a Tor-enabled version of the Firefox Web browser that hides your IP address and forces an encrypted connection where available. Sounds great, but like most anonymizing tools, Tor is flawed. It slows Web browsing and, if someone decided to keep an eye on a large enough swath of the Internet, he could theoretically analyze data patterns to guess where the communication originated.

These weaknesses haven't stopped hundreds of thousands from downloading the service. Reilly says most people use it to protect their browsing because "they think it's creepy to be tracked. They don't like the fact that there's a file on them somewhere being kept by an advertiser who knows what cereal they like to eat." And there are more weighty reasons to use Tor: Journalists and activists in oppressive regimes use it to circumvent Internet censorship. It's been reported that Arab Spring revolutionaries tapped Tor to access Facebook and Twitter, both of which were blocked at various points by Egypt, Iran and others (incidentally, Iran has the second-highest number of Tor users; the United States has the most).

Criminals, trolls and other creeps also love Tor—no surprise given their affinity for the Internet in general. In the mood for some heroin? Silk Road is a one-stop online shop for illegal goods that uses Tor to hide its location from users and, ostensibly, law enforcement. Anonymity haters reference nasty sites like these when stating their case, but Reilly thinks this is misguided. "If Tor didn't exist, criminals would have other options."

Other options used by both crooks *and* law-abiders include virtual private networks, which are faster than Tor and sometimes less secure—and generally not free. Like Tor, VPNs provide a secure

(Hidden continued on page 84)

CREDITS: ON HIM (PREVIOUS SPREAD): SWEATER BY VINCE, SHIRT BY BILLY REID. ON HER: TANK BY HAUTE HIPPIE, JACKET BY TRUTH AND PRIDE. ALL FROM NORDSTROM. STYLING: ELIZABETH DOYLE; HAIR & MAKEUP: RENE RATTLER FROM MOORE CREATIVE TALENT, INC.; MODELS: PETER HANSEN & SUN MEE CHOMET, BOTH FROM MOORE CREATIVE TALENT INC; RANSOM NOTE ILLUSTRATION: RANDALL NELSON.

(Hidden continued from page 79)

connection between computers and can be used as a gateway to websites that would otherwise be inaccessible. VPNs are all the rage in China, where government censorship of the Internet is the norm. Mara Hvistendahl, a Shanghai-based correspondent for *Science* magazine, has experimented with different privacy tools since moving to the city in 2004. She started with Tor, but found it too slow for regular Web browsing, so she switched to VPNs to access Gmail and Google Scholar, sites that have been blocked by Chinese censors. "Every foreign journalist I know in China uses a VPN," she says. Another VPN user—a China-based English and journalism teacher who spoke to *Sky* on the condition of you know what—says she pays for a VPN called Astrill to reach Facebook.

Both women mentioned pairing VPNs with other privacy tools. Hvistendahl has heard of reporters combining VPNs, multiple SIM cards and the secure email service Hushmail to protect sources. If it's true that no online cloaking device is totally effective, this bundling strategy might be our best bet for protecting ourselves online—though good luck trying to convince the average Web user to do it.

(Continued on page 86)

Silent Partners

WHO OR WHAT IS **ANONYMOUS**?

It's one voice with many vocal chords. It's a hive mind and a state of mind. It's organized when it wants to be and disjointed when it needs to be. It's a combination Zorro and computer nerd. It's Anonymous, a loose collective of hackers who joined forces in 2003 to launch gonzo viral campaigns and generally get weird online. Its earliest hits originated on message boards. Remember "LOLCats" (cat photos with absurd captions)? How about "Rickrolling," a prank in which victims unwittingly link to a YouTube clip of 1980s pop star Rick Astley?

A few years in, these digital Dadaists discovered their moral compass—and adopted a figurehead to prove it. Anons, as Anonymous members are known, began sporting masks with the smirking likeness of Guy Fawkes, a 17th-century British revolutionary who today is a Che Guevara-like symbol of rebellion (the mask in question first appeared in the *V For Vendetta* comics, worn by the series' freedom fighter). Anonymous transformed itself into a cybervigilante, shutting down pedophilia sites, hacking corporate and government Web pages, joining forces with Occupy Wall Street and teaching Arab Spring protestors how to circumvent Internet censorship. Suddenly, hackers of all ages and locales were helping to enact geopolitical change.

