ESSAY: THE TWO FACES OF ANONYMITY

ALEX KOZINSKI *

The Urban Dictionary defines "conscience" as "[t]he little voice in the back of your head that tells you somebody is watching."[1] As abundant psychological experiments bear out, the feeling of being watched is a significant restraint on our impulses.[2] Even a picture of watching eyes can alter our behavior and make us more likely to conform to prevailing social norms.[3] While anonymity has many liberating aspects that can be quite positive from a personal perspective, it's also true that from a societal perspective anonymity has many negative implications.[4] People who believe themselves to be undetectable are apt to do things that society doesn't approve of.[5] That's why bank robbers wear masks and pickpockets don't leave calling cards.

Anonymity is an artifact of modern society. When our lives were lived out in small communities, anonymity was very difficult or even impossible to achieve. As hard as it is to imagine today, most people throughout history never had the experience of feeling anonymous. My guess is most of them did not even fully comprehend the concept.[6] The emergence of the Internet

---

* Judge of the United States Court of Appeals for the Ninth Circuit.

[1] LRS, Post defining *Conscience*, URBAN DICTIONARY (Feb. 21, 2007), http://www.urbandictionary.com/define.php?term=conscience&defid=2266167.

[2] *See, e.g.*, Terence C. Burnham, *Engineering Altruism: A Theoretical and Experimental Investigation of Anonymity and Gift Giving*, 50 J. ECON. BEHAV. & ORG. 133, 139–41, Figures 2 & 3 (2003) (demonstrating the tested effects of anonymity on one's character).

[3] *See* Max Ernest-Jones et al., *Effects of Eye Images on Everyday Cooperative Behavior: A Field Experiment*, 32 EVOLUTION & HUM. BEHAV. 172, 175–76 (2011).

[4] Kimberly M. Christopherson, *The Positive and Negative Implications of Anonymity in Internet Social Interactions: "On the Internet, Nobody Knows You're a Dog,"* 23 COMPUTERS IN HUM. BEHAV. 3038, 3040 (2007).

[5] *Id.* at 3041.

[6] Lest I be misunderstood, I should add that the related concept of privacy was not unknown. It has long been understood that certain activities, like sex, bathing, sleeping, and defecation could best be enjoyed in private. Privacy and anonymity are closely related concepts, often mistaken for each other. Jed Rubenfeld, *We Need a New Jurisprudence of Anonymity*, WASH. POST, Jan. 13, 2014, at A17. But they are, in fact, quite different. It is possible to have privacy without anonymity. For example, you know exactly who's living in the house across the street, but you don't know what they do inside the house. And it's

is central to today's modern conception of anonymity, as many millions of people believe (often wrongly) themselves to be undetectable.[7] Sitting alone in front of a computer screen, it's easy to imagine that your identity is unknown and untraceable because you choose not to reveal who you are.

I remember a few years ago when blogger David Lat first made his appearance as "Article III Groupie" (A3G).[8] The conceit was that he was a woman working for a "large law firm in a major city" who blogged adoringly about federal judges but also gave fashion advice.[9] In fact, Lat was an Assistant U.S. Attorney in the District of New Jersey, working under then U.S. Attorney Chris Christie.[10] There was quite a bit of speculation as to who Article III Groupie might be, based on information revealed in the blog.[11] Right about that time, I got a call from my former law clerk, Steve Engel, who suggested that the blogger might be his classmate David Lat. He deduced this from A3G's frequent references to Yale,[12] and the fact that the blogger claimed to have had three unsuccessful Supreme Court clerkship interviews.[13] But speculating about someone's identity is not the same as knowing for sure, so we came up with a scheme to unmask Article III Groupie: we sent simultaneous emails—me to A3G and Engel to Lat—and we got back answers within 10 minutes of each other. When we opened up the headers on the two e-mails we discovered—as we had expected—that they originated from the same IP address, so it had to be Lat.[14]

---

possible to have anonymity without privacy: You are in a throng of people in the middle of Times Square on New Year's Eve but no one recognizes you.

[7] *See* Kate Murphy, *How to Muddy Your Tracks on the Internet*, N.Y. TIMES, May 3, 2012, at B7.

[8] Adam Liptak, *Mystery of Gossipy Blog on the Judiciary is Solved*, N.Y. TIMES, Nov. 16, 2005, at A14.

[9] Article III Groupie, *About Me*, UNDERNEATH THEIR ROBES, http://underneaththeirrobes.blogs.com/about.html (last visited Sept. 5, 2014).

[10] Jonathan Miller, *He Fought the Law. They Both Won: The Double Life of a Prosecutor Who Preferred Cheeky Blogging*, N.Y. TIMES, Jan. 22, 2006, at A14.

[11] Liptak, *supra* note 8.

[12] *See, e.g.*, Article III Groupie, *Judicial SIGHT-ations: SDO Watching B-Ball*, UNDERNEATH THEIR ROBES (Dec. 28, 2004), http://underneaththeirrobes.blogs.com/main/2004/12/judicial_sighta_1.html; Article III Groupie, *Judicial SIGHT-ations: Thanksgiving Special Issue*, UNDERNEATH THEIR ROBES (Nov. 24, 2004), http://underneaththeirrobes.blogs.com/main/2004/11/judicial_sighta_1.html (providing blog entries with multiple references to Yale Law School).

