In formation Polity 27 (2022) 291–304

DOI 10.3233/IP-229007

IOS Press

An essay on complex problems and simple solutions: Techno-fallacies of the information age[1]

Gary T. Marx
M.I.T., USA
E-mail: gtmarx@mit.edu

For every complex problem, there is a solution that is simple, neat and wrong.

H.L. Mencken

It is not possible, and never will be possible, to predict the future. We are left with surmise, intuition, hunch, and hope.

R. Nisbet

This article identifies and critiques many of the broad justifications and assumptions underlying the technologically based, sense extending *new surveillance*.[2][3]

AI is a key factor in digitally dependent forms of surveillance from cell phones, to the internet, the body, home, banking, consumption, work, medicine, location, travel, criminal justice, national security and warfare. My emphasis is on the cultural beliefs that inform public opinion and serve as the background for the setting of policy, rather than with specific laws, regulations, or guidelines.

The digitalization of society reflects an optimistic, techno-surveillance world view located within a broader technocratic and commercial celebratory ethos. This article examines beliefs offered to the

[1] This article received a correction notice (Erratum) post publication with DOI 10.3233/IP-229012, available at http://doi.org/ 10.3233/IP-229012.

[2] This contrasts with *traditional surveillance* which relies on the unaided senses. Marx (2017, Ch. 2) offers a systematic contrast of the two forms involving numerous dimensions.

public by technophiles found within "the surveillance advocacy community". The intertwining of fact, logic, and values with truth and falsity are of course found in any social encounter or grouping. Yet they are particularly surfaced in times of crisis and contention, even as these vary from natural disasters to economic depressions to fears of witchcraft.

In periods of moral panic (Cohen, 2002; Goode & Ben-Yehuda, 1994) receptivity to sloppy magical thinking is pronounced. When the usual stanchions of meaning are undercut and people feel powerless, adrift and that something must be done (e.g., the current pandemic), we see the appearance of, and greater receptivity to, exaggerated beliefs and sloppy thinking. Novel times, lacking strong precedents, offer advocates freer range to make claims far beyond available evidence. Unleashed technologies, untested interventions and loony policy suggestions (drinking Bleach as a response to Covid) are prominent. Armies of moral and economic entrepreneurs appear to spread the word and for many persons common sense, let alone critical thinking, is suspended.[4]

In a recent book (Marx 2017, Chapters 7,8,9) I used fictional narratives devoted to work monitoring, policing and security and protecting children to illustrate 44 *techno-fallacies* of the information age.[5] I encountered the latter in decades of watching and listening to surveillance talk. Because of the book's space limitations, the fallacies were simply listed with little discussion. Here I offer a fuller discussion of some of the fallacies that are applicable to AI and related digital forms as expressed in myriad surveillance, monitoring, sorting, predictive and prevention technologies.

The fallacies do not represent ideology as a totalizing, monolithic, closed system. Rather, they are loosely constructed worldviews involving problem definitions, explanations, justifications, and directions for action. The surveillance ideas discussed share with more developed ideologies a certainty amidst unexamined assumptions, a mixing of facts and values and calls for action. Given the strongly felt pressures of the moment ("something must be done") and entrepreneurial zeal, such claims too often go unanalyzed.

The analysis of surveillance worldviews offered here is in the tradition of sociologist Karl Mannheim (1955) if more humbly and with awareness of the paradoxical nature of claiming that the outsider could be fully outside.[6] Some aspects of the views considered are empirically wrong, logically inconsistent, or morally questionable. But this critique is not a total rejection. The worldviews intermingle compelling values, facts and social analysis with the dubious and even the outrageous. It is the mixture that makes the topic compelling and challenging. Nor do I cover all the possible fallacies.[6]

The worldviews discussed here are not set apart from other ideological systems, which also contain inconsistencies, self-serving claims disguised as high principle, deceptive facades, misleading statements, empirical errors, and both unsupported and irrefutable claims. As will be briefly noted at

[4] I am grateful to Krystle Shore for suggesting the sub-type of "crisis-driven techno-fallacies". The causal links between the appearance of new beliefs and public "demand" and receptivity to them is relatively unstudied in different contexts, as is the nature, and career, of beliefs associated with different types of problem or crisis a technology addresses. The more traditional, clearly defined, narrower, static and isolated the problem, perhaps the greater the tilt to more supportable beliefs more supported by logic and evidence.

[5] Parts of the introduction and conclusion draw from the truncated chapter 12 in Marx 2017.

[6] Of course, Mannheim's independent analysts have social locations, interests and blind spots as well. Believing in empiricism, logic and the higher aspects of western civilization reflect value commitments. But there are some central differences as well, such as adhering to an open, self-interrogating critical standard beyond specific contexts and awareness of the impossibility of ever being fully outside. [6] The number of fallacies is already too long (and to honor one of them: more need not be better!). The initial draft of the book chapter (web.mit.edu/gtmarx/www/techno_fallacies.html) had 44. More could be added: confusing the simulacra with the phenomenon; saying I'm sorry makes it! More could be added: confusing the simulacra with the phenomenon; saying I'm sorry makes it ok; crooks and suspects have no rights; contemporary wars can be won with finality; if a democratically elected leader does it is not illegal; confusing what is possible with what is, or is likely; good motives excuse bad outcomes; imputing competent, technique based intentionality to outcomes we like in the face of fortuity, while imputing ill will, incompetence and conspiracy to outcomes we don't like; the rush to inherent trade-off talk before analysis and offering ways of weighing choices.

the paper's end, surveillance technophobes have fallacies as well. The dominant surveillance discourse is not necessarily richer in these than the belief systems of opponents (a task for systematic empirical research to determine). However, consistent with Gramsci's (Forgacs, 2000) observations, the technophilic views are *dominant,* and individuals are not equal in their ability to create and propagate surveillance worldviews. As such, there is a case for analyzing the dominant views in more detail.

