Radical CS*

Phillip Rogaway
Department of Computer Science
University of California, Davis, USA

June 2024

Abstract

For years I have anguished over the direction and character of my research area, cryptography, and my field, computer science (CS). Here I own up to my grumpy discontent and identify what I take to be its primary cause: a rejection of the standard technological narrative (STN), by which I mean techno-optimism, embedded in an enticing story of technology’s central role in man’s glorious ascent. By radical CS I mean CS that rejects the STN. I try to imagine what a program of radical CS might look like. Then I provide a postmortem on three pieces of my prior work that were, in retrospect, attempts at radical CS: writing about technopolitics in The Moral Character of Cryptographic Work (2015); defining a strong secret-sharing notion in Reimagining Secret Sharing (2020); and replacing much of my technical teaching with a distressing course on ethics-and-technology (2004–2023). While none of these efforts were entirely successful, it’s better to have tried.

*This essay was written to accompany a talk given at [The Third NIST Workshop on Block Cipher Modes of Operation 2023](https://www3.nist.gov/cyber/net/Workshops/BlockCipherModes/index.html) National Cybersecurity Center of Excellence, Rockville, Maryland, 3 Oct 2023. Opinions expressed here are entirely my own.
Good morning. It’s wonderful to be here today, especially considering how close we came to this workshop not happening. \(^1\) I’d like to thank Morris Dworkin, and the entire program committee, for inviting me to speak. These days there’s no knowing what I might talk about when I get invited somewhere, so I appreciate your courage to invite me just the same.

\(^1\) A U.S. government shutdown was narrowly averted on 30 Sep, with the workshop beginning 2 Oct. In the aftermath, Speaker of the House Keven McCarthy lost his leadership position for the crime, most proximally, of cooperating with Democrats to avoid the shutdown. The incident seemed to punctuate our present predicament: the world’s current problems require extraordinary cooperation to solve, if they can be solved at all, yet come at a time when even ordinary cooperation seems all but impossible.
I have special fondness for blockcipher modes

I'm especially happy to join this workshop on blockcipher modes because I have a great fondness of them. They are like old friends. I like to figure out what cryptographic problem some existing mode aims solve—and to figure out if it actually solves it. I like to explore definitions for goals solvable by modes, and to invent new constructions to meet them. I like to draw pretty pictures of modes. I'd be embarrassed if people knew just how many hours, over the years, I've spent drawing such pictures, so I better keep that under wraps.

\footnote{I spell blockcipher solid because it is one conceptual thing, the word block no longer heard as modifying cipher. If you will not join me in radical CS, perhaps you will at least join in radical spelling. A blockcipher mode, or mode of operation, is a cryptographic scheme \( \Pi \) that depends on, at least, a blockcipher \( E \). For a classical blockcipher mode, the blockcipher is the sole source of computational hardness for \( \Pi \).}
Slide 3  There’s another reason that I like blockcipher modes: it was one of the first pieces of genuinely independent work that I did. It was the early-1990s when Mihir Bellare and I finished up at MIT and went to IBM. As grad students we had been trained to craft definitions and proofs; we learned how to do cool things from weak assumptions; we learned about interactive proofs, zero-knowledge, and multiparty computation. But I don’t think that blockciphers or their modes were ever mentioned. It just wasn’t a thing.

I think there was a reason for that: these things were viewed as outside the realm of any proof-centered discourse. Finitary objects, blockciphers weren’t amenable to the usual complexity-theoretic treatment. Without that, hope for provable-security was forfeit. On top of that, modes were simple, originated outside of academia, and rested atop complex, ad hoc primitives. Taken together, this meant that modes were something a thoughtful cryptographer should ignore. Something that modern cryptography had outgrown.

But had it? When Mihir and I got to IBM, we found out that blockciphers and their modes were ubiquitous—and this wasn’t about to change. They were the preferred tool to solve a variety of problems. Why couldn’t one demand provable security here, too? That one would reduce a problem to a complex or finitary primitive seemed irrelevant; one could still establish that if the blockcipher did well at accomplishing its (well-defined) goal, then the mode of operation based on it would do well at accomplishing its (equally well-defined) goal. To begin, we wanted to prove security for the CBC MAC, a classical message authentication code (MAC), and we wanted to develop an alternative but parallelizable technique that would be provably secure, too. If this sort of work was going to be seen as banal or in poor taste, well, that wasn’t really on us.

Some of course this was just a misunderstanding; provable-security is not forfeit for finitary objects. Indeed dealing with a finitary object motivated greater attention to tight reductions and precise analyses.

It’s not clear if this statement is still true, as wide-block permutations have emerged as an attractive alternative. This is largely due to the work of Joan Daemen.
Curiously, it wasn’t just modes that were being ignored by academic cryptographers; we soon learned about problems in entity-authentication and key-distribution (EA/KD), which lived even further afield from the body of discourse in which we had been immersed. So Mihir and I decided to work on definitions for this domain, and to develop EA/KD protocols based not on encryption, as was standard, but on a MAC or PRF (pseudorandom function), which seemed preferable. We thus needed provably secure modes not only for symmetric encryption and MACs but, also, to have provably sound solutions for EA/KD.

All of this seemed strangely basic. I would often wonder: why hadn’t all this stuff been done before? I mean, both EA/KD and modes of operation were, at the time, more than 15 years old. They were extensively used, discussed in books, and the subject of both U.S. and international standards. And the idea of provable security was, at the time, more than a decade old, and had already been applied to a wide array of cryptographic problems. Something odd was apparently true: that a problem could be conspicuous outside the disciplinary community to which it ostensibly belonged, yet invisible, or ignored within that disciplinary community. Let me call this observation the invisibility phenomenon. Without even trying, Mihir and I had found two examples of it. Likely there were more.

While we didn’t at the time use the term, Mihir and I often discussed the invisibility phenomenon. It seemed paradoxical. But paradoxes are only paradoxical so long as you don’t understand what’s going on. If you could figure out why elephant-in-the-room problems weren’t being seen, maybe you could learn to see them.