[13] *About Me*, *supra* note 9.

[14] Lat uses a similar ploy in his upcoming novel, for much the same purpose. DAVID LAT, SUPREME AMBITIONS 145–47 (2014).

Steve and I agreed not to disclose Lat's identity. But it occurred to us that it could be quite damaging to Lat's career as a prosecutor if he were outed by someone else. So that evening I wrote A3G an email explaining how someone might theoretically figure out her real identity. Lat took my advice and started using an anonymizer website for his A3G postings and correspondence; his identity remained secret until he chose to reveal himself by disclosing his identity to Jeffrey Toobin who in turn disclosed it in an article in The New Yorker.[15]

Anonymizers and onion routers make it far more difficult to do the kind of internet detective work that Steve Engel and I used to find Lat. A couple of years ago, one of my sons introduced me to the hidden Internet—websites that can only be accessed by using TOR: The Onion Router.[16] Here's a quick tutorial—via Wikipedia—for those few who aren't familiar with it:

> [TOR] encrypts and then randomly bounces communications through a network of relays run by volunteers around the globe. These onion routers employ encryption in a multi–layered manner (hence the onion metaphor) to ensure perfect forward secrecy between relays, thereby providing users with anonymity in network location. That anonymity extends to the hosting of censorship–resistant content via TOR's anonymous hidden service feature.[17]

There is a lot more, but you get the idea.[18]

To access the hidden Internet, you need to download and install the TOR browser, which is readily available on the regular Internet at torproject.org.[19] Once that's done, you can go to any number of unusual websites. Before 2013, the place to start would have been Silk Road—a secret online black market where over a million customers spent approximately $1.2 billion on

---

[15] Jeffrey Toobin, *The Bench SCOTUS Watch*, NEW YORKER, Nov. 21, 2005, at 44.

[16] Dylan Love, *There's a Secret Internet for Drug Dealers, Assassins, and Pedophiles*, BUS. INSIDER (Mar. 6, 2013, 7:00 AM), http://www.businessinsider.com/tor-silk-road-deep-web-2013-3?op=1.

[17] *Tor (Anonymity Network)*, WIKIPEDIA, https://en.wikipedia.org/wiki/Tor_(anonymity_network) (last visited Sept. 5, 2014).

[18] Jam Kotenko, *A Beginner's Guide to TOR: How to Navigate Through the Underground Internet*, DIGITAL TRENDS (Aug. 15, 2014), http://www.digitaltrends.com/computing/a-beginners-guide-to-tor-how-to-navigate-through-the-underground-internet/.

[19] TOR PROJECT, https://www.torproject.org (last visited Sept. 5, 2014).

all manner of exotic purchases.[20] Though its stock–in–trade was hard drugs (on any given day there could be narcotics listings in the thousands, all neatly categorized into groups such as opioids, psychedelics, stimulants and dissociatives), Silk Road sold everything from "Marijuana Butter Chocolate Chip Cookies" to forged Lithuanian passports.[21]

Silk Road was shut down in October of 2013 when the FBI tracked down its alleged founder and "Chief Executive" Ross William Ulbricht—or "Dread Pirate Roberts" as he is known online—and arrested him on charges of murder–for–hire and narcotics trafficking.[22] While Silk Road's demise sent shockwaves through the "darknet" economy, it wasn't the crippling blow to online black markets that the feds hoped it might be. In fact, illicit transactions on the hidden Internet are now at an all-time high.[23]

Though Silk Road had the most mainstream prominence, its offerings—even in its heyday—were always pretty limited compared to other "darknet" purveyors.[24] If you want to find truly exotic goods and services, a good place to search is "The Hidden Wiki."[25] Made out to look like a Wikipedia page, but accessible only by using an onion router, "The Hidden Wiki" has a wealth of information to satisfy enquiring minds.[26]

When I last looked, I found plenty of notable products and services on offer: "Skimmers for Sale and Rent," which are devices that attach to ATM machines and skim off the electronic data from the cards inserted into them

---

[20] *See* Donna Leinwand Leger, *How FBI Brought Down Cyber-Underworld Site Silk Road*, USA TODAY, May 15, 2014, http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/.

[21] *See* Peter Rugg, *Silk Road Drug Trafficking Site Back and Busier than Ever with More than 13,000 Listings for Drugs Just Eight Months After Being Shut Down by the FBI*, DAILY MAIL ONLINE (Apr. 30, 2014), http://www.dailymail.co.uk/news/article-2617122/Silk-Road-drug-trafficking-site-busier-13-000-listings-drugs-just-eight-months-shut-FBI.html. Silk Road has been described as "an online drug bazaar where international sales of illicit drugs and other contraband were conducted with impunity and with the ease of buying cocktail stirrers or underwear on Amazon." Kim Zetter, *How the Feds Took Down the Silk Road Drug Wonderland*, WIRED (Nov. 18, 2013), http://www.wired.com/2013/11/silk-road/.