1. Techno-fallacies

In years of listening to surveillance rhetoric I often heard things that, given my knowledge and values, sounded wrong, much as a musician hears notes that are off key. These involve elements of substance as well as styles of mind and ways of reasoning.[7]

Sometimes these fallacies are frontal and direct; more often they are tacit, buried within seemingly common-sense, unremarkable assertions. It is important to approach the commonplace in a critical fashion – whether for groups we disagree or agree with.

Some fallacies are empirically false or illogical. Other fallacies involve normative statements about what matters and is desirable. These reflect disagreements about values and value priorities. To label a normative belief a fallacy more clearly reflects the point of view of the labeler and goes beyond Mannheim's methodological neutrality. However, normative positions are often informed by empirical assumptions (for example, believing that negative sanctions work better than rewards as motivators). In sniffing out fallacies, one must identify and evaluate the intermingling of fact and value and the quality of the facts (Rule,1978; Bell, 1997). At a very general level, people often agree on values (though they often disagree over how to prioritize and implement these). Disagreements are more common over what evaluation measure(s) and specific tools for judgment are most appropriate and over how evidence is to be interpreted, with respect to what it says empirically and to it's meaning for a given value such as liberty or voluntarism.

I will consider two broad types of fallacy: those involving beliefs about technology per se and those involving humans and values.

1.1. Fallacies of technological determinism and scientific and technical perfection

With many of these fallacies we see logical and/or factual errors and faulty conclusions under the sway of technology infatuation and the engineering of social control. They reflect an overly optimistic, even utopian, faith in the efficacy of technology and its ability to solve problems without simultaneously creating new ones. The often disingenuous and self-serving hype of entrepreneurs can mask the role played by humans and the weakness of science in addressing and prioritizing value questions.

1.1.1. The fallacy of autonomous technology, emanative development, inevitable adoption and happy endings

The technology is seen to drive itself and follow an internal logic that must unfold. It's as if the technology resulted from immaculate conception, apart from human will or interests. This fallacy ignores the role of values, design, interests, contexts and contingencies in technical developments. Technology grows out of specific historical and social settings rather than being external to them.

[7] See for example Lee and Lee (1939), Lowenthal (1949), Shils (1956), Hofstadter (1965) regarding simplistic, manipulative, non-refutable, demagogic, sloppy, heated, energized, dark, conspiratorial, paranoid, apocalyptic, Manichean, true-believer rhetoric and propaganda that continue to find such fertile ground in sectors of the United States.

Maximal gains from technology are expected and likely costs (if acknowledged) are minimized. Here we see assumptions of inevitability and irreversibility and optimism regarding outcomes. The assumption of an unstoppable, progressive (in both a technical and social sense) logic of technological determinism obscures responsibility and alternative approaches, as well as history. The development of surveillance technologies is hardly self-evident. The statement, "you can't stop progress" cries out for social and cultural analysis of the meanings of progress. There are no natural laws that require particular technical developments and applications, and rarely can the social meanings and impacts of new technology be fully anticipated. We need to ask, "what are the likely consequences of using this technology, and how does its use compare to that of other technologies and to the consequences of doing nothing?"

1.1.2. The fallacy that greater expenditures and more powerful, sophisticated and faster technology will continually yield benefits in a linear fashion

This is the American-inspired ideal that bigger is better; it might be termed a techno-phallicsy as well. With respect to opening up the coffers and ratcheting up the technology, we face issues of appropriateness of the technology, proportionality, threshold and time frame. There's nothing inherently good or bad about the increased power of a technology. Our judgments must flow from analysis, not from the ability to increase the dosage. As Simmel (Coser, 1964) noted in situations of conflict, more may simply result in escalation, as opponents turn to equivalent means and discover ways of neutralization.

Greater speed can ironically offer advantages of currency and prevention but, in tandem with enhanced speed, there is less time for careful deliberation. Surveillance agents may tilt toward the kind of data that can be immediately gathered and processed, which may not be the kind of data that are most important or supportive of fairness or justice. With respect to linearity, as with medicine, one usually reaches a point where increases in dosage do not have equivalent therapeutic effects (e.g., some aspirin will help, but if you take the entire bottle, you may die).[8] This aspect is central to the next fallacy.

1.1.3. The fallacy that if some information is good, more is better

Issues of converting data to knowledge, data overkill, information glut, and drowning in data need consideration. For example, the East Germans were apparently able to tap most phone calls of West German and NATO officials, but do not appear to have been able to make very effective use of this. The quality not the quantity of information is what matters. The U.S. Census has found that samples of the U.S. population reveal more reliable data than is the case with data collection on the entire population.