Exploiting the invisibility phenomenon became my favorite strategy for writing papers. Mihir and I would try to find obvious questions that our peers had ignored. Could it really be the case that nobody had worked out the provable-security basics for symmetric encryption? Were there really no definitions capturing the various properties that real-world cryptographic hash functions supposedly enjoyed? Had nobody specified what problem that a garbled circuit aims to solve? And so on. There was actually much “dark matter” to be found.

Work in this vein soon led me to realize something: that sometimes the most radical thing you can do in life, and sometimes the most fulfilling, is simply to pay attention to something that those around you aren’t paying attention to. The key move is to take seriously the problem that’s smack in front of you—the problem that others don’t seem to see. Or they may see it just fine, but for reasons cultural, personal, or philosophical, they don’t care to go there.

Today’s talk is a continuation of this mindset. It is invisibility phenomenon writ large.

---

5 I don’t make much of a distinction between seeing something and ignoring it, versus not seeing it at all. The impact on one’s field is identical. These things might be different philosophically, but that’s not really relevant.

6 Sentiment and phrasing similar to Brandon Ogbunu, The Liberation of RNA, Radiolab interview, 13 June 2020. “Sometimes the most revolutionary thing, or the most subversive thing you can do, is just focus on the right things in life.”
A growing ennui

I spent most my career
- Writing technical papers,
- giving technical talks,
- teaching technical subjects.
It was fun, and I am grateful.

But doing these things these
days has came to feel
increasingly misguided.
Even self-indulgent.

The climate crisis is here. The biodiversity crises. 6th
Tipping points. And with these things: social, political,
and economic turmoil; civilizational collapse. For young
people: the future is bleak.

Slide 4 For a long time I was satisfied with the kind of research questions I’ve described. And
I liked the life of a professor. I’d write papers, rather slowly, obsessing over each word. I’d give
talks on the papers. I’d travel to give those talks—or just to travel. I was attracted to the figure of
the itinerant scientist. I also loved to teach. While everyone around me thought that teaching was
a burden, I thought it was great. I am grateful for the life that being an academic cryptographer
afforded me.

But sometime around the mid-2000s I started to feel that my way of living was somehow off.
The work was fun, and maybe it worked to benefit people’s privacy or security. But it felt as though
my colleagues and I were ignoring something huge. Another elephant-in-the-room, still bigger than
before.

I am speaking, of course, of the climate crisis, and the broader environmental crises of which
it is a part. And I am speaking of all that will accompany this crisis. Pandemics. Extreme wild-

It should go without saying, yet seems necessary to say, that all of our cryptographic cleverness
will not matter one bit if the world blows up in a nuclear holocaust, burns down over a few hot
summers, or slowly contracts, ending not with a bang but a whimper[1]

Are my colleagues working on these things? Am I? Buried in this narrow problem or that, it
seems as though, operationally, we ignore the overarching trajectory of CS … of technology …
and of the whole damn world.

that the world must end with a bang or a whimper, commenting that people whose houses were bombed have
told him that they don’t remember hearing anything. Henry Hewes, Saturday Review, September 13, 1958, p. 32.
https://tinyurl.com/tse001
Slide 5  For decades most of us have dismissed the climate crisis. Dismissed it, I mean, in the operational sense, that it has played no real role in shaping our life’s work. This probably wasn’t sensible in the 1970s or 1980s, but it’s even less sensible today.

For me, the world already feels radically diminished. The sense of that became more profound when COVID arrived. Here (slide #5) are a couple of views of my own university, UC Davis, in 2020. I remember walking through campus one clear and peopleless day. We had reached the final chapters of a book. The book was the story of this civilization. While it wasn’t yet clear just how our decline would play out, it actually was rather clear that this civilization is finished.\footnote{The phrase, and the emphasis on this, is taken from Rupert Read and Samuel Alexander: This Civilisation is Finished: Conversations on the end of Empire—and what lies beyond. Simplicity Institute, 2019. The book is short enough to have students read, in full, in my ethics class (slides #35–#39). One key point of the book is that this civilization ending does not preclude the possibility of a different and better civilization arising in it’s place.}

Now, a few years after COVID, many imagine that campus life has returned to its prior state. It has not. For one thing, students did not return to the classrooms. One colleagues told me that he sees about 30% attendance in his classes. Another admitted that, for him, it was more like 15%. Then again, faculty did not return to their offices, either. Walking about the floor of my building might yield two or three open doors (out of ∼50). Are the students and faculty now working from home? Or, what I suspect as the bigger factor, are faculty just way less willing to work, and working way less?

One missed-opportunity about COVID-19 was that people never connected its emergence with our own bad behavior; it was just this thing that happened to us. Which is probably wrong, since most COVID-origin theories, from direct zoonotic transmission to laboratory accident, have man’s incursions into nature playing a pivotal causal role.\footnote{Of course new diseases can emerge in any population of animals; all that can be said at present is that climate change, overpopulation, habitat destruction, our frivolous food choices, and poor laboratory safety all increase the}
Slide 6  It wasn’t just the pandemic that decimated the character of life in my little town a few months after the virus shut things down the 2020 fire season ravished California like never before.

Wildfire smoke first forced me to flee Davis in 2018. I have a little asthma, you see, usually it’s nothing, but smoke can shut me down. That November smoke from the Camp Fire descended like a black specter. So by the time the 2020 wildfires arrived, with the campus indefinitely closed down due to COVID, I knew what to do: we left Davis and rented an apartment 600 miles to our north, in Portland, Oregon.

It didn’t work; the fires and smoke pursued. This (slide #6, top) is a picture from outside my window in September from 2020.

When the smoke finally clears it doesn’t mean that all will return as it was before.