[22] Zetter, *supra* note 21.

[23] *See* Digital Citizens Alliance Investigative Report, *Busted, But Not Broken: The State of Silk Road and the Darknet Marketplaces*, DIGITAL CITIZENS ALLIANCE (Apr. 30, 2014), https://media.gractions.com/314A5A5A9ABBBBC5E3BD824CF47C46EF4B9D3A76/5f8d4168-c36a-4f78-b048-f5d48b18dc0a.pdf.

[24] *See id.*

[25] *See Exploring the Hidden Wiki–What Is Inside?*, HIDDENWIKI.ORG., http://www.hiddenwiki.org/exploring.html (last visited Oct. 19, 2014).

[26] *See id.*

by unsuspecting ATM patrons; Tor University, which offered "Research and Writing services for the college student"; Rent–a–Hacker, who boasted that "(Illegal) Hacking and social engineering is my bussiness [sic] since i [sic] was 14 years old, never had a real job so i [sic] had the time to get really good at hacking and i [sic] made a good amount of money last +-16 years"; Pirax Web DDOS, which offered denial of service attacks on your enemies or competitors for a price.[27] Or, if your problem is really serious, you could try Killer for Hire, whose logo is "Permanent Solutions to Common Problems!" or Quick Kill, whose logo is "Remove That Problem From Your Life."[28] Both seemed to offer contract killings for $20,000—half up-front and half upon proof of completion.[29] In fact, their terms of service were so similar, I thought of alerting the FTC that they may be engaged in price-fixing.

How does one pay for these goods and services? After all, it wouldn't look so good to get your American Express bill and have a charge for Contract Killing or Brown Heroin. The preferred method of payment on the hidden Internet consists of Bitcoins, and there seem to be plenty of places to buy them.[30] I haven't actually tried to buy anything from the hidden marketplace, so I don't know how many of these websites deliver what they promise, how many are scams, and how many are police sting operations. But it's clear that a market for illegal and highly dangerous goods and services does, in fact, exist. And it does so only because it's possible to use the Internet to render transactions anonymous and thus, drastically reduce the risks of engaging in anti-social behavior.

But you don't need the hidden Internet to cause mischief online when you think you're anonymous. For instance, Lori Drew concealed her Internet identity by faking a MySpace account and caused Megan Meier, her

---

[27] *The Hidden Wiki*, DEEP WEB WIKI (July 31, 2013, 3:35 PM), http://deepweb.wikia.com/wiki/The_hidden_wiki; RENT-A-HACKER, http://rentahackeronline.weebly.com/ (last visited Oct. 19, 2014); *How to Access the Deep Net: Working Links to the Deep Web*, GOOGLE SITES, https://sites.google.com/site/howtoaccessthedeepnet/working-links-to-the-deep-web (last visited Oct. 19, 2014).

[28] *See* Joel Falconer, *Mail-Order Drugs, Hitmen & Child Porn: A Journey into the Dark Corners of the Deep Web*, NEXT WEB (Oct. 10, 2014), http://thenextweb.com/insider/2012/10/08/mail-order-drugs-hitmen-child-porn-a-journey-into-the-dark-corners-of-the-deep-web/.

[29] *Id.*

[30] *See Buying Bitcoins (the newbie version)*, BITCOIN WIKI, https://en.bitcoin.it/wiki/Buying_Bitcoins_(the_newbie_version) (last visited Oct. 19, 2014).

daughter's erstwhile friend, to kill herself.[31] Uncounted millions routinely engage in copyright infringement by downloading unlicensed music, videos, and software from off-shore servers or by "borrowing" from friends.[32] And you need only glance at the anonymous comments on websites like Above the Law[33] and AutoAdmit[34] to detect a level of malice that is seldom observed among people whose identities are known.

Of course, it's not just on the Internet that anonymity has been used to nefarious ends. The 9/11 terrorists used anonymity in key aspects of their evil enterprise.[35] They were able to circulate freely, get flight lessons for commercial aircraft, obtain airline tickets, and otherwise remain hidden in plain sight.[36] The participants in the conspiracy could have been identified by name and other characteristics—they had, after all, been subject to inspection and registration in the government's computers.[37] But they were effectively anonymous, not because their identities were masked in any way, but because none of their activities attracted any official attention.[38]

Americans are, in fact, highly ambivalent about anonymity.[39] On the one hand, we see anonymity as a positive value, the handmaiden of privacy.[40] If you're anonymous—truly anonymous—no one will know your business. If you're anonymous, you can speak your mind freely without fear of retaliation. Hence the popularity of *V for Vendetta*[41] and the Guy Fawkes

---

[31] United States v. Lori Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009). *See also* Kim Zetter, *Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury*, WIRED (July 2, 2009), http://www.wired.com/2009/07/drew_court.

[32] *See Technical Report: An Estimate of Infringing Use of the Internet*, ENVISIONAL REP., LTD. (Jan. 2011), http://documents.envisional.com/docs/Envisional-Internet_Usage-Jan2011.pdf.