By early 2012, Anonymous was more powerful than ever. On January 19, roughly 5,000 Anons launched a digital assault on supporters of the U.S. government's proposed Stop Online Piracy Act, a bill that Anonymous and others feared might lead to Internet censorship (one of Anonymous' main platforms is a free and open digital space). The attack was the group's largest yet, underlining its strengths—namely, strength in numbers—and weaknesses—e.g., not all Anons are created equal (a handful were tracked down by the FBI and arrested). A few months later, *TIME* put the group on its annual "100 Most Influential" list.

Not surprisingly, the world's most famous hacktivist organization has as many enemies as friends. Law enforcement would prefer that Anons left Internet policing to the professionals, while the group's victims view it as a terrorist syndicate. The problem with typecasting thousands of faceless hackers, though, is that just when you think you've got them figured out, they upend your expectations. Perhaps it's best just to sit back and wait for Act III—and hope it doesn't involve you. —*C. C.*

Puzzle Answers //

Easy KENKEN

2÷ 2	3– 1	4	3 3
1	1– 4	3	16× 2
7+ 4	3	2	1
3 3	2÷ 2	1	4

Hard KENKEN

1 1	30× 6	5	1– 2	3	2÷ 4
2÷ 4	1	3 3	11+ 6	5	2
2	3÷ 3	1	80× 4	11+ 6	5
6× 3	2	4	5	5– 1	6
1– 6	5 5	1– 2	1	12× 4	3
5	10+ 4	6	3 3	2÷ 2	1

©2012 KenKen Puzzle, LLC www.kenken.com

Trademark Nextoy, LLC Dist by Universal Uclick for UFS

Easy Sudoku

2	4	3	1	8	6	7	9	5
8	1	6	7	9	5	4	3	2
5	9	7	4	3	2	6	8	1
3	5	4	9	7	1	2	6	8
7	2	1	6	5	8	3	4	9
6	8	9	2	4	3	1	5	7
1	6	8	5	2	4	9	7	3
9	3	2	8	6	7	5	1	4
4	7	5	3	1	9	8	2	6

Hard Sudoku

9	7	4	1	3	6	8	2	5
2	5	3	8	9	7	1	4	6
1	8	6	5	4	2	7	3	9
6	1	8	9	2	4	3	5	7
5	4	7	3	6	1	9	8	2
3	2	9	7	5	8	4	6	1
7	9	5	6	8	3	2	1	4
4	3	1	2	7	5	6	9	8
8	6	2	4	1	9	5	7	3

5/23

© 2012 Knight Features/Distributed by Universal Uclick

O	H	N	O	■	■	B	R	O	■	■	T	W	O	D
M	O	O	R	■	S	L	O	B	■	B	O	O	R	S
O	T	R	O	■	C	O	L	O	■	R	O	N	D	O
O	L	D	S	C	H	O	O	L	■	O	T	T	O	S
■	■	■	C	O	M	P	S	■	H	O	T	■	■	■
H	O	H	O	H	O	■	■	K	O	M	O	D	O	■
O	R	O	■	O	S	M	O	N	D	■	O	R	R	S
S	L	O	P	S	■	O	S	O	■	S	T	O	O	L
P	O	C	O	■	M	O	T	T	S	T	■	O	N	O
■	P	H	O	B	O	S	■	■	P	R	O	L	O	G
■	■	■	L	O	W	■	S	T	O	O	D	■	■	■
S	C	O	R	N	■	S	N	O	O	P	D	O	G	G
N	O	T	O	K	■	H	O	O	K	■	L	O	O	T
O	C	H	O	S	■	O	W	L	S	■	O	P	T	O
B	O	O	M	■	■	O	S	S	■	■	T	S	O	S

Trademark Nextoy, LLC Dist by Universal Uclick for UFS

5/23

© 2012 Knight Features/Distributed by Universal Uclick

“Most people have a difficult time with far-off risk,” says Ashkan Soltani, a former technologist with the Federal Trade Commission’s privacy division who’s currently a privacy/security researcher and consultant. “That’s why we passed seat belt laws. The likelihood of you getting in a car accident is low, but the harm that you might experience in that accident is potentially high. It’s the same online. We’re bad at figuring out how our data could be used against us in the future, so we don’t care.”