For years I used to hike and backpack in the Sierra Nevadas. A day hike I often did was a jaunt up Ralston Peak. Here’s a picture (slide #6, left) doing that last July. Now it’s tracts of blackened tree trunks. The sky too bright, the air too hot, and everything smells of soot.

“Won’t that trees return?” asked my friend. “Forests do burn down.” They may, I explained, but it will not be beautiful again during my lifetime. Not even my son’s. And, in fact, the trees might not return. Why would one assume that the same sort of coniferous forest will return when the environmental conditions that gave rise to it are no more?

The California megafires have become a regular event. This isn’t just my anecdotal sense of things; it’s what the data shows (slide #6, right). The largest fire since records began in California had been the Matilija Fire, in 1932, which burned 220,000 acres. This was first eclipsed in 2007. Since then we’ve had fifteen fires larger than the 1932 blaze. Some have been four or five times as large. Wildfires are not the same kind of thing they were before.

likelihood that nasty zoonotic transitions will arise.

Our forests are largely ruined. California’s forests are so degraded that they release more carbon than they fix\textsuperscript{11} Even Canada’s forests, massive as they are, became net carbon-sources in 2023. Canada’s managed forests passed that threshold around 2002\textsuperscript{12}

If the forests are our planet’s lungs, the patient is dying from emphysema.


\textsuperscript{12}Robson Fletcher, CBC News, Feb 12, 2019: Canada’s forests actually emit more carbon than they absorb—despite what you’ve heard on Facebook. Leyland Cecco, Wildfires turn Canada’s vast forests from carbon sink into super-emitter. The Guardian, Sep 22, 2023.
Our assault on animal life
Biomass of land chordates

Wild mammals & birds $\gg 99\%$
Humans & our domesticated animals $\ll 1\%$

10,000 BP

Wild mammals & birds

Humans $35\%$
Livestock $60\%$

Present

Slide 7  I’ve spoken of COVID and fires, but in almost every direction one looks one see signs of collapse. Here (slide #7) is a visualization based on data from a well-known PNAS 2018 paper. It shows the fraction of bird and mammalian life that is us—humans and the livestock we like to eat. We now comprise 95% of the bird and mammalian biomass on this planet. Apparently, we allow birds and mammals to live only if they are us or we like to eat their flesh.

Our eradication of vertebrate life is a stunning expansion of Adam Smith’s vile maxim. Speaking of man’s rapaciousness against his fellow man, Smith warned that “All for ourselves, and nothing for other people, seems, in every age of the world, to have been the vile maxim of the masters of mankind.”\textsuperscript{13} Now the target of our acquisitiveness is nothing short of the biosphere itself. Adam Smith’s admonition would have to be enlarged: “All for ourselves, and nothing for other species, has become the vile maxim of mankind.”

Are we worth saving?

At this point it would seem that much non-human life on Earth needs to be saved from us. But are we worth saving? The question comes to mind most every day as I wander around campus and watch people. The students have been transformed into a new kind of being. They are cyborgs—a biological portion merged with a smartphone. It is not an addiction, as it is so often misdescribed; it is the emergence of a new kind of being. Less individuated, autonomous, and biological; more networked, engineered, and electronic. In the end, Apple’s creation was not some gizmo they coaxed us to buy: it was nothing short of us, a new kind of being.

When I see a scene like the one shown above (slide #8), or when I see the students lined up along a hallway, suckling their electronic parts, I don’t just feel sad for what we became: I feel guilty. For who has built this new kind of being, these cyborgs that I don’t much like? While blame doesn’t fall on any one discipline, my own—computer science—is clearly at the center.
And the role of CS?
Bringing enormous harms and risks — that mostly get ignored from within

The distraction economy
Killer robots
Imperiling democracy
Face recognition
Governmental mass-surveillance
Unaccountable AI

Slide 9 You scoff. You don’t see yourself as a cyborg; you are the master of your electronic kitsch. The conventional narrative frames the problem differently, as the emergence of a distraction economy. Which is bad, but not so big a deal. There are benefits as well as costs, and ways for you to take back control.

Even if you buy such a framing, what, really, is the point? Of you. You have been reduced to a data source for surveillance capitalism, a target for behavior interventions. A body to be tracked and redirected. Nudged by corporations that want to separate you from our money, or create brand associations within your brain. Tracked by governments working hand-in-hand with the same corporations, eager to detect dissent and head off social-change movements before they get off the ground. A landscape of subtle, high-tech control.

Or we can look in a different direction and witness the technology-fueled rise of authoritarianism. The increasingly effective means for shaping or subverting elections. In the U.S., where representative democracy was always kept closely in check, we must add to innovations like the electoral college, gerrymandering, the three-fifths person, and Super PACs the use of complex and secret algorithms to tune and individualize propaganda.

From where does all this masterful technology come? Surveillance and behavioral intervention is the primary purpose to which AI/ML is put. It is the primary reason that the area is regarded as booming. Why is this so rarely acknowledged? Even in computer vision, which is so obviously about human surveillance that you might imagine it impossible to position otherwise, even there, research papers almost never even use the word surveillance, and often obscure that it is people that are the usual target of the machine’s gaze.¹⁴

¹⁴For a recent effort to extract values implicit in vision research despite academic and obfuscatory language, see Pratyusha Ria Kalluri, William Agnew, Myra Cheng, Kentrell Owens, Luca Soldaini, and Abeba Birhane: The Surveillance AI Pipeline. arXiv:2309.15084v2, 2023.09.26 (revised 2023.10.17).
Finally, let's not forget the increasingly effective ways to kill people from a distance, which again depends on CS. The business-end of the weapon system might be a bullet or bomb, but the communications, targeting, and control is mostly on us computer scientists.

Because we are so much in the thick of these things, you might expect that computer scientists would be worried, if not panicked, about how we are changing the world. We’d be issuing strident warnings, desperately working to maximize benefits or minimize risks. Nothing could be further from the truth. Rather, the technical folks are among the biggest cheerleaders for change. Usually rapid, reflexive, power-centralizing change. And that is, perhaps, what I find most disagreeable about the character of modern CS: that we don’t just enable our collective stumbling into whatever, but that we do so without compunction, driven, almost exclusively, by a personal desire for money, challenge, or prestige.
Wait! How about some optimism, instead?