[33] *See, e.g.*, Anonymous, Comment to *Caption Contest: Three Chiefs*, ABOVE THE LAW (Sept. 5, 2014), http://abovethelaw.com/2014/09/caption-contest-three-chiefs/ (providing an example of vitriolic anonymous comments).

[34] *See generally*, AUTOADMIT, http://www.autoadmit.com (last visited Sept. 5, 2014) (a law school discussion board comprising of anonymously authored posts).

[35] *See* Brian Ross, *While America Slept: The True Story of 9/11*, ABC NEWS (July 29, 2011), http://abcnews.go.com/Blotter/ten-years-ago-today-countdown-911/story?id=14191671#all.

[36] *See id.*

[37] *See id.*

[38] *See id.*

[39] *See generally* Terry W. Lynch, *Nameless, Faceless Comments Fading*, USA TODAY, Mar. 6, 2014, at 6B (discussing the debate on anonymous website comments).

[40] *See id.*

[41] Warner Bros. 2005.

mask worn by the hero of the film, who used terrorist tactics to achieve political ends.[42] The Guy Fawkes mask has popped up at political rallies, apparently in conscious imitation of the title character in *V for Vendetta*.[43]

Anonymity has venerable historical roots in political, religious, and social revolutions.[44] Many religious sects, including early Christians, survived only because they were able to keep their membership secret until they gained the critical mass to come out in the open.[45] Similarly, the Federalist Papers and many other Revolution-era pamphlets were circulated anonymously.[46]

More recently, Mark Felt—known for decades only as Deep Throat—revealed to Washington Post reporters Woodward and Bernstein (a.k.a. Robert Redford and Dustin Hoffman)[47] secrets about the Watergate cover-up that led to the resignation of President Nixon and the conviction of several White House officials.[48] Deep Throat's identity did not become public until 2005 when he outed himself in an effort to reap some of the adulation and glory that he had been denied for three decades while he remained anonymous.[49] Just in time, too, as Deep Throat died not long after

---

[42] *Id. See also* Nick Bilton, *Masked Protesters Aid Time Warner's Bottom Line*, N.Y. TIMES, Aug. 29, 2011, at B4; Tim Murphy, *The Last Laugh, 500 Years Later*, N.Y. TIMES, Oct. 30, 2011, at ST6.

[43] Bilton, *supra* note 42; Murphy, *supra* note 42.

[44] Victoria S. Ekstrand, *The Many Masks of Anon: Anonymity as Cultural Practice and Reflections in Case Law*, 18 J. TECH. L. & POL'Y 1, 11–14 (2013).

[45] *See* Dr. Sophie Lunn-Rockliffe, *Christianity and the Roman Empire*, BBC HISTORY, http://www.bbc.co.uk/history/ancient/romans/christianityromanempire_article_01.shtml (last updated Feb. 17, 2011) (discussing the persecution of Christians throughout history).

[46] Eckstrand, *supra* note 44, at 14. *See also* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 360 (1995) (Thomas, J., concurring).

[47] *See* ALL THE PRESIDENT'S MEN, (Warner Bros. 1976) (starring Dustin Hoffman and Robert Redford as the Washington Post reporters that used "Deep Throat" as a source). *See also* David Von Drehle, *FBI's No. 2 was 'Deep Throat': Mark Felt Ends 30-Year Mystery of The Post's Watergate Source*, WASH. POST, June 1, 2005, at A1.

[48] *See generally* CARL BERNSTEIN & BOB WOODWARD, ALL THE PRESIDENT'S MEN (40th Anniversary ed., 2014) (1974) (written by Washington Post reporters, detailing the Watergate scandal and the use of their source "Deep Throat" to uncover important information). *See also* Karlyn Barker & Walter Pincus, *Watergate Revisited*, WASH. POST, June 14, 1992, at A1; Von Drehle, *supra* note 47.

[49] Von Drehle, *supra* note 47.

disclosing his identity, hopefully still basking in the afterglow of his self-revelation.[50]

The Internet has, of course, created new opportunities for those who would use anonymity as a tool for social and political change. The release of classified military documents to WikiLeaks is a recent example of someone who hoped to use the cloak of anonymity to influence political processes,[51] as the Pentagon Papers had done four decades earlier.[52] Another example is the internet meme "Anonymous"—a loosely associated group of online activists that band together for concerted action on a variety of political and economic issues.[53] Such activities are sometimes referred to as "hacktivism."[54]

But, of course, one man's social protest is another man's vandalism. So, while many Americans admire anonymous rebels who disrupt society to achieve political ends, many others find the concept of an anonymous cyber–mob very scary.[55] Take, as an example, Aaron Swartz, "organiz[er] and webiz[er]" of "The Unofficial Judge Alex Kozinski Site,"[56] who also happened to moonlight as a dotcom millionaire and notorious hacktivist.[57] Many remember Swartz as a hero of open-source initiatives and effective, albeit subversive, public advocacy; yet he was also an alleged cyber-criminal, relentlessly hounded and pursued by our government.[58]

---

[50] Patricia Sullivan & Bob Woodward, *'Deep Throat' Mark Felt Dies at 95*, WASH. POST, Dec. 19, 2008, at A2.