Of course, the enlightenment heritage of asking questions and valuing knowledge is fundamental, but that doesn't mean that all forms of personal information must be widely available or maximally processed ("e.g., "we never know when we might need it"). Openness can have negative consequences in some contexts (e.g., diplomacy, strategic endeavors, manners). At times, it is morally, strategically and practically better not to know, and at other times, "it's none of your business".

1.1.4. The fallacy that technical solutions are always to be preferred

This is an error in both logic and definition. An even stronger version holds that when there is a technical problem (or better, a problem tied to the technology) there must be a technical solution. For example, a common response to problems created by Caller-ID (e.g., revealing unlisted numbers) or eavesdropping devices is to come up with a counter- technology that blocks or distorts. But such

[8] Yet in a wonderful example of the centrality of contingency, aspirin, even in small doses, can be harmful (e.g., for babies or people with blood clotting issues, etc.); thus there is a circumstantial element to appropriateness.

problems could also be addressed by regulating, prohibiting or limiting the technology and by education and manners. In a different context President Reagan's "Star Wars" program was a continuation of the early response to atomic weapons which involved building bomb shelters and bigger bombs. An alternative was to define the problem as calling for understanding of mutual grievances, negotiation and disarmament. Renee Shelby (2020) offers a nice example of how responsible design and more explicit attention to values embedded in technological solutions to sexual violence (rape kit, reporting app) could create more meaningful, victim-centered interventions.

Rarely will complex problems existing within contexts of human liberty, conflict, and creativity yield best (or only) to simple technical solutions based on stand-alone, causal explanations. Even when all goes according to plan, at some point, the technology may malfunction, and given enough time or cases, it is likely to. A society that can only maintain civil behaviour by technical means is a society in deep yogurt.

1.1.5. The fallacy that correlation must equal causality

This is a re-occurring failing of those in the persuasion business. Given dynamic conflict settings and a large number of interacting variables, it is often difficult to say with certainty that tactics work as well as advocates claim, nor that they fail as badly as critics claim, absent empirical specification and qualification.

A given cause or level of analysis is presented as sufficient for explaining and/or offering a simple (often unitary) solution. As the H.L. Mencken quote at the start of the paper implies, many problems have a multiplicity of causes at different levels, and the causes may show varied interactions (although if the Mencken quote is applied too universally, it illustrates its central idea). Also lurking here is the sub-fallacy of focusing on a minor cause. Misplaced responsibility is another sub-fallacy. Michael Welch (2003) shows how the moral panic of the 1990s led to the criminalization of immigration.

Even when very strong correlations are present, inferences of causality can be difficult to disprove. Consider a story about a young man who each evening played the flugelhorn in the town square. He refused any tips. When asked why he came each night to play, he responded, "to keep the elephants away". He was told, "there are no elephants here". To which he replied, "you see".

1.1.6. The fallacy that the facts speak for themselves

Data are not knowledge. Seeing should not automatically be equated with believing. The facts do not speak for themselves. They are inert artifacts. Any human knowledge, no matter how powerful, valid and useful is always abstracted out and partial. It represents a fraction of what might be attended to, and it might be intended to deceive.

Buried deep within this fallacy are sub-fallacies of literalism, universalism, sample representativeness and acontextuality. Here a normative principle or empirical finding is asserted with no qualifications or allowance for shadings, contingencies, mitigating circumstances, atypicality, or context.

The discretionary elements regarding measurement, standard-setting and interpretation must be seen. Alternative measures and seeing a fuller picture could suggest different meanings. To adequately interpret we need to know what is specific to the setting and how data determination and interpretation are constructed. "Objectivity" buried in tech narratives (along with strategic and heightened assumptions of risk) allow such practices to go unnoticed, much less critiqued.[9]

[9] A nice example of involving electronic location monitoring is in Shore (2021).

1.1.7. The fallacy of delegating decision-making authority to the machine

When human life and life chances are involved, there are risks in automatically delegating decisionmaking authority to a machine, absent human review, as commonly happens. As William James (1950) argued, "the art of being wise is the art of knowing what to overlook". Discretion – a capacity that is central to wise actions – can be severely limited by the automatic quality of the machine. As proponents claim, machines can be programmed to ignore variables deemed not to count by programmers such as religion or gender. Yet, because computer programs rely on selected broad categories of information, they are not equipped to deal with much of reality's richness, atypical cases and sudden, unexpected developments the way a human can. The nightmare version of this is a war automatically generated in response to faulty data from sensors. Elephants, as well as soldiers (one's own and adversaries), step on land mines.

1.1.8. The fallacy of explicit agendas

Beyond goals that are not unitary, well thought out or in conflict, surveillance advocates may deceive subjects and the broader public in the reasons they give for using a tactic. It is wrong to automatically assume that the technology is applied only for the publicly stated, rather than unstated, reasons, including obfuscation. Such proclamations may receive legitimation when offered by elites. But even when sincerely offered as ideals, applications on the ground may serve other goals, whether for practitioners or the organization. For example Benjamin Fleury-Steiner (2019) nicely illustrates how the rhetoric surrounding a web platform Amazon designed for ICE (the U.S.'s Immigration and Customs Enforcement agency) obscures and distorts ICE's objectives and abuses. Video surveillance ostensibly undertaken to counter theft has been used as a cover for gathering information during unionization drives.