The dominant narrative — techno-optimism — says that modern technology is not the problem — it's the solution

“I really do believe when ingenuity gets involved, when invention gets involved, when people get determined and when passion comes out, when they make strong goals — you can invent your way out of any box. That's what we humans need to do right now. I believe we're going to do it. I'm sure we're going to do it.” J. Bezos, 2019

“Computer science is marking an epical change in human history. We are conquering a new and vast scientific continent. ... Virtually all areas of human activity ... [and] virtually all areas all areas of human knowledge ... are benefitting from our conceptual and technical contributions. ... Long live computer science!” S. Micali, 2013

Slide 10 I should emphasize at this point how different my framing of where we are at is from the conventional framing. The conventional framing is one of extreme technological optimism. Thanks to technology, things are great and getting greater. Problems arise with tech, sure, but they can be fixed with better tech. What we need, principally, is cleverness, economic freedom, and the will to stay the course.

I encounter techno-optimism, often quite extreme, in most every grant proposal or CS research paper I read, and in most every tech-centered interview or faculty-hiring discussion I ever hear. Techno-optimism is the dominant religion of our time, expressed by everyone from preschool children to Turing-award winners.

As a random example, here is Jeff Bezos, from a 2019 interview with Brad Stone:

I really do believe when ingenuity gets involved, when invention gets involved, when people get determined and when passion comes out, when they make strong goals—you can invent your way out of any box. That’s what we humans need to do right now. I believe we’re going to do it. I’m sure we’re going to do it. 15

Or here is my own advisor, Silvio Micali, accepting the Turing award for his fundamental contributions to cryptography:

Computer science is marking an epical change in human history. We are conquering a new and vast scientific continent. ... Virtually all areas of human activity ... [and] virtually all areas all areas of human knowledge ... are benefitting from our conceptual and technical contributions. ... Long live computer science!

What exactly is the goal to which we are heading? Some would say that there is none—that no particular utopian vision animates our forward drive. But in one recent telling, related by another white billionaire, we are striving for a world of perpetual material creation, growth, and abundance. We need to claim our birthright, which is the control of nature. The world shall be shared by an earthly population of some 50-billion people. While these people have essentially infinite wants and needs, we can continuously grow everything necessary so as satisfy those needs. To get there we need a massive build-out of atomic energy (just until fusion-energy becomes practical), laissez-faire economic policies, and the defeat of bad ideas (like my own). The lies of the techno-pessimists have been dragging us down; we need confidence and optimism. Join us optimists; the water is warm!

Dystopian films and TV series like The Matrix (1999) or Black Mirror (2011–23) are widely popular and culturally significant. Are they the seeds of a nascent opposition to our technological race-to-whatever? I wish it were so. But I think they are mostly a form of play. We all know that tech could go terribly wrong, which is a hard reality to stomach, especially if you’re a nerd helping to make weird stuff happen. So we make it Hollywood-creepy. We make it slick and fun. This redirects anxiety in a harmless direction, away from politics, policy, or planning. We don’t need to stop creating a Black-Mirror universe, we only need to get used to the ideas, to play with them, because, after all, there’s not a whole lot you can do about it.

---

16I.e., not Jeff Bezos. The remainder of the paragraph is paraphrased from Marc Andreessen: The Techno-Optimist Manifesto, 16 October 2023, [https://tinyurl.com/techno-opt](https://tinyurl.com/techno-opt). Not all accounts of techno-optimism are as extreme or creepy as Mr. Andreessen’s; for more cautious arguments for tech-optimism, see, for example, John Danaher, Techno-optimism: an Analysis, an Evaluation and a Modest Defence, Philosophy & Technology, 35(2), pp. 1–29, 2022. For a book-length argument for techno-optimism, complete with graphs that aim to prove what a wonderfully improving world we now live in, see Steven Pinker, Enlightenment Now: The Case for Reason, Science, Humanism and Progress, Viking Press, 2018.
Why does techno-optimism dominate?

It’s the culture, stupid.

Cognitive biases: optimism bias, the bandwagon-effect
Quick rewards; slow, nearly invisible harms, especially to the environment

Cool gadgets: Washing machines, cars, smartphones, washing machines, ...

Still here almost 80 years after nuclear weapons – way to go!

Benefits are concrete and immediate; risks are abstract and long-term

Moore’s law (see, it’s even be legislated)

Plastics

Make stuff, make money

The economy

Vaccines

Antibiotics

Anesthesia

Bezos, Gates, Jobs, Musk

Did you ever try to read Jacques Ellul of Lewis Mumford?

Just read Steven Pinker, man

Green Revolution

I want to say one word to you. Just one word. ... Are you listening? ... Bitcoin. ... There’s a great future in Bitcoin. Think about it.

Don’t worry, be happy

11.8 billion people

Slide 11 But why has the the promise of techno-bliss so vastly out-competed calls for caution?

Techno-optimists like Steven Pinker would have you believe that they are just following the evidence: techno-optimism is correct perspective because technology has made everything objectively better. Lifespan, health, leisure time, violent deaths, agricultural yields, ... anything and everything. Yet the evidence is cherry-picked and decontextualized. The most important metrics—those that would assess the health of the entire biome—are in radical decline. Regardless, not many of the world’s techno-optimists—meaning most on the world’s people—could articulate the competing claims. In the end, they believe in technology simply because that belief is embedded in the prevailing culture. Our basic beliefs about technology are not the product of a self-directed and rational evaluation of facts; the beliefs reflect, almost reflexively, our cultural milieu.
In Quinn’s telling, “mother culture” envelops us in a suspect story

“Once when I was in college,” the nameless protagonist explains to his gorilla teacher in *Ishmael*, “I wrote a paper for a philosophy class. . . . Here’s what I said . . . . Guess what? The Nazis didn’t lose the war after all. They won it and flourished. They took over the world and wiped out every last Jew, every last Gypsy, black, East Indian, and American Indian. Then . . . they out the Russians and the Poles and the Bohemians [and so on]. . . . When it was all over, everyone in the world was one hundred percent Aryan, and they were all very, very happy.