[51] *See* Julie Tate, *Manning is Sentenced to 35 Years for Leaks*, WASH. POST, Aug. 22, 2013, at A1, A4.

[52] *See* David Rudenstine, *The Pentagon Papers Case: Recovering Its Meaning Twenty Years Later*, 12 CARDOZO L. REV. 1869, 1869 (1991).

[53] *See* David Kushner, *The Masked Avengers: How Anonymous Incited Online Vigilantism from Tunisia to Ferguson*, NEW YORKER, Sept. 8, 2014, at 52.

[54] *See id.* at 50.

[55] *See id.* at 56–57.

[56] THE UNOFFICIAL JUDGE ALEX KOZINSKI SITE, http://notabug.com/kozinski/ (last visited Sept. 12, 2014).

[57] John Schwartz, *Internet Activist, A Creator of RSS, Is Dead at 26, Apparently a Suicide*, N.Y. TIMES, Jan. 13, 2013, at A25.

[58] Justin Peters, *The Idealist*, SLATE (Feb. 7, 2013), http://www.slate.com/articles/technology/technology/2013/02/aaron_swartz_he_wanted_to_save_the_world_why_couldn_t_he_save_himself.html. Swartz took his own life on January 11, 2013, almost two years after he was first indicted for multiple federal felonies, based on his unauthorized download of thousands of academic articles from JSTOR. *Id.*

When anonymity strikes hard at our core values—as happened on 9/11—most of us are happy to trade a great deal of anonymity for a small measure of security. Cast your minds back to the days following the 9/11 attack. We had been attacked on our own soil by an enemy that had infiltrated our borders and used our own airplanes as weapons against us.[59] Nobody in our government noticed a thing until the planes started hitting buildings.[60] Afterward, I don't remember very many voices crying out that we had too much government surveillance. Instead, there were tons of complaints that the government hadn't been vigilant enough and hadn't looked for unusual patterns that would have caused the anonymous terrorists to stick out.[61]

And there were few protests when Silk Road was closed down and its operators arrested.[62] Government officials, in their public statements, positively reveled in their ability to pierce the veil of internet anonymity.[63] As Keith Bristow, director of Britain's National Crime Agency, put it, "These arrests send a clear message to criminals: The hidden Internet isn't hidden, and your anonymous activity isn't anonymous. We know where you are, what you are doing and we will catch you."[64] Yeah, right.

The government's attempts to isolate and weed out nefarious activities has an inevitable and incorrigible effect on private citizens. The government can only identify unusual or atypical patterns if it figures out what is usual and typical—which it can only learn by looking at a lot of ordinary people. It would be very nice, indeed, if terrorists were to list their occupation on

---

[59] Serge Schmemann, *US Attacked: Hijacked Jets Destroy Twin Towers and Hit Pentagon*, N.Y. TIMES, Sept. 12, 2001, at A1.

[60] NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES: EXECUTIVE SUMMARY, 1–2 (2004).

[61] Kurt Eichenwald, Op-Ed., *The Deafness Before the Storm*, N.Y. TIMES, Sept. 11, 2012, at A23.

[62] *See* Alex Hern, *FBI Pranked by Furious Bitcoin Users Since Silk Road Shutdown*, GUARDIAN (Oct. 7, 2013, 8:08 AM), http://www.theguardian.com/technology/2013/oct/07/fbi-bitcoin-pranked-silk-road (showing only 200 messages in protest sent to the FBI).

[63] *See* Press Release, FBI New York Field Office, *Manhattan U.S. Attorney Announces Seizure of Additional $28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website*, (Oct. 25, 2013), http://www.fbi.gov/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website.

[64] Leger, *supra* note 20.

their passports and give advance notice to the authorities that they planned to launch a terrorist attack—just to be good sports. But terrorists and other wrongdoers aren't good sports. They exploit the weaknesses of our open society, and the only practical way to head them off before they cause harm is for the government to look at everything and everyone to try to figure out who means to do us harm.

This has been the project of the last thirteen years since 9/11. It started with the widely-ridiculed Total Information Awareness program.[65] But government surveillance has gotten a lot more sophisticated since then. In 2013, the NSA opened a state-of-the-art facility "to intercept, decipher, analyze, and store vast swaths of the world's communications."[66] Working with computers of unimaginable speeds—ten to twenty petaflops for starters—and gathering data at the rate of twenty terabytes per minute, for a total storage capacity that may amount to a yottabyte of data (that would be over a trillion terabytes),[67] the facility is designed to sweep in and analyze "private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails [like] parking receipts, travel itineraries, bookstore purchases, and other digital 'pocket litter.'"[68] The facility is at the core of what some have called the NSA's "collect-it-all" strategy.[69] That strategy involves amassing an extraordinary amount of private information about U.S. citizens, authorized in large part by bulk data collection warrants issued by the Foreign Services Intelligence Court under § 215 of the Patriot Act.[70]

---

[65] *See* Farhad Manjoo, *Total Information Awareness: Down, But Not Out*, SALON (Jan. 29, 2003, 3:33 PM), http://www.salon.com/2003/01/29/tia_privacy/.

