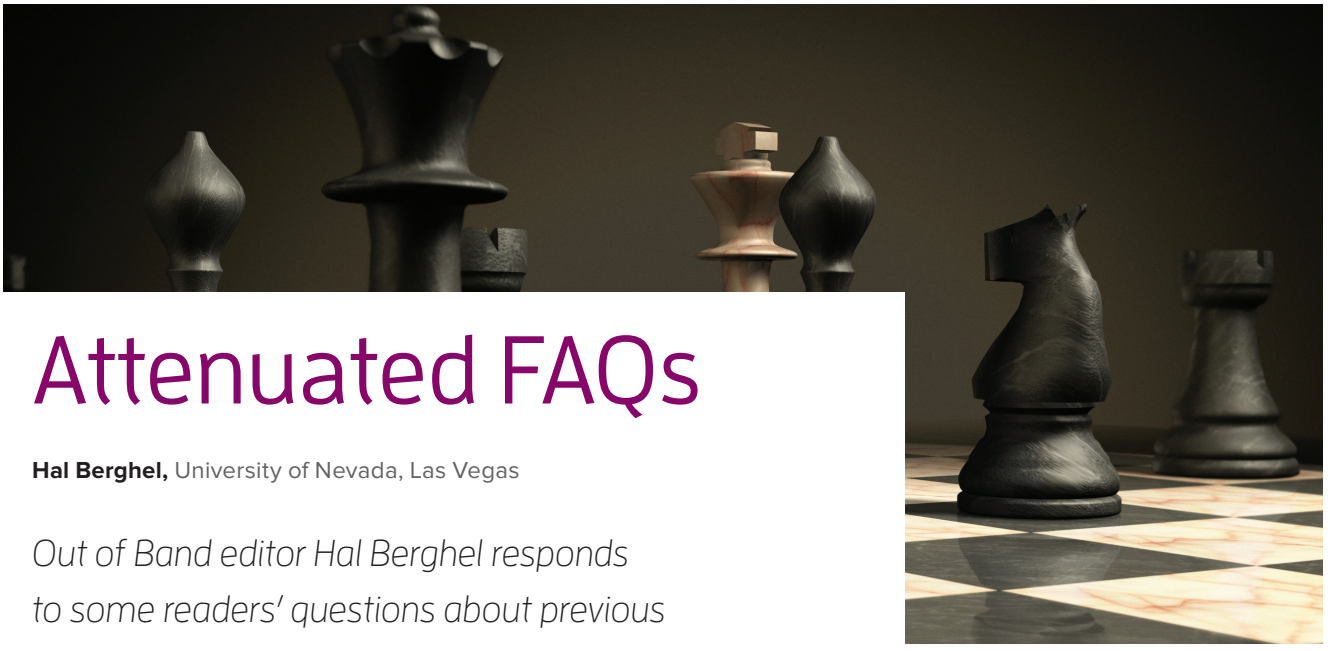
EDITOR **HAL BERGHEL**
University of Nevada, Las Vegas; hlb@computer.org



Attenuated FAQs

Hal Berghel, University of Nevada, Las Vegas

Out of Band editor Hal Berghel responds to some readers' questions about previous columns.

Over the years I've received great feedback about this column, and I'd like to share some of the exchanges I've had with readers. (Note: the original questions and answers might be altered from the email exchanges.)

EXPOSING PRIVACY EROSION

> *Do you think people are generally unaware or simply indifferent to the severity of privacy erosion? ("Defending against Big Dada: Defensive Tactics for Weapons of Mass Deception," vol. 47, no. 10, 2014, pp. 94–98)*

This is a mixed bag. Better-informed citizens are aware of the severity of privacy erosion. Information on this issue is available to those who take the time to look—the most reliable sources are from respected journalists, historians, and social scientists. Or, people can do their own analysis based on the wealth of ground-truth data available online; of course, this is a lot more work than relying on reliable print journalists and scholars. In my columns, I cite important, reliable sources. On the other hand, those who choose to get their information from the mass media outlets tend to be less concerned, because the dominant Orwellian "newspeak" holds that there's nothing to worry about.