In addition to asking what the agenda is, we must ask, "whose agenda? whose goals?". In settings of crisis and risk, with the blurring of lines between the public and the private, ostensibly public goals may be undercut by commercial goals and ostensibly caring goals may be overwhelmed by coercive goals. In delegating enforcement of red-light violations to private contractors, cities such as San Diego and Washington, D.C. ran the risk of confounding the ostensible goal of public safety and justice with the business goal of profit maximization. Beyond the private sector, the city, too, while talking about traffic rules (whether for speeding or parking) may have as a more basic goal maximizing revenue. The mixing or obfuscation of goals with such delegation can also insulate and distance government from accountability.

1.1.9. The fallacy of the sure-shot

Here we see a loose canon related to the fact that loose cannons may over-or under-shoot the target. This fallacy assumes that surveillance obtains its goal with laser-like precision and has no impact on adjacent or unintended targets and broader surroundings. But in a complex world much can go wrong and there are often missed shots and second order and spillover effects, as well as unrecognized tradeoffs. [10] The biases and failures of AI-fueled facial recognition technology (NIST, 2019) are illustrative, as are the early injustices of computer matching and profiling reported in Marx and Reichman (1984). Beyond errors, there may be subject displacement. As research on video surveillance and crime suggests, a problem may simply be moved. With respect to displacement a prosecutor notes, "the bad pennies never get lost, they just move from one pocket to another".

Fallacies can be inextricably interlocked and function in tandem to spread obfuscation dust (note how this overlaps with several including that of the fail-safe system below).

[10] In a criminal justice example, a good profile of offenders may increase arrests among the less competent, but make it easier for skilled offenders knowledgeable about the system to avoid detection. The smaller a camera lens the easier it is to hide, but the more limited the range.

1.1.10. The fallacy of a passive, non-reactive environment

The previous fallacy too often assumes that environments, especially those where there are conflicts of interest, are passive rather than reactive. But subjects often find ways of thwarting surveillance and machine predictions via reverse engineering. Innovations in surveillance must be seen as variables in dynamic situations. When combined, humans and machines are co-constitutive in creating new contexts. The failure to note the changes (like generals always fighting the last war) is a factor in technological failures.

There is a Social Heisenberg principle in which the act affects what is acted upon in a changed environment. This may be particularly noticeable over time, as the effectiveness of a solution lessens. New controls create new challenges and opportunities. Every lock has a key. Any solution that one group of smart people creates can usually be circumvented by another group, whether through technical or social means. There are always tacks in the shoe.

1.1.11. The fallacy of the short run

A focus on success in the present may mean a failure to consider longer-range negative consequences, including undesirable precedents and creeping encroachments upon liberty. Consider the story about the person falling from the top of a 200-floor building. As the 150th floor is passed, a friend on that floor asks, "how are you doing?". The reply, "so far, so good".

1.1.12. The fallacy of the free lunch or painless dentistry

There are no free meals, and your teeth may hurt when the Novocaine wears off. Those under the sway of this fallacy may ignore or fail to see collateral costs, especially when they involve powerless groups and future costs. But any format or structure both channels and excludes, generating trade-offs.

In gaining one advantage we may lose another (e.g., breadth vs. depth, validity vs. low cost, short vs. long term gains, solve one problem while creating or worsening another). If nothing else (and in a highly interdependent world with imperfect knowledge, there almost always is something else), a given use of resources involves forgone opportunity costs. In the case of police for example, where might some of the vast expenditures for equipment go instead (training, better working conditions) or to social services involved in order maintenance and community support?

1.1.13. The fallacy of the 100% fail-safe system

In complex environments rich in uncertainty, machines and those who run them can be imprecise and fallible. As the work of Perrow (1984) on Three Mile Island, Vaughan (1996) on the Challenger disaster, and Tenner (1996) on a broad range of technologies suggests, mistakes and unintended consequences adhere and inhere.

Claims such as, "but the computer says" or "it's in the computer" are offered as equivalent to laws of nature. But being "in" the computer guarantees neither accuracy, nor appropriateness. Human agents have set the rules for collecting, entering, and analyzing the data; even machines may do it through processes incomprehensible to humans. Yet given the messiness of the real world the best made plans are too often awrysome. Consider some of the problems initially found with the use of electronic location-monitoring devices for those under house arrest in which mylar in the walls gave false readings or that eating a poppy seed bagel can cause one to fail a drug test. Even where the measure is in principle valid and reliable, it may be incompetently applied or thwarted by subjects.

1.1.14. The fallacy that the means will never come to determine the end

Albert Einstein observed, "perfection of means and confusion over ends seems to characterize our age". To a person with a can opener, the whole world looks like a can. *Where here is a way, there is*

often a will. The means too often impact and can even determine the end; a related form involves the ritualistic danger of the means becoming the end. (Merton, 1956).

It is vital for civilization (if not always for self- or organizational interests) that public policy start with goals – asking what is to be accomplished – instead of starting with a tool and asking how can it be applied. Problems should drive solutions rather than the reverse.

