Cutter IT Journal

The Journal of Information Technology Management

Vol. 29, No. 5
May 2016

"It should be readily apparent that information systems and technology pose a wide range of thorny ethical questions. Software, given its invisibility, provides tempting opportunities for unethical behavior."

— Robert N. Charette, Guest Editor

The Role of Ethics in Algorithm Design

CUTTER CONSORTIUM

Bad Faith Technology

by Hal Berghel

When discussing the morality of technology and its use, people tend to fall into two camps. On one side of the debate we have "anthropomorphists," who hold that technology can easily take on a moral character. They cite the atom bomb and Nazi gas chambers as examples of inherently immoral technology. On the other side are "amoralists," who claim that technology is ethically neutral and that the only ethical considerations derive from its actual use. This position has been likened to a soft form of social determinism whereby one would look to the social and cultural contexts in which a technology arises for ultimate judgment on its value and effect. In this account, it is the *use* of the technology in context that takes on moral character: it makes no more sense to attribute morality to technology than it does to rocks and fallen timber. However, there is an important intermediate case that both sides overlook: *bad actor technology* or technology offered in *bad faith*. In this article, I will try to expand upon the last clause of Kranzberg's First Law of Technology: "Technology is neither good nor bad; nor is it neutral."[1]

Those who claim technology is ethically neutral tend to focus attention on the underlying processes, to the exclusion of the original motivation. While I lean in this direction,[2] I recognize that bad actor/bad faith technology provides an important exception.

To amoralists, judging technology in ethical terms is a category mistake — it is as if we adjudge shoes by the paths traveled. However, in order to deal adequately with bad faith technology, we need to inject some measure of substantive assessment and recognize that as with due process of law, we must not ignore the circumstances that give rise to technology and the intention of the developers. As human artifacts, technologies must be evaluated in the social and political contexts in which they are embedded. An example or two will make the concepts clearer.

BAD FAITH TECHNOLOGY

Let's return to the original position described above — that some technology is unethical. Zyklon B, Nazi death chambers, the atomic bomb, land mines, torture devices of sundry stripe and form, and chemical and biological weapons are frequently used as examples of immoral technology. This turf is, of course, both slippery and slopey. Many lethal substances only become so when removed from natural settings (e.g., extracting ricin from the castor bean). This is usually not of practical concern, as intentions are normally clear. For example, there aren't too many biological weapons that I know of that were originally intended to be food flavorings or medicines. On the other hand, we can't blame the bean for the ricin.

So what would be our criterion for judging a technology as unethical? It would appear that we have to go beyond mere use to intention. If a technology itself is blameworthy, it derives its immoral status from the inception of the idea and whatever intention the designer had in mind. It is only in this way that we may separate technology with harmful effects from those that are legitimate candidates for immorality. If we don't take this step, it would appear that nuclear physicists, biological chemists, and weapons manufacturers would all have to share some responsibility for the ultimate effects. This is not to deny that there are people who *do* hold such positions; people who argue that ammunition manufacturers are partly responsible for homicides come to mind. However, in this article, we're going to focus on specific technologies and not deal with claims of inherent immoralities by category.

Let's frame our question thusly: is it possible to design a technology with unethical use in mind from the start? Phrased in this way, the inclination is to assent, yet examples that might qualify for the label of unethical may be difficult to find. What might qualify? I'll suggest that they will be technologies that (a) are inherently capable of being used in ways that society would adjudge unethical, immoral, or illegal, and (b) that the full intent of the designer(s) was not disclosed to the stakeholders (users, customers, stockholders, regulators, etc.) when the technology was developed. In this sense, we may say that the technologies were developed covertly. With these two conditions, we can still maintain the ethical neutrality of

the controversial technologies mentioned above, as all of the stakeholders were fully aware of their intended use.