Twenty years ago I was concerned that we were drowning in an ocean of Web guano—gratuitous multimedia, vanity home pages, poor scholarship, and sloppy journalism.[1] It's nearly impossible to find relevant information quickly (the needle-in-the-haystack phenomenon). The most insidious aspect of information overload is that misinformation dominates in most communication venues. I likened online information overload to the chatter problem that rendered citizens' band radio relatively ineffective by the 1980s. In both cases, the ultimate problem stems from the lack of user discipline. However, I failed to appreciate that the Web was a natural weapon of mass deception; I thought that we'd be able to deal with information overload with programs that served as information agents or customizers. I now realize that this analysis was simplistic. We need something akin to personal investigative agents, prosecutors, and judges. The weaponization of cyberspace has added a new dimension to Orwellian dystopia; indeed, Orwell might have had a clearer vision of the Internet's potential than his contemporary, Vannevar Bush.

For every insightful investigative journalist, there are legions of polemicists—many supported by "think tanks" (read: propaganda mills) with innocuous-sounding names. A few examples to illustrate this come from the past century. Award-winning environmentalist Rachel Carson almost single-handedly introduced the public to the harmful effects of pest-control regimens, and caustic ad hominem attacks from the chemical industry followed her until her death. The link between smoking and cancer

dates back at least as far as 1929, when Fritz Lickint and his colleagues published a case study on the subject; this held enough sway to give rise to the Nazi anti-smoking campaign. Although the proposition that smoking isn't healthy has been floating around for many decades, Big Tobacco has waged a continuous war against all critics, scientific and social, under the banner of "our product is doubt."[2] All too often, truth plays second fiddle to toxic messaging.

In government, secrecy is a cult that rarely works in the public's interest, and usually it's incompatible with a fully functional democracy.

BIGGEST PRIVACY THREATS

> *Do you see one particular entity—an agency, plan, platform, or something else—that's the most dangerous in terms of privacy? ("Mr. Snowden's Legacy," vol. 47, no. 4, 2014, pp. 66–70)*

The government three-letter agencies and the pure-play contractors that feed on them are the biggest threats. This was demonstrated in the materials leaked by National Security Agency (NSA) contractor Edward Snowden. In government, secrecy is a cult that rarely works in the public's interest, and usually it's incompatible with a fully functional democracy. This clearly isn't the message handed out by apologists for big-and-powerful government. The prevailing "govspeak" is that the important threats are inbound attacks from external sources such as criminals, terrorists, and hostile nation-states, and certainly not from internal government-led threats—that's inconceivable.

The more insidious threats are of course internal, for the simple reason that it's difficult to rally people around a threat coming from the very institution created to protect against such threats that also denies involvement. This is the issue behind the current flap between Apple and the Federal Bureau of Investigation (FBI) over the encrypted iPhone used by the perpetrators of terrorist attacks in San Bernardino, California. The official claim doesn't pass my smell test: the government can't protect us unless Apple rewrites their operating system with a built-in back door for the three-letter agencies. Give me a break! Thanks to Snowden, we know the NSA already had programs in place (such as XKeyscore, the Quantum programs, MARINA, and Pinwale) to collect and retrieve all mobile communications. So what was left to discover on the old iPhone that was worth unconstitutional intrusions into the operation of a premiere high-tech company?

When the NSA considers anyone looking for information on the Linux Journal suspicious (www.linuxjournal.com/content/nsa-linux-journal-extremist-forum-and-its-readers-get-flagged-extra-surveillance), we can't help but call into question their assessment of "relevance." The big-and-powerful government mantra says it all: "If you have nothing to hide, you have nothing to fear" (https://nsa.gov1.info/utah-data-center). That same tag line has been used by all recent tyrannies, by the way.

POINT OF NO RETURN

> *Are we at the point of no return: can we ever get our privacy back? ("Moral Hazards, Negative Externalities, and the Surveillance Economy," vol. 47, no. 2, 2014, pp. 73–77)*

If we're not at the point of no return, we can certainly see it from here. There are several independent, closely related, and powerful special interests at work that seek to compromise individual privacy expectations. But this is nothing new. Individual rights have always taken a back seat to the interests of federal and state governments in the US. Recall that at our country's infancy, the debate between the Federalists and the Anti-Federalists was not over individual sovereignty!