1.1.15. The fallacy that technology will always remain the solution rather than become the problem

All of the above contribute to this capstone fallacy. Today's solutions often become (or contribute to) tomorrow's problems. Contrary to Dr. Frankenstein's experience, this fallacy involves the belief that we can fully control the technology, rather than the reverse. An aspect of this fallacy is failing to ask what the technology might lead to and what precedents it might create. A questionable means applied on behalf of an urgent goal is sometimes justified by the argument that "we can control it and will apply it only in this one narrow area". But given power differentials and temptation, there is a tendency toward surveillance creep, as a once-restricted tactic spreads to new uses, users a and targets and becomes normalized as "just business as usual".

The fallacies considered thus far tie directly to technology. We next turn to those more directly involving values, social consequences and beliefs about persons.

1.2. Fallacies involving values and persons

Here, we find the view that people are objects to be controlled rather than citizens to be treated with dignity. Whatever the varied technologies, with each of the fallacies in this category, the proponent communicates a symbolic message of objectification and manipulation of the human in the service of presumed efficiency and effectiveness.

1.2.1. The fallacy of neutrality

When asked, "isn't the technology neutral?" George Orwell reportedly replied, "yes and so is the jungle". The neutrality argument can conceal the hidden hands and unequal social terrain often lurking in the background. Rob Pallitto (2013) offers a way of unmasking the haze here in suggesting the adoption of a bargaining perspective. In asking a series of questions involving surveillance subjects and the machines and human agents behind them, buried claims may be surfaced, such as how unequal the bargaining setting is. That also applies to the design of a tool, with regard to 10 principles suggested by the Design Justice Network, such as: are the voices of the subjects/communities impacted by the tool considered in its design? and, are traditional ways that may be currently working considered?

The distancing of the technology from its creators and its automatic (rather than direct human) application do not mean that the technology has equal impacts across society or that moral responsibility has been eliminated. The fallacy can mask power relations and draw attention from social and ethical questions involving fairness, reciprocity and accountability and racist and sexist outcomes.[11] Singer Tom Lehrer's parody of Wernher von Braun's rockets applies: "where they go up and what they do when they come down depends on the technology, not me."

The neutrality fallacy denies the political character of much surveillance. If questions are merely technical, and if surveillance is neutral in its impact, then there is no need for discussion or negotiation, and the structural roots of the problem that remain unresolved.

A technology can fail to be neutral in several ways. Inequality in power and resources determines which groups are best positioned to sponsor the *development* of new technologies.

Regardless of who develops the technology, it is rarely *equally available or useful* across society. The rich have little need to shoplift or to sleep behind malls, let alone under bridges and may persons can't

[11] Noble (2018) shows how search engines such as Google's are not neutral with respect to gender and race.

afford fast track access at airports. Nor are the "equal opportunity" monitoring tools such as video-cameras and phone and computer monitoring that are applied to workers as likely to be used for executives.

Regardless of who develops the technology, it is rarely *equally available or useful* across society. In some ways modern means of communication and surveillance, from the printing press through to the Internet, tilt toward greater equality and participation. But the individual who can access the Internet just as a large organization can is not therefore made equal to them. To the extent that access is restricted by proprietary codes or cost, the ease or difficulty of using the tool is irrelevant. Furthermore, while the cost along with the skill required to use much of the technology has steadily decreased, the skill required to understand and fix it has in general steadily increased and is controlled by those owning the software, increasing dependence on, and trust in, distanced, unseen specialists not fully acting in the subject's
interest.[12]

1.2.2. The fallacy that personal information is just another kind of property or material to be bought, sold, altered and manipulated

Personal information has a special quality, something that under some conditions is sacred and inviolate. It is not the same as raw materials or office furniture.

Europe recognizes this to a greater extent than has the United States. The former's concern to protect the dignity of the person (as broadly defined) restricts the sale of personal information, while in the U.S. the focus has been on regulating specific technologies, rather than applying broad principles such as respect for human dignity.

Those in the data warehouse and analysis business often show inconsistency and self-serving attitudes, toward personal information. On the one hand, in the collection phase, personal data is treated as a free public good, like air. It is just there waiting for whoever wants it. Yet once it is harvested, it becomes private property to be used as the possessor wishes, even including selling it back to those it pertains to (e.g., credit scores). This contrasts with other free goods such as radio transmissions or a photo of a person taken in a public place.

Even if viewing personal information as property is appropriate, there is likely a need for a safety net or equity principle guaranteeing a minimum threshold for withholding information. There must be limits on the extent to which data about persons is treated simply as a free good and commodity.

1.2.3. The fallacy of implied consent and free choice

Consent and choice are very difficult concepts to assess. To be meaningful choice should imply genuine alternatives and refusal costs that are not wildly exorbitant, absent that we have trickery, double-talk, and the frequent spoiled fruit of inequitable relationships. Individuals face cognitive limits on what they can know, and factors at many levels limit the amount of freedom in a "free" or willing choice. Certainly, one can protect one's privacy by not using a phone or computer or driving a car. But that is almost like saying if you breathe polluted air or drink contaminated water, you consent to these environmental circumstances. The conditions of modern life are often such that one can hardly avoid choosing actions that are subject to surveillance. While the surveillance may be justified on other grounds, it is disingenuous to call it a free and informed choice. Nor is it necessarily preferable because it seems less directly coercive.