WINNER'S THESIS

So what are purported bad faith technologies? As it turns out, political scientist Langdon Winner has given considerable thought to this topic.[3] He observes that "Unfortunately, a great many of the technical devices and systems that surround us are designed, built, and deployed in flagrant disregard of humane principles.... includ[ing] the waste of material resources; the destruction of living species and ecosystems; pollution of the air, land, and water; surveillance as a means of social control; and militarism as first response to disagreement and conflict."[4]

Winner is clearly correct in criticizing technology boosters who "have insisted that the 'biggest and best' that science and industry made available were the best guarantees of democracy, freedom, and social justice."[5] Today these boosters seem to champion the Internet as the liberating technology flavor of our time. Some have even given a name to the enthusiastic belief in technology's power to liberate: the Google Doctrine. In what is arguably the single most important piece of scholarship on this topic, Evgeny Morozov easily disposes of this naive doctrine as another case of foolish technopomorphism that seeks to imbue technology with such qualities as intention, resolve, purpose, and single-mindedness.[6] Morozov justifiably challenges the bogus claims of social media's liberating power in Iran's 2009 "Twitter Revolution." With the passage of time, we now see that Twitter and all of its Internet siblings had little enduring effect on the power elite — in the end tyranny, not Twitter, won the day.

Technologists should see through the hyperbole and recognize that the Internet (qua technology) is no more likely to set people free than rubbing a lamp will produce a genie. But the public gets caught up in the spin and becomes lulled into supporting foolish beliefs and counterproductive policies. Were similar claims made of fiberoptic technology or integrated circuits, they would be immediately dismissed as folly. But because of the ubiquity of the Internet and its importance in our daily lives (online shopping, video chatting, etc.), the claim attracts serious attention that it doesn't deserve.

Winner understands the absurdity of this technopomorphism and goes one step further by claiming that technology may on occasion take on an unethical quality that may go virtually undetected. If we adopt his broad sense of the "inhumane" — meaning not taking into account human concerns when a technology is designed or operated — then the Internet would be a prime example of this phenomenon. The Internet was built for technologists by technologists, whose primary concern in the early days was getting something to work, not anticipating that it would morph into what it is now.

In "Technologies as Forms of Life," Winner writes:

> the important question becomes, as we "make things work," what kind of world are we making? This suggests that we pay attention not only to the making of physical instruments and processes … but also to the production of psychological, social, and political conditions as part of any significant technical change.[7]

Once the Internet started to take off, these issues were pretty much ignored, so now we have an Internet that, according to Winner's definition, is inhumane: insecure, exploitative, and providing surveillance over hundreds of millions of individuals by private enterprise and the state. People are reportedly changing how they use the Internet for these three reasons; they also explain why there is a movement by many leading computer scientists to rebuild the Internet from scratch.

It's All About Intention

So what would constitute technological bad faith? Winner directs us to search for socially unacceptable ulterior motives behind the design and implementation of a technology, rather than study end use. Consequently, we can dismiss most of the world's great man-made disasters like the Tacoma Narrows Bridge collapse and the Fukushima Daiichi nuclear meltdown, as both still qualify as good faith technology efforts. These disasters may have involved human error, a lack of understanding, poor craftsmanship, or outright criminal neglect, but we can still reasonably characterize the results as unforeseen or unintended consequences.

Winner gets at the intention behind unethical technologies in two ways: "First are instances in which the invention, design, or arrangement of a specific technical device or system becomes a way of settling an issue in a particular community.... Second are cases of what can be called inherently political technologies, man-made systems that appear to require, or to be strongly compatible with, particular kinds of political relationships."[8] For example, Baron Haussmann built the broad Parisian thoroughfares, so admired today, at the direction of Louis Napoléon as part of the renovation of Paris. Their width was at least partly dictated by the desire to prevent the reoccurrence of street riots, such as those that occurred before and during the 1848 February Revolution that brought Louis Napoléon to power.

To give another example, Winner claims that New York urban architect Robert Moses attached a social meaning to the curiously low-hanging overpasses he built on the parkways of Long Island. Moses, acting out of social class bias and racial prejudice, fully intended his parkways to be a barrier to public transportation access to the borough by constructing the overpasses too low for buses to pass under them. The goal seems to have been to render public assets, such as popular Jones Beach, useless to the tired, poor, and huddled masses. Simply put, this is de facto segregation by class: the upper classes don't use mass transportation. Winner makes a good case that the low-hanging overpasses took on an unethical character as tokens of bad faith technology. I would note in passing that such examples tend to support a hard technological determinism: in this case the overpass technology directly impacted social and cultural norms. In a phrase, the overpasses exhibited bad faith design.