As it's currently used by politicians and ideologues, the term democracy is usually contrasted with tyranny. In that sense it has a certain memetic quality; it stands for the absence of tyranny, but not much more. Implicit in the notion of democracy proffered by the Founding Fathers was the recognition of the importance of the propertied class and the politics of advantage. There was never an inclination to extend the electoral franchise to the underrepresented subgroups identified by ethnicity, gender, sexual orientation, poverty, lack of education, and so on. Voting was restricted to people just like them: the white male propertied class—those rich, well-born, and able. They decided who qualified for inclusion into this auspicious group. Any government that empowered them, and only them, was by definition democratic—a view, incidentally, that wasn't too different from that in Plato's *Republic*. The principles of universal suffrage; one person, one vote; equality under the law; and the like have always been anathema to the power elite. Under the Three-Fifths Compromise included in Article 1, Section 2, Paragraph 3 of the Constitution, the dominant minority double dipped into the pot of power: not only weren't slaves (then representing 20 percent of the population) entitled to constitutional guarantees, they were only counted as fractional persons for purposes of apportionment so that the slave owners could derive an extra measure of political clout in Congress.

So it's in keeping with history that the ruling elite want protection of property and privilege against all threats foreign and domestic to be the top priority of their government—even at the cost of the average citizen's privacy. The power elite—described by C. Wright Mills in a book of the same name—are passionate about accumulating and holding onto their stuff.[3] That's far more important to them than individual privacy, individual sovereignty, protection against illegal search and seizure, freedom of speech, and all those other vestiges of what they consider quaint concessions toward populism.

In short, it doesn't look good on the privacy front because of the convergence of big-and-powerful government and authoritarian interests that are allied against it.

PRIVACY SUPPRESSION

> *People tell me "I'm not doing anything wrong, so I'm not worried what they find on me." Is this kind of thinking an obstacle for scholars such as yourself, who are trying to sound the warning? ("Secretocracy," vol. 49, no. 2, 2016, pp. 63–67)*

Privacy suppression has a chilling effect on free expression, full stop. People who don't mind being surveilled don't care about exercising their right to free expression—it's just that simple. And there's nothing wrong with that. However, they have no right to prevent the rest of us from exercising free expression. Therein lies the rub.

In computing terms, we should have to *opt in* to give up civil liberties. Big-and-powerful government types don't think we should have that choice. In fact, it's worse than that: they don't think we should be informed when we've lost these rights. That's why illegal domestic surveillance programs like the FBI's COINTELPRO program, the Central Intelligence Agency's (CIA's) HTLINGUAL program, and the NSA's MINARET and SHAMROCK projects were never seriously opposed by any members of Congress or presidential administrations while they were conducted.

When congressional overseers were told that Jane Fonda, Muhammad Ali, Art Buchwald, Senator Frank Church, and Dr. Benjamin Spock were dangerous domestic targets, they willfully acquiesced even though it was known that some of these programs were specifically designed to suppress free expression and civil rights. Was there any reasonable person at the time who felt threatened by Senator Church or Dr. Spock? Painting them as subversives was used justify a power grab.

There's no question that journalists, scholars, and open-minded intellectuals of all stripes were and are intimidated by big-government forces. In addition to reading the forewarning of George Orwell's or Aldous Huxley's works to understand the ultimate effect, I recommend civil rights attorney Glenn Greenwald's TED talk on this subject (www.ted.com/talks/glenn_greenwald_why_privacy_matters).

TECHNOLOGICAL BAD FAITH

> *I disagree that technologies are strictly neutral—their design influences, affords, and constrains the way they can be used. Atomic bombs aren't neutral. A phone network that requires the phone company's permission to attach a foreign device isn't neutral (and, as Langdon Winner would argue, the regulatory issues are as much a part of the technology "regime" as the wires and chips). ("Net Neutrality vs. Net Neutering," vol. 49, no. 3, 2016, pp. 73–77]*

I agree that there's something missing in my account, but it isn't the evil side of technology use. The use of atomic energy is ethically neutral: it can be used for bombs to be sure, but it can also provide inexpensive, green energy to the disadvantaged. As a technology, atomic energy is just a powerful tool. But as the reader and Langdon Winner[4] might point out, indeed that framework might need additional clarification.

That technology could be designed with ill intent from the start never occurred to me as I wrote the column. There's a difference between the technology's harmful effects and its ethics. That's the context that gives rise to phrases like negative externalities and collateral damage. Many argued during the Manhattan Project that although atomic weapons were designed with murder and mayhem in mind, the effort wasn't unethical as it was a defensive measure to offset capabilities of powerful adversaries in a two-ocean war. So I don't see the atomic bomb's creation alone as a counterexample; the particular uses, perhaps, but not the weapon as such and in general.