[66] Rory Carroll, *NSA Data Centre Opening Delayed After Series of Electrical Surges in Utah*, GUARDIAN (Oct. 8 2013, 3:47 PM), http://www.theguardian.com/world/2013/oct/08/nsa-data-centre-utah-electrical-surge; James Bamford, *The NSA is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 15, 2012, 7:24 PM), http://www.wired.com/2012/03/ff_nsadatacenter/all/.

[67] Lucas Mearian, *From Bits to Yottabytes. How Much Data Is That?*, COMPUTERWORLD.COM (Feb. 23, 2007, 12:59 PM), http://www.computerworld.com/article/2476838/data-center/from-bits-to-yottabytes--how-much-data-is-that-.html.

[68] Bamford, *supra* note 66.

[69] Glenn Greenwald, *The Crux of the NSA Story in One Phrase: 'Collect it All'*, GUARDIAN (July 15, 2013, 6:40 AM), http://www.theguardian.com/commentisfree/2013/jul/15/crux-nsa-collect-it-all.

[70] *See Section 215 of the USA PATRIOT Act*, ELEC. FRONTIER FOUND., https://www.eff.org/foia/section-215-usa-patriot-act (last visited Sept. 5, 2014). *See also* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM

We discovered the true scale of NSA surveillance in 2013 when Edward Snowden released documents relating to a litany of government programs, most notably Prism—through which the NSA can obtain the contents of private emails, chats, photos and other media stored by companies like Google and Facebook[71]—and XKeyscore, a program that "allows [NSA] analysts to search with no prior authorization through [the] vast databases" of private online information that the agency is continuously collecting.[72]

The aim of all this data collection is to detect the types of patterns and connections that would make terrorist activities stand out.[73] It's hard to argue with the objective, of course. We all want to be safe from terrorists and other nefarious actors. And many people would not be the least offended by having their personal data stored and analyzed by a computer. After all, a machine can't think, it can't make judgments about your personal life, it can't really "know" who you are the way a human being does. And a machine cannot gossip about you, blackmail you, or release damaging or embarrassing information to your enemies. So you might applaud the effort to gather your data, along with that of millions or billions of other people, and use it as a background—a sort of chaff—that would make the activities of evildoers stand out by contrast.

But the line between anonymity and privacy can be very fuzzy. I would offer at least three cautions if you believe you can maintain your privacy because the government is looking for bad guys and you're not a bad guy. First, you could easily become a focus of the government's attention by interacting, even remotely and accidentally, with someone who is a target. The comprehensive nature of the data gathering operation and the lightning speeds with which the data is processed means that the government can keep an eye on a great many people at once, and you may well wind up being one of them for some totally innocent reason. Misdial a phone number that happens to be used by suspected terrorists and you (and your entire contact list) could become a subject of government attention.

OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (PRE-RELEASE) (2014).

[71] Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[72] Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'*, GUARDIAN (July 31, 2013, 8:56 AM), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

[73] Greenwald & MacAskill, *supra* note 71.

Using software developed by a company named Narus, the government can "conduct 'deep packet inspection,' examining internet traffic as it passes through . . . 10-gigabit-per-second cables at the speed of light" for "target addresses, locations, countries, and phone numbers, as well as watch-listed names, keywords, and phrases in email."[74] "[C]ommunication that arouses suspicion . . . [is] automatically copied or recorded and then transmitted to the NSA."[75] I wouldn't be surprised if the research I did using my TOR browser triggered the focus of some government attention in my direction.

The second caution I would offer is that it takes surprisingly little trivial information about an individual to pinpoint his identity. Steve Engel managed to identify David Lat based on two facts Lat mentioned on his blog: his Yale connection and his Supreme Court interviews.[76] Back in 2006, AOL released 20 million web search queries by over half a million of its customers.[77] The customers were identified by numbers so as to protect their privacy.[78] AOL released the data to help academic research,[79] and it certainly did. In no time at all, the data for a particular customer assigned the number 4417749 revealed that this was a woman by the name of Thelma Arnold, aged 62 and living in Lilburn, Georgia.[80] Thus, the flotsam and jetsam of even a few months of your online activity, if compiled and analyzed, can paint a very clear picture of who you are and what you're up to.

Third, once you start mining the data for terrorists, it's an easy step to also look for other criminal activities, such as drug importation or money laundering. One logical step leads to another until you then have a much broader surveillance system in place than the one you started out with.

I have some personal experience with this. About thirteen years ago, right before 9/11, some of my colleagues and I discovered that the Administrative Office of the United States Courts—in other words, the bureaucrats in Washington who administer the federal judiciary—had installed monitors at our internet gateways, and these monitors were set to detect various types of communications, specifically when someone within the judiciary accessed internet porn and gambling sites. The monitoring had

---

[74] *See* Bamford, *supra* note 66.

[75] *Id.*

[76] *About Me*, *supra* note 9.

[77] Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A1.