“Naturally the textbooks used in the schools no longer mentioned any race but the Aryan or any language but German or any religion but Hitlerism or any political system but National Socialism. . . . After a few generations of that, no one could have put anything different into the textbooks even if they’d wanted to, because they didn’t know anything different.

“But one day two young students were conversing at the University of New Heidelberg in Tokyo. Both were handsome in the usual Aryan way, but one of them looked vaguely worried and unhappy. . . . His friend said, ‘What’s wrong, Kurt? Why are you always moping around like this?’ Kurt said ‘I’ll tell you, Hans. There is something that’s troubling me—and troubling me deeply. . . . It’s this,’ Kurt said. ‘I can’t shake this crazy feeling that there is some small thing that we’re being lied to about.’ . . .”

Daniel Quinn, *Ishmael*, 1992

---

18 Framing the STN as a myth that we’ve been indoctrinated into, yet can see our way out of, feels ironic, or suspect, because those who feel themselves enmeshed in a matrix of lies seem far more likely to turn towards conspiracy theories, like QAnon, and right-wing authoritarianism (RWA).
What is the small thing we’ve been lied to about?

The “Standard Technological Narrative” (STN)

1. Technology is a tool. It is apolitical and ethically neutral.
2. Due to technology, things are great and getting better.
3. Better technology will fix what inferior technology broke.
4. We will overcome the climate/environmental challenges.
5. Tech is driven by brilliant individuals, advanced by the marketplace.
6. We have risen far above animals, are creating a technological utopia.

My problem with the STN:

It’s bullshit

Slide 13  Let me enumerate some six intertwined beliefs of the STN.

13.1 The first is that technology is just a tool. Tools are neither good nor bad; what matters is how they’re used. A knife can be used by a surgeon to cure or by a madman to maim; the knife doesn’t know the difference. Endowing technologies with socio-political properties is fundamentally stupid.

13.2 The next tenet of the STN is that modern technology has vastly improved human lives. We live longer, have greater opportunities, and so on. Overall, technology has been a huge, huge win.

13.3 Now even the most diehard technological optimist will admit that some technologies have brought problems. A third tenet of the STN is that better technology will fix these problems. Driven by need, ingenuity, and economic incentives, technological fixes can be found. When the problem with CFCs was recognized, for example, they were phased out, and the hole in the ozone layer was able to mend. Unwanted impacts bring improved designs.

Technology can even fix problems that aren’t technological in origin. Street cameras won’t fix the causes of crime, but they can reduce criminality where they’re deployed. Leaving the elderly alone isn’t ideal, but electronic monitoring and chatbots can make them more safe and less lonely.

13.4 While our environmental problems may be serious, these are among the problems that improved technologies will fix. Wind, solar, and other renewables are rapidly growing. EV sales have skyrocketed, while the price of batteries for them has plummeted. Nuclear fusion will soon

---

19 Chlorofluorocarbons, phased out under the Montreal Protocol (1989), for damaging the ozone layer in the upper atmosphere.
provide an endless supply of safe and clean energy. Not only will we stop producing greenhouse gases, but carbon sequestration will reverse damage that’s already been done. Climate change is real, but we’re already on the mend.

13.5 From where do our technologies come? From the wellspring of empowered individuals and innovative companies. Our world is being remade by the the likes of Apple, Facebook, Google, and OpenAI. Entrepreneurship, under an economic system that provides big rewards for innovation, has advanced mankind. While wealth inequality has increased, it’s not a zero-sum game: in the end, everyone benefits.

13.6 Man’s technology has taken him far beyond Earth’s animals. Now we no longer strive for mere survival; we are on a journey to a utopia of our own design. It may entail colonizing countless planets, near immortality, and human lives, perhaps trillions of them, of unimaginable richness.

My problem with the STN is that, fundamentally, I think it’s bullshit. More charitably: it’s a story. A story that takes in some facts, weaves in falsehoods, and smothers it all in wishful thinking. And it’s a story that, conveniently, benefits those with money and power. I won’t counter each and every claim I just listed as part of the STN, but let me address some of it.

To begin, the technology-is-just-a-tool claim is extremely ill-informed. If there’s one thing about which every STS scholar agrees, it’s that technologies are not value-neutral tools. Each is produced by a specific group of people for specific purposes. The technology will embed its creators’ values and purposes. And it’s not just the low-level design choices: there’s a near-infinite array of potential technologies that are not pursued due to social, political, or economic reasons. Science sets boundaries for what is possible, but politics, economics, and culture shapes all the things that come to exist, and all the things that never come to be, and that we fail to even imagine.

Of course modern technologies have made some things better. They have made other things worse. Whether it’s a net-win or a net-loss will depend on where you sit. All technologies have costs as well as benefits, and the costs and benefits are never distributed evenly. The winners are most often affluent, white, and male; marginalized people, animals, and the planet usually come up short. Technologies are tools for redistributing who has what power.

I think it is foolishly optimistic to assume that technological solutions will arise, and in time, to fix the climate crisis or the biodiversity crisis. The evidence points in the opposite direction: that we are heading for environmental collapse and mass extinctions. Our environmental problems are an existential threat. Not just for H. sapiens, but for millions of other species with which we share this planet.

Technological advance really is not driven by smart people, a story to stoke up an inflated sense of self-importance. It is primarily driven by companies that are driven to make money. The general

---

20 For the talk at NIST I adjusted the language in of slide #13 from “It’s bullshit” to “It’s a fantasy.” See footnote 26.