The problem with my generalization about technology's ethical neutrality is precisely this: it ignores the possibility that, from the beginning of a technology's design, unethical uses were the objective. It doesn't make sense to say that we only want that part of nuclear fission that can be used in power plants and medical laboratories. If you want atomic energy, you get atomic bombs as part of the package. Drone technology provides a more current example. Drones can be involved in military operations to avoid putting pilots at risk—a good thing. They can also be used to target civilians and produce extensive collateral damage—a bad thing. We shouldn't focus exclusively on the end use, we also need to consider the motives and intentions behind the technology—was the full intent disclosed when it was developed. The atomic bomb's ethical neutrality derives from the fact that everyone who knew about it was fully aware of the intended use.

The naivety of the technology-is-ethically-neutral position is subtle. It arises when technology is developed in bad faith (read: toward ends that

are both undisclosed and unethical to those who would be affected). Again, Winner's discourse on whether "artifacts have politics" is useful because he offers several examples.

So, what constitutes technological bad faith? We must look for socially unacceptable ulterior motives in the design and implementation, not in the end product. Presuming that the world's great manmade disasters still qualify as good-faith technology efforts, we're assuming that whatever the defects might have been, the results were never anticipated. Nothing, we presume, was held back. Although they might have resulted from human error, a lack of understanding, poor craftsmanship, or outright criminal neglect, all of these cases could be reasonably characterized as the results of unforeseen or unintended consequences.

Winner, in his counterexamples, claims that New York urban architect Robert Moses attached a social meaning to the low-hanging overpasses that he built on the parkways of Long Island. Without disclosure, Winner says, Moses fully intended them as a barrier to public transportation from the New York City boroughs to uphold social-class bias and racial prejudice. He made the parkway useless to the tired, poor, and huddled masses, so they would stay away.

To the extent that Winner and others' suggestion that designing immorality into a project isn't very unusual is true, my view that technology is inherently neutral must be considered incomplete. Although I focused on the ethical *use* of technology, Winner rightly shows that we must also examine the ethical *design* of technology. Bad-faith design—often with undisclosed political advantage in attendance—intentionally builds negative externalities into the product.

Are there other current examples of bad-faith design? I'll defer detailed discussion to another forum but technology-based offenders might be found in the hardware and software associated with digital voting, flash-trading systems, encryption and security products, government and contractor surveillance systems and databases, and so on. In general, the perps are likely to be found in the nexus of big government and big money.

> Healthy democracies maintain an equilibrium between respect for personal privacy (privacy), public awareness of what the government is doing (publicity), and the government's need to maintain secrets (secrecy).

THE SURVEILLANCE STATE

What's the impact of the surveillance state on civil liberties? ("Secretocracy," vol. 49, no. 2, 2016)

There are several civil liberties issues that mustn't be conflated. First and foremost are threats to constitutionally protected guarantees in the Bill of Rights—that is, freedom of speech, protection against unreasonable search and seizure, and so on. Second are infringements on privacy "rights" that are inferred from the so-called "penumbras" and "emanations" of other constitutional statutes and principles. Third is the government's intentional withholding of information on threat of punishment (secrecy)—especially through the Executive Orders (EOs) vehicle. These issues all have distinct legal and moral consequences, although they are tightly interwoven in law and policy.

Sociologist Edward Shils held that healthy democracies maintain an equilibrium between the respect for personal privacy (privacy), the public's awareness of what the government is doing (publicity), and the government's need to maintain secrets (secrecy).[5] He argued that the US lost this equilibrium in the 1950s, when privacy began to erode and secrecy began to dominate. The stress that citizens feel today is a product of this disequilibrium, which has worsened over time. This was the reason former Wisconsin Senator Russ Feingold gave for his singular opposition to the Patriot Act. This very disequilibrium is at the heart of the current debate on privacy and the surveillance state—although the debate has become very one-sided since the Patriot Act. This is a fascinating topic, and the best place to start is Sen. Daniel Patrick Moynihan's book, *Secrecy*.[6]

PII PROTECTION TACTICS

What's the best practice for protecting individual privacy? ("PII, the FTC, Car Dealers, and You," vol. 47, no. 5, 2014, pp. 102–106)

There are many answers to this. The vanilla, run-of-the-mill, corporate-friendly, chamber of commerce–and government-approved version can be found at the end of this link: www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure#offline. In addition, I offer two additional standards to protect personally identifiable information (PII) for your consideration.