[12] See for example Tusikov (2019) re how in retaining control over software, even after a consumer purchases a product, the company can monitor and control how products are used. You don't have to agree, but then you can't use the product.

1.2.4. The fallacy of the velvet glove

The softer means of implied consent in the above can be beguiling. It is hard to say "no" if you are unaware of what is going on and are not inconvenienced. Just because personal data can be collected relatively silently and non-invasively, does not justify doing it apart from the goals. Judge Brandeis noted that vigilance was most needed when purposes were benign. The same might be said for the softer, non-invasive means. Soft surveillance (Marx, 2017) is still surveillance. The challenges of "mandatory voluntarism" and "voluntary servitude" (Rosen, 1996) are vital topics for a democratic society and the person as a maker of genuine choices.

The seemingly non-problematic nature of choices that are not genuine choices may take attention away from other aspects. Even when there is genuinely free consent for given types of personal data collection and technological operations, that should not be seen as an open invitation to any type of data *analysis, usage and sharing*. Such is often the case with AI, and the merging of big, unrelated data sets gathered under different conditions.

1.2.5. The fallacy of meeting rather than creating consumer needs

This fallacy overlaps the notion of free choice and implies that consumption "needs", including perceptions of an appropriate level of security, rise up spontaneously within the individual rather than being generated by entrepreneurs. Of course, there is always a mixture, but advocates seek to soften the harsher edges of manipulation by claiming that they are simply giving the public what it wants. Here, they deny the role played by propaganda, marketing strategies, unseen manipulation and the creation of desires, rather than the meeting of needs (however hard the latter is to define).

1.2.6. The fallacy that individuals are best controlled through fear

Nineteenth-century positivist theories of law and the presumed link between rationality and conformity gave great force to the belief that the more anxiety people felt over discovery, apprehension and sanctioning for normative violations, the better their behaviour would be.

It is often impractical to watch everyone all the time. The effort to engender fear and apprehension is an important part of some contemporary surveillance rhetoric. Things are usually much more complex than the messengers claim. Democratic principles require respect for the individual and toleration of a degree of disorder as a concomitant of a free society.

Certainly, in many settings accountability increases proportionally with the visibility of compliance. But no such simple statement can be adequate for all complex human situations. Other factors being equal, good behavior is more likely to occur when individuals have participated in setting the standards, understand the reasons for them and feel respected by an organization. Climates of fear and suspicion work against innovation and adoption of new ways.

Even holding apart issues of effectiveness, means have a moral quality as well as ends. Policies to effect behavior out of fear, coercion (whether technical or social), and threat of punishment, while sometimes needed, need not be unleashed or unreflectively favored over other approaches.

1.2.7. The fallacy that because it is possible to skate on thin ice, it is wise to do so

When critics of technology point out possible negative consequences, a standard response is, "that's never happened" or "that couldn't happen". Yet foresight remains better than hindsight. It is unwise to wait until the dam breaks to decide to reinforce or move it. There was a time when the nuclear accident at Three Mile Island and the Alaska Exxon oil spill had not happened as well. It is not enough to show that a tactic has thus far been without disastrous consequences.

1.2.8. The fallacy of re-arranging the deck chairs on the titanic instead of looking for icebergs

A cartoon shows a seated man with a knife stuck in his back. A doctor leaning over him says, "this will have to come out, but of course it doesn't address the deeper problem". And so it is with many

quick-fix technical solutions to organizational or social problems; they are sometimes no more than Band-Aids on a haemorrhaging wound (e.g., removing benches from public areas as a response to homelessness).[13]

The emphasis may be on the wrong problem as a result of bad analysis or political factors. Technical solutions are often sold as cleaner, quicker and less expensive – as something that can be done – relative to the messy business of dealing with people and trying to understand the complex cultural and organizational causes for many problems. As noted, the mindset may in turn lead to the distorted view that "if you can't fix the real problem, fix whatever the technology permits you to fix". In such cases Thoreau's (2015) observation in Walden holds:

> but lo! Men have become the tools of their tools.
> Our inventions are wont to be pretty toys which distract our attention from serious things.

Attention to deeper causes and bigger pictures (with the implication that broad changes in a system may be required) do not play very well in the short run when the focus is on the bottom line or in a moral panic.

While symptoms must often be treated as well as broader causes (if a bathtub is overflowing, the floor needs to be mopped, as well as turning off the faucet. Deeper analysis might even lead to the pessimistic conclusion that there are no realistic solutions, or none that do not bring other problems.

1.2.9. The fallacy of confusing data with knowledge and techniques with wisdom

To varying degrees, all these fallacies reflect a broad, unquestioned faith in the efficacy of science and technology and the denial of trade-offs or the legitimation of specious trade-offs. Technologies for extracting and processing personal information are neither givens nor an automatic reflection of the natural world. The social hands behind the curtains and the levers of the machine need to be scoped out. Above all, technical mastery, or even knowledge, must never be equated with wisdom.

2. One person's fallacies can be another's truths

A necessary condition of wisdom is identifying and evaluating the web of tacit assumptions that are so intertwined with beliefs and action. The techno-fallacies discussed are illustrative and far from exhaustive. They differ in seriousness, and are expressed neither universally, nor with equal intensity and conviction.