21 The acronym stands for either Science and Technology Studies (mostly in the U.S.) or Science, Technology, and Society (mostly in Europe). It seems less than accidental that the word society vanishes in the country whose technologists go so far as to doubt existence of society as a meaningful construct. In teaching ethics to CS students I found that, at the beginning of each term, many students believed that they had formed all important beliefs on their own, that the surrounding culture dictated nothing enduring. Society may shape clothing fads or musical offering, many would suggest, but not the important stuff. The students’ position is that society really does not exist, because individuals maintain autonomy and freedom to believe what they wish.

19
strategy is to manufacture stupid wants that your company can get rich fulfilling, or pretending to fulfill.

Finally, we are *obviously* animals. It is hard to think of a more obvious biological fact. Like all other animals, we depend on a complex web of living and non-living things. While animals can adapt to changing conditions, there are hard limits on the extent of adaptation possible. When the environment falls too far outside of the conditions under which the species evolved, it dies. No species is exempt.
The thing about the STN

1. Even if you don’t believe it, you might behave as if you do
2. Rejecting the STN will have a profound impact on your views.
   - Eg: What work is worthwhile? What faculty should we hire? What should we do in the classroom?
3. The STN is fundamentally a religious point of view
4. It paints the technologist as the savior / hero
5. It serves corporations and the elite
6. It de-politicizes and de-moralizes our current crises
7. In its most extreme form, it devolves into the TESCREAL bundle of beliefs
   (= Transhumanism, Extropianism, Singularitarianism, Cosmism, Rationalism, Effective Altruism, and Longtermism) [Timnit Gebru, Émile Torres 2023]

Slide 14  I would like to make a few more comments about the STN.

14.1 The first is that even if you feel like you know better, that you see through all this crap, it might be irrelevant insofar as you live your life as though it were true. It might even seem that there’s no choice.

   Maybe you check your phone 144 times a day\(^{22}\) and you can’t really see a way to get along without the damn thing. Maybe you work for an employer that says they want to do great things for humankind, but you know full well that they haven’t a clue what that would look like. Maybe you eat factory-farmed chicken, cows, or pigs, aren’t too proud of that, but, well, nobody’s pure. Basically, just living out one’s life in the way that most everyone does will entail numerous behaviors and assumption rooted in the mythic corpus of beliefs I’ve called the STN.

14.2 Second, rejecting the STN will ultimately impact your view on just about everything. It will make you eccentric for a computer scientists or engineer. It will lead to significant isolation. That’s a high price to pay.

   Consider an everyday question, for a CS faculty member, like: what new faculty members should your department hire? Well, if you reject the STN then the last thing you’re going to favor is the kind of candidates most frequently sought and seen: a career-focussed, can-do, hot-area, run-a-big-group, strong-ties-to-industry, throw-tech-at-it evangelist. And when you argue against your colleagues’ flavor-of-the-day for this, on the basis that the candidate is yet another cog who doesn’t seem to actually care about the social impact of their work, your colleagues will pick up, correctly, that your critique is broad enough to sweep in them, too. Not a route to popularity.

14.3 I would note that the STN is ultimately a religious point of view. Like other religions, it is ultimately grounded in faith and an appealing narrative. Like other religions, it serves to separate rightful pursuits—those that advance technology and its use—and wrongful ones—those that would delay or thwart technological progress. And, like other religions, the STN promises some future utopia.

14.4 The STN is especially appealing to scientists and engineers. One reason for this is that it paints us as the heros of our culture’s story. Having mastered the technical arts, we can go about the important technical work of reinventing the world. I am not addressing here the megalomania of Elon Musk, Mark Zuckerberg, and the like, but the self-image of the ordinary computer scientist and engineer. Having learned the art of getting the machine to do your bidding, and having learned that you can pull a 300K+ salary for this, people come to see themselves as important. And since technological advance is itself seen as something good, there is little need for interrogating the specifics of one’s work. The work is well-paying and important. I must be, too.

14.5 The STN doesn’t just serve the economic interests of the individual technologist: it serves, even more, the economic interests of corporations, their principals, and their shareholders. By fostering a belief that technological advance is the natural order of things, the technological corporation is on a mission not just to make money, the story would go, but to advance mankind. What better narrative could there be to minimize taxes and regulatory controls, to position the corporation as having primacy over the lesser needs of individual and governments? Opposing the corporation is opposing progress, unethical way to be.

14.6 The STN works to de-politicize and de-moralize our current crises. In a world that fully embraces the STN, wiping out species and biomes isn’t a failure of ethics or governance; it’s just the cost of doing business. It’s only a problem, and a distant one, if it comes back to bite us.

14.7 Finally, in the cauldron of Silicon Valley, in the eyes of those who see themselves as rational, effectual, and ethical, the STN morphs into what Gebru and Torres have called the TESCREAL cluster of ideas: Transhumanism, Extropianism, Singularitarianism, Cosmism, Rationalism, Effective Altruism (EA), and Longtermism. The beliefs, which are strongly rooted in past eugenic movements, can be used to justify both extreme wealth and morally reprehensible behavior. For example, many EAs (ethical altruists) would maintain that working in finance, doing nothing of identifiable value, and giving some of your wealth to a well-chosen charity is a more ethical way to live than, say, being a compassionate physician devoting your life to Médecins Sans Frontières. And it gets worse. Some longermists believe that the world we should all be working to create is one in which trillions of human minds are embodied within super-galactic-scale Silicon computers. Under the logic of longtermism, an individual, culture, or government that made realizing such a vision 1% less likely would need to be stopped—killed or overthrown—for mankind’s own good. This is all just arrogant and stupid.

---

23 See, e.g., http://tinyurl.com/fb-salaries for software engineering salaries at Facebook.

While it is unclear that a commitment to the STN inevitably entails a commitment to TESCREAL ideologies, for the person who imagines himself a rational utilitarian, particularly one unmoored by humility or human emotions, it is an easy progression. Sam Bankman-Fried is an obvious example.  