Langdon Winner rightly shows that we need also be concerned about the ethical intent of technology.

Winner and others suggest that designing immorality into a project is not that unusual. To the extent that this is true, my default position that technology is inherently neutral must be considered incomplete. My emphasis was on the ethical use of technology. Winner rightly shows that we need also be concerned about the ethical *intent* of technology. Consider two other examples Winner cites: the introduction of pneumatic molding machines to the McCormick reaper manufacturing plant in the mid-1880s and the introduction of the mechanical tomato harvester in California in the 1960s. In both cases, he argues, the technologies were specifically introduced to undermine the effectiveness of union organization by replacing the skilled workers who were union members. In the case of McCormick, the introduction of the new pneumatic molding technology actually created a loss for the company for three years, but by then union organization was broken. At that point, McCormick ripped out the technology.

In both of these instances, Winner argues, undisclosed political advantage was also in attendance. It is of considerable importance for society to address the extent of this phenomenon, in which technology is claimed to be employed for the user's benefit (e.g., to "improve customer convenience"), but is actually used to their detriment (e.g., secretly harvesting customers' personal information for future exploitation).

DIESELGATE

Careful observation will support Winner's thesis. By now we have all heard of the Volkswagen "dieselgate" scandal, which revealed that Volkswagen intentionally altered the control code in its turbocharged direct injection diesel engines to circumvent accurate testing of nitrogen oxide (NOx) exhaust emissions on as many as 11 million vehicles manufactured from 2009 to 2015. The cheating involved sensor-induced control code routines that resulted during the emissions testing procedure. This was detected by a university research team that was testing emissions during actual road trips rather than in stationary emission testing settings.[9] Volkswagen US President and CEO Michael Horn admitted that the company used a "software program that served to defeat the regular emissions testing regime,"[10] so there's no doubt at this point that the engine control program contained code that was specifically included to circumvent emissions compliance tests in violation of air quality laws. While VW has at times tried to diminish the scale of the culpability, it has not denied wrongdoing since the exposure.[11]

VW's infamous engine control system was apparently a descendant of some code changes developed by Audi engineers in 1999 as a means to quiet diesel engines.[12] Audi engineers found that their "acoustic mode" of operation not only silenced the engine, but also increased NOx emissions, so they shelved the software modifications. Parties as yet unidentified at VW apparently resurrected Audi's concept of multi-modal operation of the control system, but this time in reverse. The normal operation would be something like the "acoustic mode," but during emissions testing, the control system would sacrifice performance for compliance and switch to deceit mode. German auto parts maker Bosch GmbH warned VW in 2007 not to use software modifications to its engine management system to defeat emissions testing[13] but was ignored. It has since been discovered that VW was fined for using defeat devices to disable pollution control systems in 1973.[14] Further, an internal VW PowerPoint presentation has recently surfaced that discusses the deception regimen,[15] so emissions cheating takes on legacy status at VW. The Volkswagen diesel scandal is a recent confirmation of Winner's thesis that some technology is just unethical from the start.

We should note that this scandal satisfies both of our conditions for unethical technology in that it was inherently capable of being used in ways that society would

adjudge unethical, immoral, or illegal and that the full intent of the designer(s) was not disclosed to the stakeholders (users, customers, stockholders, regulators, etc.) when the technology was developed. In the VW case, there were no irregularities to be found in the supply chain. Nor did blatant consumer frauds take place. From a business process perspective, everything was in order after the design. What was not in order was the willful and intentional attempt to subvert environmental protection laws. At bottom, VW's innovative code might be meaningfully said to be unethical.

CONCLUSION

And so Winner's thesis is demonstrable. There are technologies that are created in bad faith by bad actors. Two questions arise. First, where would such technologies likely be found, and, second, what should be done about them?