The minimal standard

To deter identity theft:

- crosscut shred everything with PII on it;
- protect and conceal Social Security numbers (SSNs);
- don't use revealing data as user IDs and passwords;
- keep personal data in a small office/home office safe or safety deposit box;

- sanitize mobile devices (especially secondary storage) before yielding care, custody, or control;
- use long and complex passwords (25 characters and symbols);
- don't "overshare" social networking data;
- use security software; and
- don't leave mail in a mailbox unattended for long periods.

To effectively monitor financial/billing accounts:

- pay attention to arrival dates of financial documents;
- look for unauthorized credit charges or account creations;
- investigate surprising credit denial;
- get free annual credit reports from Experian, TransUnion, and Equifax;
- close unused accounts promptly; and
- keep PIN numbers hidden and concealed at point-of-sale terminals and ATMs.

The silver standard

To get ahead of privacy invaders, it's best to take matters more firmly into your own hands. What follows are suggestions for a more aggressive defense:

- Never give out your SSN to any nongovernment agency unless required by law to do so (such as to a bank or employer). Healthcare providers, car dealers, loan companies, and the like have no legal basis for requiring your SSN. If you're on Medicare or Medicaid, the Medicare number might be similar to your SSN, which is done for the convenience of their collections departments or agencies. Modern healthcare providers use insurance ID numbers, group plan numbers, and so on, for billing, not SSNs.
- Don't keep contact information on your person unless required by law. That way even if a criminal gets your wallet, they won't know where to find you. And then, in jurisdictions that allow it, driver's licenses, vehicle registrations, and the like should only have your PO box on it. Most states allow this, although there are a few states stuck in the Jurassic period of the information age that still require a street address.
- Internet data (email address, office info) should be munged to prevent Web harvesting by screen scrapers; "name at company dot domain" just won't cut it anymore with modern harvesters. Get creative. Even a JPG of your email address will thwart most screen scrapers—they're not that sophisticated. Use Captcha if you can. I use a rectified challenge (with no response required) that I call Gotcha.
- Don't give contact information to vendors and merchants. Car dealers, cell phone companies, and pharmacies don't need to know your land line, cell number, and address to sell you something.
- Don't save your home address on your GPS. Instead, use a major intersection a few miles from your house. If you can't find your way home from there, you probably shouldn't be driving.
- Don't use social networking. You're above that!
- Don't use search engines that store search data. DuckDuckGo is an attractive alternative in this regard.
- Sanitize all mobile devices, computers, and computer peripherals before repurposing. This especially relates to persistent storage media (disk, semiconductor, optical backups, and so on). Don't forget the secondary storage in your printer.
- Augment security software with browser add-ons (No Script, HTTPS Everywhere, and the like)
- Have mail delivered to a PO box.
- Don't look for silver bullets when it comes to protecting your privacy. There aren't any. The only defense is eternal vigilance. Remember that the two potential threat vectors that loom largest are criminals and your own government.

Needless to say, there's no gold standard available in surveillance states.

These are just a few of the thought-provoking questions that have come my way. I hope that you find these exchanges useful. And, by all means, keep those e-cards and e-letters coming.

REFERENCES

1. H. Berghel, "Cyberspace 2000: Dealing with Information Overload," *Comm. ACM*, vol. 40, no. 2, 1997, pp. 19–24.
2. N. Oreskes and E. Conway, *Merchants of Doubt*, Bloomsbury, 2010.
3. C.W. Mills, *The Power Elite*, Oxford Univ. Press, 2000, reprint (1956).
4. L. Winner, "Do Artifacts Have Politics?," *Daedalus*, vol. 109, no. 1, 1979, pp. 121–136; http://innovate.ucsb.edu/wp-content/uploads/2010/02/Winner-Do-Artifacts-Have-Politics-1980.pdf.
5. E. Shils, *The Torment of Secrecy: The Background and Consequences of American Security Policies*, Ivan R. Dee, 1996, reprint (1956).
6. D.P. Moynihan, *Secrecy: The American Experience*, Yale Univ. Press, 1999.

HAL BERGHEL is an ACM and IEEE Fellow and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.