Radical CS recognizes that CS — and technology more broadly — embeds values. It is never neutral. It rearranges power. It has tended to disproportionately empower big corporations, tech workers, and the elite. Doing so, it creates significant peril for people and the planet.

Radical CS aims to confront this. We want to reinvent CS in ways that empower ordinary people and disempower the already powerful. We want to reverse the environmental, social, and political peril we have helped create. We want to stop creating new risks.

Radical CS accepts that it may be better to dismantle a system than to tweak it. It recognizes that some projects ought not to be pursued at all — at least not now.

Viewed negatively: -STN-
Viewed positively: Radical CS

Slide 15  So what, finally, is radical CS? It is what you’d probably believe if you’re a computer scientist and, against all odds, you reject the STN. It is the negation of the STN, at least the aspects relevant to the practice CS. What does radical CS entail?

15.1 First, radical CS recognizes that CS—and technology more broadly—embeds values. CS is never ethnically neutral. It rearranges power. Often the shifting of power is not an accidental adjunct to some other purpose: it often is the purpose. Radical CS recognizes that the practice of CS has, since it’s inception, empowered governments, corporations, tech workers, and the elite. It was designed to do this. Radical CS recognizes that the shift in power associated to the growth of CS creates significant peril for people and the planet.

15.2 Radical CS aims to confront this shift in power. We want to reinvent CS in ways that empower ordinary people and disempower the already powerful. We want to reverse the environmental, social, and political peril that we have helped to create. We want to stop creating new risks. We need to do this even if it means that we must stop doing what we are currently doing, and don’t know what to do instead.

15.3 Radical CS accepts that it may be better to dismantle a system than to tweak it. Tweaking a system can be a move to make more palatable that which ought not have come to be. Tweaking a system—for example, claiming that you have made it more “fair”—can more deeply entrench a thing we do not want, and should be resisting.
Suggestions for a radical CS

1. Stop pretending that things are not fucked-up. It’s disempowering and dishonest
2. See the STN for what it is. A story. A culturally-fabricated narrative.
3. Identify the embedded values. They’re often explicit. Or easily coaxed out.
4. Stop pretending that CS holds answers it does not. AI is going to fix the climate crisis, food insecurity, lousy schools, ... Or: blockchain is going to be democratizing, stabilizing. ... Give me a break.
5. Don’t try to instill improved characteristics into rotten enterprises. “21st century liberalism is ensuring a panel at a defense industry conference called Building a Deadlier Drone has adequate gender diversity” Fredrik DeBoer
6. The first question to ask: should you build the thing at all? When we emphasize properties like fairness, accountability, and transparency we skip this question and get to lower-level ones. This is unthreatening to power and careers.
7. Attend to the primary reason for the thing; follow the money. Sure, a good ML-based system might read x-rays better than most radiologists. But that’s not from where the push comes.
8. Move slow and fix things. Flip the FB motto. Caveat: don’t move slowly on things that imperil us, like environmental collapse.
9. Foreground your employer’s social impact. Your own positive social impact outside the workplace won’t compensate for negative social impact in the workplace.
10. Stop the Orwellian double-speak. A whole slide for that!
11. Don’t sleep with the enemy. Don’t work for or accept money from those whose values you disagree with.
12. It’s the system, stupid. Growthism; industrial-growth capitalism.

Slides 16, 18, 20, and 22  Let me try to give some more concrete suggestions towards a radical CS.

16.1 To start, I think it’s important that we stop pretending that things are not fucked-up. We routinely do just that. When positioning where we are and how we can help, researchers seem to routinely lie in their papers and grant proposals. At the same time, teachers lie to their students, parents lie to their children, and most everyone lies to themselves. We might think we are protecting the vulnerable with all of this lying. But pretending that we are not on the brink isn’t protecting anyone. It’s telling someone to be calm when they need to get the hell out of the burning building.

Some people take issue with this suggestion. They say: You don’t want to come across as pessimistic because it disempowers. It kills the will to act. First, I think this is backwards. Our technological society is a culture of reflexive optimism. And if you believe that all will be well because technology will save the day, then there is no need for urgent action, no reward for broad thinking, and no basis for social-change movements. It is only when you believe that the world might not be okay that there is motivation for doing terribly hard and unpleasant things.

Anyway, what plays out better in the culture—optimism or pessimism—just isn’t the point. As a scientist or academic, honesty is supposed to be one’s first obligation. If you look out at the world and see grave problems and risks, is it not obligatory to frame one’s work in a way that reflects that?

There is a further reason to give primacy to the the possibility of doom: the precautionary principle. It holds that we must act so as to ensure the continuation of humanity—that we have no

---

26In deference to a request from NIST, whose code of conduct aims to protect conference attendees from offensive language, I changed the slide used in the NIST presentation from fucked-up to seriously messed up. Here I revert to my cruder diction. You messed up when you double-booked your appointments or wrote a bad final-exam question. The world’s problems are not of this sort.
Isn't it **better** to be optimistic?

**No** — at least not for society.

Excessive optimism — not pessimism — undermines social progress. It obviates
- the need for broad thinking
- the recognition of emergency
- the basis for social-change movements

Regardless: "better" isn't the point — there's that annoying honesty-thing

Also: existential threats motivate giving primacy to predictions of doom over prophesies of bliss even if one is skeptical of the former.

right to do that which has a realistic risk of ending us.\(^{27}\)

Unfortunately, however obvious or natural the principle may sound, we would seem to lack legal and political means to make it actionable.

16.2 Second, we should see the STN for what it is: a story. A culturally-fabricated narrative. The story that quietly and invisibly shapes our professional work.

16.3 Radical CS urges us to identify the embedded values within technological work. Often this is easy: in many research papers authors’ motivations are explicitly stated. Even if many researchers write their Introductions according to what they think will sell, well, even then, the values expressed will expose what the researchers themselves understand to be the values embedded within their community.