In the IT world, likely places to look would be hardware and software associated with high stakes enterprises with little oversight and regulation in name only. My current candidates would include direct-recording electronic voting systems, flash trading systems, encryption and security products, government and contracted surveillance systems (e.g., Xkeyscore) and databases (e.g., no-fly lists, the NSA's PRISM program), commercial software with back doors, government-issued malware, ransomware (drive-by infectious websites), and so on. In general, the perpetrators of such threats are likely to be found in the nexus of big government and big money. The only reason that more VW-level scandals haven't been exposed is that tight control is maintained over proprietary information by big government and big business. In both cases, the default is to conceal anything that might prove embarrassing or encourage litigation. I predict that many more fruitful confirmations of Winner's thesis are only one whistle-blower away from public view.

So what should be done about such technologies? By the time some university researchers discovered the VW deception, scores if not hundreds of VW, Audi, and Bosch employees were aware of the problem, yet no one blew the whistle. Fear of reprisal is as great a deterrent to public disclosure of bad faith technology as it is to disclosure of government malfeasance. That's not likely to change unless whistle-blowing becomes far more lucrative.

A more subtle, but perhaps in the long run more effective, tactic might be to head off bad faith technology through the certification process. We can see that VW's behavior in its engine maintenance system code is in direct violation of portions of the ACM's Code of Ethics and Professional Conduct, to wit:

> Section 1.1 When designing or implementing systems, computing professionals must attempt to ensure that the products of their efforts will be used in socially responsible ways, will meet social needs, and will avoid harmful effects to health and welfare. In addition to a safe social environment, human well-being includes a safe natural environment. Therefore, computing professionals who design and develop systems must be alert to, and make others aware of, any potential damage to the local or global environment.
>
> Section 1.2 To minimize the possibility of indirectly harming others, computing professionals must minimize malfunctions by following generally accepted standards for system design and testing. Furthermore, it is often necessary to assess the social consequences of systems to project the likelihood of any serious harm to others.... In the work environment *the computing professional has the additional obligation to report any signs of system dangers that might result in serious personal or social damage. If one's superiors do not act to curtail or mitigate such dangers, it may be necessary to "blow the whistle" to help correct the problem or reduce the risk*.
>
> Section 2.3 ACM members must obey existing local, state, province, national, and international laws unless there is a compelling ethical basis not to do so.... If one decides to violate a law or rule because it is viewed as unethical, or for any other reason, one must fully accept responsibility for one's actions and for the consequences.
>
> Section 3.1 Because organizations of all kinds have impacts on the public, they must accept responsibilities to society. Organizational procedures and attitudes oriented toward quality and the welfare of society will reduce harm to members of the public, thereby serving public interest and fulfilling social responsibility. Therefore, organizational leaders must encourage full participation in meeting social responsibilities as well as quality performance.
>
> Section 4.2 Adherence of professionals to a code of ethics is largely a voluntary matter. However, if a member does not follow this code by engaging in gross misconduct, membership in ACM may be terminated.[16]

Without belaboring the point, a casual review of these fragments of the ACM code shows that the software developers involved in the VW scandal were poster children for distorted ethics and misplaced loyalties. Perhaps a solution to the bad faith technology challenge would be through increased awareness of ethical principles and closer scrutiny of applicable standards. This is best addressed at the university and even the high school level. The new high school Advanced Placement (AP) courses in computer science, for example, teach ethical principles as part of their curriculum.

Kranzberg's First Law, while true, is not really helpful. Perhaps a more useful guide would be to reevaluate the ethical standards we set for ourselves in terms of such things as ethical codes, duties, procurement policies, and the like. Perhaps if Volkswagen had been slapped with a 10% import tax after the 1973 disclosure, the 2015 disclosure wouldn't have happened. It is axiomatic that when ethical violations lead to no unpleasant consequences, we can expect a good deal more of them. Let the word go forth that bad faith technology is both real and unworthy of us.

ACKNOWLEDGMENT

My thanks to Howard Rheingold for encouraging me to revisit my naive default position that technology is inherently neutral.