This article has focused on views of the technophiles, often nesting in engineering, computer science, business, and government environments, as cheerleaders in a world seen to be on the brink, they too often uncritically, and optimistically, welcome the new surveillance. As noted, when the technophiles are forced to acknowledge problems with a new tool, they call for improved or breakthrough technology to resolve it.

They are techno-fallacies of the technophile. The more extreme advocates favour maximum security and minimum risk. They fail to appreciate the virtues of civil society and traditional borders and the ubiquity of social change, nor to recognize the limits on human rationality and control, let alone on human perfectibility and utopias.

The technophobe discussed above are not offered in a spirit of prohibiting new technology. Rather, they are offered in a spirit of sensitizing conservatism. This asks us to pause in the face of any proposed change and ask critical questions. Consistent with this spirit is the need to examine all claimants, including critics.

---

[13] Byrne and Marx (2011) and Marx and Guzick (2013), Marx (2017) analyze aspects of the engineering of social control.

The world is filled with academic analysts who are often technophobes. They tend to be isolated in social science and humanities environments and too often talk only to each other. Sometimes they raise their concerns about technology explicitly, but more often their concerns appear as underlying themes or subtexts: for example, that we should be skeptical and suspicious about contemporary surveillance, and that the social analyst has a responsibility to sound the alarm. The extensive and intensive recording of "every move you make, every breath you take" is seen as a major element in the destruction of the human in an increasingly engineered, antiseptic, fail-safe, risk-adverse society. In the worldview of many technophobes, technology furthers inequality and domination and eliminates meaningful choices. Critics further argue that publicists for surveillance often deny the real motives and ignore unintended consequences.

Technophobes with extreme libertarianism and/or prejudicial skepticism too often fail to appreciate the advantages of technology, the virtues of community, and the dangers of anarchy, -thus holding their own fallacies, or sharing some with their opponents (for example, too cleanly separating the human and the machine).[14] By adding "never" or otherwise reversing some of the statements listed in this article, we have some mirror-image fallacies of the technophobic (e.g., the fallacy that technical solutions are never to be preferred).[15]

But critics have some distinctive fallacies as well: the fallacy that the sky is falling or the apocalypse is approaching; that if you can imagine bad things happening, they surely will; that the people always know what's best (the populist fallacy); that privacy is an unlimited good (or if some is good, more must be better); that privacy is primal (i.e., that it ought to take precedence over other values); that privacy is only an individual value rather than a social value; that privacy can only be taken from someone, rather than imposed upon them; that because something worked (or failed) in the past, it will in the future; that technology is always the problem and never the solution (the Luddite fallacy); and related to this, that technology can only be used to cross informational borders rather than to protect them.

Of course, Karl Mannheim notwithstanding, the academic analyst who tries to stand above the fray and between the technophilic and the technophobic may show fallacies as well. The analyst sees and speaks from a particular social location with values and interests. Those on the front lines – whether those who want to unleash or stop a technology – don't share the analyst's effort to be neutral, or at least independent.

A fallacy list surfacing the tacit and debatable assumptions of the academic is also in order. Such a list might start with these: the risk-free Monday-Morning Quarterbacking; the overly broad academic generalization; the dressing of common sense (or non-sense) in multi-syllabic jargon replete with esoteric references; the use of Ockham's razor to nit-pickingly slice the world into too many categories; the timid waffling in the face of complexity and always imperfect data; the failure to clearly enough differentiate value statements from scientific statements; and the reverse of failing to specify how the empirical within the value might be assessed.

Besides understanding the claimant's assumptions and possible fallacies, and to further dialogue, we also need to know what rules the claimant plays by. The worldview of those who start with advocacy rather than analysis is by definition more narrowly self-serving. The rhetorical devices expected there differ from those of the academic analyst, who must start with questions not answers and question all claimants. The scholar of course serves his or her interests in the pursuit of truth. But especially because

[14] That distinction worked for much of human history. But with the increasing inter-dependence seen with cyborgs, advanced robots, implants and people hooked up to machines, the lines are less clear now.

[15] Of course, many critics are not technology-phobic, rather they question the design, uses and control of the technology and wish to see it disproportionately pointed upward, rather than downward, as it currently is, with a more explicit focus on inequity and social injustice and leveller playing fields.

they are making truth claims, they must also strive for consistency and a strong tilt toward logic and evidence because that is right and can add legitimacy.

An academic analyst should offer data, methods, concepts and theories in an open, civil, selfinterrogating, and critical environment. This should be accompanied by healthy doses of qualification, caution and humility (given dynamic situations, measurement challenges, and the paradoxes of the sociology of knowledge) in the face of complex, interdependent problems.

Undue confidence can be a danger for science and technology advocates. Undue timidity can be a danger for academic analysts as well. For complex issues of social policy, limits must be acknowledged, but they must not immobilize. One can rarely wait until all the data are in and there is scientific consensus. Even then, the non- scientific aspects of values and goals remain.

With the above cautions, analysts are often called upon for advice. In offering advice they must try to keep statements of fact distinct from statements of value, while acknowledging the tensions and interconnections between them. The key is awareness and tentativeness (or at least continual openness to examining assumptions and alternatives). The presence of values is nothing to run from. Indeed, the failure to acknowledge values and to coat them in the camouflage of pseudo-scientific neutrality and precision is at the heart of many problems. The quest for absolute objectivity and nonjudgmental fiddling can make one a moral eunuch in the face of a deaf world on the brink.