[78] *Id.*

[79] *Id.*

[80] *Id.*

been implemented without approval of the judiciary's governing body, which is made up entirely of judges (as you would expect). The monitoring was discovered when the AO, as the Administrative Office of the United States Courts is known, started sending out letters to various chief judges, attaching long print-outs of salacious web traffic and suggesting that the responsible employees be disciplined.

The monitors came about innocently enough. The federal judiciary has a huge intranet: we communicate with each other by e-mail, have internal websites and data transmissions, etc. So long as you communicate from one point within the judiciary to another point within the judiciary, your communication is protected within our firewall. But if you send an e-mail or access a web page outside the judiciary, your communication needs to pass through one of the electronic gateways that connect our intranet to the Internet. For example, if a judge in Kansas City wants to access a web page hosted on a server in New York, he'll type a command into his browser. The command travels to the designated gateway, and from there it hops various servers to reach New York. The page sent back travels the reverse journey through the same internet gateway.

At that time, denial of service and tunneling attacks were quite common, and some in the judiciary feared we could be a target. So the AO decided to install monitors at the gateways—computers that examine all of the data traveling through—to try to detect such attacks. For example, if the monitor noticed 500 identical signals from the same IP address in rapid succession, it would bring the situation to the attention of a human being who would figure out if we were under attack and take any necessary defensive measures.

So far so good. But once you have a monitor in place, why stop with denial of service attacks? Because the monitors look at all data going across the gateway, they could easily be set to identify any other pattern that someone might be interested in—sex.com, gamblers.com, newyorktimes.com or, for that matter, "Alex Kozinski." Commands are nothing but strings of code, and it was simplicity itself to set the monitors to look not only for attacks but also for people accessing saucy websites. As often happens, the possible became the inevitable, and the monitors were programmed to detect commands accessing certain websites.

It may well be that, just as nature abhors a vacuum, society abhors anonymity and seeks to develop mechanisms for pulling all of us back under

the watchful eye of the community. No man, after all, is an island.[81] Quite aside from the NSA, there are many other eyes watching what we do: phone companies can log whenever we connect to cell towers and thereby keep close track of our movements;[82] RFID chips in Fast-Trak devices can provide a map of our travels by car;[83] the government is amassing an ever-increasing supply of DNA samples in the CODIS database,[84] as state and federal governments widen the scope of who is subject to DNA typing.[85] A company called "PlateNet," using a fleet of cars that roam the streets scanning license plates, has created a giant police-accessible database to store the location and movement of millions of vehicles.[86] Cities like London have developed ubiquitous networks of cameras that record the public movements of thousands of people every hour.[87] Face-recognition and gait-decoding technologies capable of recording the whereabouts of large throngs of people are used in many places abroad and are starting to be deployed by law enforcement in the United States.[88] "Smart meters" installed in millions of American homes can record and divulge exactly which home appliances an occupant is using based on the distinct energy

---

[81] JOHN DONNE, DEVOTIONS UPON EMERGENT OCCASIONS: MEDITATION XVII (1624), *reprinted in* THE NORTON ANTHOLOGY OF ENGLISH LITERATURE 628, 629 (Stephen Greenblatt & M.H. Abrams eds., 8th ed. 2006).

[82] *See* Charles Arthur, *iPhone Keeps Record of Everywhere You Go*, GUARDIAN (Apr. 20, 2011, 9:06 AM), http://www.theguardian.com/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears.

[83] *See* Mark Baard, *Watchdogs Push for RFID Laws*, WIRED (Apr. 5, 2004), http://archive.wired.com/politics/security/news/2004/04/62922.

[84] *See* Andrea Roth, *Maryland v. King and the Wonderful, Horrible DNA Revolution in Law Enforcement*, 11 OHIO ST. J. CRIM. L. 295, 295 (2013) ("The Federal Bureau of Investigation . . . boasts that its Combined DNA Index System [CODIS], a group of state and federal databases containing over ten million profiles, has been responsible for over 219,700 hits assisting in more than 210,700 investigations.").

[85] *Id.*

[86] *How Does PlateNet Work?*, PLATENET, https://www.platenet.com/praweb/howitworks.jsf (last visited Sept. 13, 2014). PlateNet claims to have over 250 million license plate scans in its database. *Id.*

[87] *See* Paul Lewis, *You're Being Watched: There's One CCTV Camera for Every 32 People in UK*, GUARDIAN (Mar. 2, 2011, 4:19 PM), http://www.theguardian.com/uk/2011/mar/02/cctv-cameras-watching-surveillance.

[88] *See New Facial, Gait Recognition Software to be Integrated in CCTVs*, HOMELAND SEC. NEWS WIRE (Feb. 25, 2009), http://www.homelandsecuritynewswire.com/new-facial-gait-recognition-software-be-integrated-cctvs.

consumption pattern of each device.[89] And, of course, companies such as Google, Facebook and Double Click are constantly tracking our online presence[90]

It is entirely possible that, even as we speak, the idea that any one of us is ever anonymous—even in a strange city in the middle of a crowd—is an illusion. In terms of anonymity, we may well be back to the days of the village or township. Except that our neighbors now not only know all of our movements, activities and contacts, but they can also look into our yards and have a pretty good idea what's going on in our heads by mining the cookie-crumb trail of electronic detritus that we routinely shed as a concomitant of daily life.