ENDNOTES

[1]Kranzberg, Melvin. "Technology and History: 'Kranzberg's Laws.'" *Technology and Culture*, Vol. 27, No. 3, July 1986 (www.jstor.org/stable/3105385?seq=1#page_scan_tab_contents).

[2]Berghel, Hal. "Net Neutrality vs. Net Neutering." *IEEE Computer*, March 2016 (www.computer.org/csdl/mags/co/2016/03/mco2016030073.pdf).

[3]Winner, Langdon. "Do Artifacts Have Politics?" *Daedalus*, Vol. 109, No. 1, Winter 1980 (http://innovate.ucsb.edu/wp-content/uploads/2010/02/Winner-Do-Artifacts-Have-Politics-1980.pdf).

[4]Langdon Winner's Home Page (http://homepages.rpi.edu/~winner/).

[5]Winner (see 3).

[6]Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom*. Public Affairs, 2011.

[7]Winner, Langdon. "Technologies as Forms of Life." *The Whale and the Reactor: A Search for Limits in an Age of High Technology*. University of Chicago Press, 1989.

[8]Winner (see 3).

[9]Bigelow, Pete. "West Virginia Researcher Describes How Volkswagen Got Caught." autoblog, 23 September 2015 (www.autoblog.com/2015/09/23/researcher-how-vw-got-caught/).

[10]Chappell, Bill, "'It Was Installed for This Purpose,' VW's US CEO Tells Congress About Defeat Device." NPR, 8 October 2015 (www.npr.org/sections/thetwo-way/2015/10/08/446861855/volkswagen-u-s-ceo-faces-questions-on-capitol-hill).

[11]Cremer, Andreas. "VW Says CO_2 Emissions Scandal Not as Bad as Feared." Reuters, 9 December 2015 (www.reuters.com/article/us-volkswagen-emissions-carbon-idUSKBN0TS12I20151209).

[12]Ramsey, Jonathon. "Audi Invented the VW's Dieselgate System in 1999." The Drive, 21 April 2016 (www.thedrive.com/news/3104/audi-invented-the-vws-dieselgate-system-in-1999).

[13]Arvinth, Karthick. "VW Scandal: Carmaker Was Warned by Bosch About Test-Rigging Software in 2007." *International Business Times*, 8 September 2015 (www.ibtimes.co.uk/vw-scandal-carmaker-was-warned-about-test-rigging-software-2007-1521442).

[14]Gardella, Rich, and Mike Brunker. "VW Had Previous Run-In over 'Defeat Devices.'" CNBC, 23 September 2015 (www.cnbc.com/2015/09/23/vw-had-previous-run-in-over-defeat-devices.html).

[15]Ewing, Jack. "VW Presentation in '06 Showed How to Foil Emissions Tests." *The New York Times*, 26 April 2016 (www.nytimes.com/2016/04/27/business/international/vw-presentation-in-06-showed-how-to-foil-emissions-tests.html?ref=world&_r=1).

[16]"ACM Code of Ethics and Professional Conduct." ACM Council, 16 October 1992 (www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct).

Hal Berghel is currently Professor of Computer Science at the University of Nevada, Las Vegas, where he has previously served as Director of both the Schools of Computer Science and Informatics, and as Associate Dean of the College of Engineering. His research interests are wide-ranging within the binary and digital ecosystem, ranging from logic programming and expert systems to relational database design, algorithms for non-resolution-based inferencing, approximate string matching, digital watermarking and steganography, and digital security and privacy. Since the mid-1990s, Dr. Berghel has applied his work in digital security to law enforcement and intelligence gathering, particularly with respect to digital crime, digital money laundering, information warfare, and trusted identities. His research has been supported by both industry and government for over 30 years. In addition to his academic positions, Dr. Berghel is also a popular columnist, author, frequent talk show guest, inventor, and keynote speaker. For nearly 15 years, he wrote the popular "Digital Village" column for the Communications of the ACM, *and he has written the "Out-of-Band" column for* IEEE Computer *since 2011. Dr. Berghel is a Fellow of both the IEEE and the ACM and serves both societies as a Distinguished Visitor and Distinguished Lecturer, respectively. He can be reached at hlb@berghel.net.*