Acknowledgments

The Open Access publication of this paper was supported by the Panelfit project. This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039. This document reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

References

Bell, W. (1997). *Foundations of futures studies: History, purposes, and knowledge*. New Brunswick, NJ: Transaction Publishers.

Byrne, J., & Marx, G. (2011). Technological innovations in crime prevention and policing. A review of the research on implementation and impact. *Journal of Police Studies*, *20*(3), 17-40. Cohen, S. (2011). *Folk devils and moral panics*: Routledge.

Coser, L. A. (1964). The Social Functions of Conflict. Glencoe, Ill. Free Press.

Design Justice Network at https://designjustice.org/. 2022.

Fleury-Steiner, B. (2019). Deportation Platforms: The AWS-ICE Alliance and the Fallacy of Explicit Agendas. *Surveillance & Society*, *17*(1/2), 105-110.

Goode, E., & Ben-Yehuda, N. (1994). Moral panics: Culture, politics, and social construction. *Annual Review of Sociology*, *20*(1), 149-171.

Gramsci, A. (2000). *The Gramsci reader: selected writings*, 1916–1935 (Forgacs Ed.). New York: NYU Press.

Hofstadter, R. (1965). *The paranoid style in American politics and Other Essays*. New York: Knopf Publishers.

James, W. (1950). The Principles of Psychology. In. New York: Dover Books.

Lee, A., & Lee, E. B. (1939). *The fine art of propaganda*. New York: Harcourt Brace.

Lowenthal, L., & Guterman, N. (1949). *Prophets of deceit*. New York: Harper & Brothers.

Mannheim, K. (2015). *Ideology and utopia: An Introduction to the Sociology of Knowledge*. Eastford, Conn: Martino Books.

Marx, G. T. (2006). Soft surveillence: a growth of mandatory volunteerism in collecting personal information – "Hey Buddy Can You Spare a DNA? In T. Monahan (Ed.), *Surveillance and security: Technological politics and power in everyday life*: Taylor & Francis.

Marx, G. T. (2015). Technology and social control: : The Search for the Illusive Silver Bullet Continues. In *Encyclopedia of the Social & Behavioral Sciences, 2nd edition*.

Marx, G. T. (2017). *Windows into the soul. Surveillance and society in an age of high technology*. Chicago: Univ. of Chicago Press.

Marx, G. T., & Guzik, K. (2017). The uncertainty principle: Qualification, contingency and fluidity in technology and social control. In *The Routledge handbook of technology, crime and justice* (pp. 481-502): Routledge.

Marx, G. T., & Reichman, N. (1984). Routinizing the discovery of secrets: Computers as informants. *American Behavioral Scientist*, *27*(4), 423-452. Retrieved from https://web.mit.edu/gtmarx/www/secrets.html.

Merton, R. K. (1956). *Social Theory and Social Structure*. Glencoe, IL: Free Press.

Nisbet, R. (1994). *History of the Idea of Progress*. New York: Routledge.

NIST. National Institute of Standards and Technology. (2019). Facial Recognition Vender Test. In. Gaithersburg, MD: NIST.

Noble, S. U. (2018). *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: NYU Press.

Pallitto, R. M. (2013). Bargaining with the machine: A framework for describing encounters with surveillance technologies. *Surveillance & Society*, *11*(1/2), 4-17.

Perrow, C. (1984). *Normal accidents: living with high-risk technologies*. New York: Basic Books.

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: Or how the sociology of science and the sociology of technology might benefit each other. In W. E. Bijker, T. P. Hughes & T. J. Pinch (Eds.), *The Social Construction of Technology Systems: New Directions in the Sociology and History of Technology* (Vol. 14, pp. 17-51). London: M.I.T. Press.

Rosen, M. (1996). *On Voluntary Servitude*. Cambridge MA.: Harvard University Press.

Rule, J. B. (1978). *Insight and social betterment: A preface to applied social science*. Oxford: Oxford University Press.

Shelby, R. (2020). Value-Responsible Design and Sexual Violence Interventions: Engaging Value-Hypotheses in Making the Criminological Imagination. In *Routledge Handbook of Public Criminologies* (pp. 286-298): Routledge.

Shils, E. (1956). *The Torment of Secrecy*. New York: Free Press.

Shore, K. (2021). Targeting vulnerability with electronic location monitoring: paternalistic surveillance and the distortion of risk as a mode of carceral expansion. *Critical Criminology*, *29*(1), 75-92. Retrieved from https://link.springer.com/content/pdf/10.1007/s10612-021-09558-0.pdf.

Tenner, E. (1997). *Why things bite back: Technology and the revenge of unintended consequences*: Vintage.

Thoreau, H. D. (2017). *Walden*. Layton, Utah: Gibbs Smith.

Tusikov, N. (2019). Precarious Ownership of the Internet of Things in the Age of Data. In *Information, Technology and Control in a Changing World* (pp. 121-148): Springer.

Vaughan, D. (1996). *The Challenger launch decision: Risky technology, culture, and deviance at NASA*. Chicago: University of Chicago press.

Welch, M. (2003). Ironies of social control and the criminalization of immigrants. *Crime, Law and Social Change*, *39*(4), 319-337.