Which leaves the question: Is there a right to anonymity? The European Court of Justice held in *Google Spain v. Mario Costeja González*[91] that there is a "right to be forgotten," which is fairly close.[92] But, so far, no American court has recognized a similar right.[93] The Supreme Court has dealt with anonymity only rarely, and with mixed results.[94]

In 1958, the Court held in *NAACP v. Alabama*[95] that the NAACP had a First Amendment right to keep its membership list confidential, reasoning that disclosing the information in response to the state's subpoena would interfere with the members' right to associate.[96] And in 1960, the Court, in

---

[89] *See* Sonia K. McNeil, Note, *Privacy and the Modern Grid*, 25 HARV. J. L. & TECH. 199, 204–05 (2011) ("Individual appliances and other sources of energy use have unique 'load signatures,' which are the distinct energy consumption patterns specific to each source. A refrigerator, for example, draws power in a different way than a television, a respirator, or high-wattage indoor marijuana 'grow lights.'").

[90] *See* Elizabeth Dwoskin, *Web Giants Threaten End to Cookie Tracking*, WALL ST. J., Oct. 28, 2013, at B5.

[91] Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=64543 (May 13, 2014).

[92] *Id.*

[93] *See* Jasmine E. McNealy, *The Emerging Conflict Between Newsworthiness and the Right to be Forgotten*, 39 N. KY. L. REV. 119, 133 (2012). *See also* Douglas J. Sylvester & Sharon Lohr, *The Security of our Secrets: A History of Privacy and Confidentiality in Law and Statistical Practice*, 83 DENV. U. L. REV. 147, 173 (2005).

[94] *See* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958); Branzburg v. Hayes, 408 U.S. 665 (1972); McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995); McConnell v. Fed. Elections Comm'n, 540 U.S. 93 (2003).

[95] 357 U.S. 449 (1958).

[96] *Id.* at 462, 466.

Talley v. California,[97] struck down, under the First Amendment, an ordinance that prohibited the distribution of any handbill that didn't have printed on it the names and addresses of anyone who prepared, distributed, or sponsored it.[98]

But twelve years later, in *Branzburg v. Hayes*,[99] the Court held that reporters do not have a First Amendment privilege to keep news sources confidential.[100] Swinging back in the other direction, the Court in *McIntyre v. Ohio Elections Commission*[101] held that under the First Amendment, the state could not force an author of a handbill distributed in support of a ballot measure to disclose her identity.[102] But eight years later still, in *McConnell v. FEC*,[103] the Court upheld various disclosure requirements of the McCain-Feingold Campaign Finance Reform Act.[104]

My best guess is that there is a limited right to anonymity when it comes to political speech and association, but that right will not trump other concerns—such as anonymous campaign contributions that could be disguised bribes.

The question remains whether there is a more general right to anonymity aside from speech or association. My guess is there isn't, at least not in the Constitution. Privacy is protected by the Fourth and Fourteenth Amendments,[105] but it's difficult to find a constitutional anchor for blanket anonymity. While I don't rule out the possibility that such a right will be developed if the appropriate case comes along, it is likely to be a relatively anemic right, if it exists at all.

---

[97] 362 U.S. 60 (1960).

[98] *Id.* at 61.

[99] 408 U.S. 665 (1972).

[100] *Id.* at 667.

[101] 514 U.S. 334 (1995).

[102] *Id.* at 357.

[103] 540 U.S. 93 (2003), *overruled in part by* Citizens United v. Fed. Elections Comm'n, 558 U.S. 310 (2010).

[104] *Id.* at 143–223 (discussing constitutionality of provisions in the Act, formally known as the Bipartisan Campaign Reform Act of 2002). *See also* Adam Liptak, *On Campaign Finance, Rulings for Advocacy Groups and Against Parties*, N.Y. TIMES, Mar. 27, 2010, at A13.

[105] U.S. CONST. amend. IV, XIV. *See also* Thornhill v. Alabama, 310 U.S. 88, 95 (1940) (holding freedom of speech and freedom of the press are protected by the First Amendment against abridgment by the United States, and are further protected as fundamental rights by the Fourteenth Amendment against abridgment by a state); Mapp v. Ohio, 367 U.S. 643, 655 (1960) ("the Fourth Amendment's right of privacy has been declared enforceable against the States through the Due Process Clause of the Fourteenth" amendment).

Why? Because—unlike privacy, speech, association and the rights connected with criminal process—we do not have a societal consensus that anonymity is inherently good. We all think it's great for us, but we're not so sure we trust other people with it. Some scary things happen when people are—or feel to be—anonymous, and any right that has such highly anti-social aspects is unlikely to be greeted with enthusiasm by the Supreme Court.

That means that if a right to anonymity is to exist, it must come from Congress and the state legislatures. And it must be a finely sculpted right that takes into account both the good and the bad aspects of anonymity. Anonymity may well be one of the key policy issues of the 21st century and beyond, and it is time to think seriously about how we are to develop informed and rational policies to strike the delicate balance required.