We should care, says Lee Tien, senior staff attorney for the Electronic Frontier Foundation, because data privacy laws are “not incredibly strong.” This is an understatement in countries such as China and Iran, where Web users have little or no online freedom. The US has the Wiretap Act and the Stored Communications Act, both of which address basic privacy issues such as police needing an interception order to tap emails. But these laws fail to look at how private corporations handle our digital footprint, and as a result, we’re at the mercy of, say, Facebook’s data policy or Google’s data policy, and we all know that they have our best interests in mind . . . .

But here’s the real stinger: Let’s say you decide to take control of your digital footprint and start using some of the tools mentioned above. Also, you begin paying closer attention to the privacy policies on the various sites you visit, clicking “do not track” when possible and opting out of initiatives such as Google’s targeted ads program, which is based on the content of your email. Congratulations, responsible netizen, you now have more online security than most—have fun on your cumbersome, hard-to-manage, less optimized version of the Internet!

Ken Berman puts it another way: “If you want to be on Facebook, there are certain things—anonymizing tools that prevent tracking,

Additional Photography Credits //

Page 14 & 15 //
John p. Johnson/Twentieth Century Fox (Butler); Everest (Everest Shrimp); Kevin Lynch (De Laurentiis); Chanon Kanjanavasoontara/Getty Images (Bangkok); Paul Schiraldi/HBO (Pierce); Moises De Pena (Lauder).

Page 52 & 53 //
Circle: Daniel Cheong/Getty Images (Wat Arun Temple)

Page 52: Scenester: Manoo Manookulkit (Hotel Muse); Issaya Siamese Club (Mussamun lamb shank); Bruno Ehrs/Corbis (Bed Supperclub); Sky Bar (bar); Design Junkie: Igor Prahin (Maenam Suite, The Siam); Luca Tettoni/Corbis (18th C. pieces from the Bencharong Collection); dk/Alamy (Bangkok Arts and Culture Centre); Nahm (minced prawn and cucumber salad with green mango).

Page 53: Foodie: Mandarin Oriental Bangkok (The Author's Lounge); Blue Elephant Cooking School & Restaurant Bangkok (class); Tourism Authority of Thailand, tatnews.org (street vendor); Mr.Vutikorn Sintuvatin (Bo.Lan).; Fashionista: SofitelSo (Metal Element Room); Rod Porteous/Corbis (slippers); David Ball/Alamy (Siam Paragon).; Off the Grid: Bangkok Tree House (outdoor room); Banyan Tree Spa Bangkok (spa treatment); Urban Tree Organics (store).

prevent cookies, prevent identifying behavior—that make some of these social media tools difficult to work with." Berman, an IT security expert who for years worked at the Broadcasting Board of Governors (the United States' international broadcasting arm), sees two options for Internet users: "Either you say, 'I give in. I enjoy the Web, so I'll put up with walking by a store and getting a text message that says go in this store and you'll get an immediate 10 percent coupon.' Or you say, 'No, I don't want to play in that world, so I'm going to use Tor or a VPN. I'm going to clean up my session every time I log out and not leave any remnants of my behavior.' I don't see how there's anything in between."

Soltani is more optimistic. He sees a future where governments pass stronger digital privacy laws and geeks build easier-to-use privacy controls that work seamlessly with the slobbering puppy version of the Internet we all love. In the meantime, he's doing his best to educate as many people as possible on the virtues of proper digital hygiene, whether that means using anonymity tools or simply being more aware of the fact that you leave a data trail wherever you go these days (don't even get us started on smartphones).

"My big thing is to demystify I.T.," says Soltani. "It doesn't help to think of it as magic or something that's bringing the world to an end. Tech changes the way we interact with one another and our society—and we should be cognizant of that and adjust accordingly."

For now, it remains to be seen how these changes will affect online anonymity, a concept that begs important questions about what sort of society we want to live in: Is anonymity a right? Should we be able to engage in discourse anonymously? Should beaniebabyaddict47 be allowed to have such an obnoxious alias? Stay tuned. //

With consultation on information systems security from Matt Lange at Milwaukee Area Technical College.