Slide #19 is from a paper called *The Values Encoded in Machine Learning Research*.\(^{28}\) The paper’s authors looked at a corpus of the 100 most cited papers from particular years of two top ML conferences. They identified sentences that spoke to the papers’ contribution. The tabulated results show that the well-cited ML authors hardly mention proximal human aims; instead, the authors focus almost exclusively on work that, compared to what it builds on, is more general, efficient, scalable, and such. Nerd-values, might one say. We must remind ourselves is that these aren’t the *only* potential values one can focus on in technical work.

Sometimes one must look a bit harder to see what’s valued. A paper entitled *The Surveillance AI Pipeline* uses bibliometric methods to evidence the seemingly obvious: that a primary purpose for

---


The Values Encoded in Machine Learning Research
[Birhane, Kalluri, Card, Agnew, Dotan, Bao 2021/22]

computer-vision research is mass surveillance. The paper documents, for example, that computer
vision research is cited by more than 11,000 surveillance patents. It also discusses the obfuscatory
language used by researchers to avoid expressing plainly what the work is used for.

Do the strong ties between computer vision and human surveillance mean that someone con-
cerned about the latter should avoid working on the former? I believe it does. But if when you’ve
invested years of your life in an area you may not want to reach that conclusion.

16.4 Next, I think we need to stop pretending that CS holds answers it does not hold. Nowadays
we see entire conferences and tracks of conferences that promise, for example, that AI is going to be
instrumental in fixing the climate crisis. Or food insecurity. Or the high cost of medical care. Or
the problems experienced in the “developing” world. Or lousy schools. Give me a break. These are
not issues caused by AI, and there are no remotely convincing arguments why AI would, overall,
make any of these problems better and not worse.

Closer to my own area, I don’t know how many times I’ve heard ridiculous claims about
blockchains being democratizing—this amazing tool to empower ordinary people. The claim seems
kind of absurd. And ironic, given that the primary use of crypto—meaning cryptocurrency—has
have been illegal drug purchases, financial speculation, ransomware and other financial scams, and,
nowadays, human trafficking—all activities that disempower ordinary people. Still, the STN
urges us to keep the faith. All of those democratizing, socially constructive uses of crypto—far
more significant than what crypto has been used for so far—they’re coming any day.

Why do technical people routinely believe that the tech they’re working on will end up doing

30For a harrowing account of Chinese-run, Tether-based cyberscam compounds in Cambodia, see Zeke Faux,
good—even when there’s little evidence to support that belief, and when it’s not what’s happened so far? Because we want to believe it. We all want to be working for more than our own self-interest. “I want to believe” worked well as a catchphrase for the X-Files. But magical thinking shouldn’t undergird one’s career.

16.5 Next, I want to warn about trying to instill improved characteristics into rotten enterprises. Doing so doesn’t make things better; it likely makes things worse.

As an example, a sizable community of researchers are working to make AI systems more fair. Never mind that nobody actually knows what fair means; we don’t have to answer that to be sure that it’s better if, for example, face-recognition systems do equally well on Black women and White men.

Except—not really. It’s reasonable to expect that lowering the error rate for face-recognition systems will just make it harder to get rid of them. Which is bad, because it’s hard to think of face-recognition scenarios that, even if they worked perfectly, have more upsides than downsides. They’re just too likely to contribute to mass-surveillance, resurgent fascism, and fear.

Other application areas where making it better just makes things worse include job-applicant screening and parole decisions. Removing human agency and accountability from domains that strongly impact people’s lives allows human to sidestep the ethically fraught decisions at the heart of being human.

Fredrik DeBoer once quipped that “21st century liberalism is ensuring a panel at a defense industry conference called Building a Deadlier Drone has adequate gender diversity.”

I think that a lot of us get caught in that trap, working on the edges to improve something that ought to be pulled out by its roots.

16.6 So the first question to ask about a technology is not how to improve it; it’s whether we want the thing, in any form, in our world. When we emphasize secondary concerns like fairness, accountability, and transparency we skip this most basic question. Which, conveniently, makes your work unthreatening to power. After all, one can always find some way to plausibly improve a system’s fairness, say, without eroding its ability to make its owner money. Which is why companies like Apple, Google, or Microsoft are fine with AI researchers trying to hack the fairness, accountability, or transparency of their stuff. They’ll even support it. It only becomes problematic when detractors begin to argue that the thing in question shouldn’t exist at all.

16.7 In assessing an area’s impact it is important to focus on its primary purpose. Follow the money; follow employment prospects. Yes, an AI-based system might do a great job of reading mammograms, say—but that’s not from where the push for AI comes, that’s not what students trained in AI will likely do. Most will work on that which drives AI forward: human surveillance, behavioral redirection, and job elimination. So it’s kind of disingenuous when the student or researcher says: Look, I’m interested in working in AI because I’m excited about what I’ve seen it do for radiology, astronomy, or the game Go. These are sideshows. They give the area a better reputation than it deserves.

Fredrik DeBoer, Tweet, user freddiedeboer, posted 3/14/2016 at 2:50pm.

This triple of desiderata comes from the FAccT Conference, the ACM Conference on Fairness, Accountability, and Transparency. In fact, the conference does have papers that go beyond this triumvirate.
The sideshows serve another important purpose: as a society, we can train students on scientific or whimsical problems and then ease them into the real stuff later on. The approach helps keep academics academic. Busily training an endless stream of young droids, CS professors become the functional antithesis of radicalism, regardless of the politics they espouse.

16.8 Every movement needs a motto. Here’s one motto for radical CS: *Move slow and fix things.* Just flip that idiotic Facebook motto.

What exactly are people rushing to, anyway? When we move fast and break things, the thing that breaks is usually *us*—particularly the most vulnerable of us. And the environment, that breaks, too.

Under the STN, rapid technological change is seen as inevitable and good. But it not a law of nature. Moore’s law is just stupidly named.

To make things worse, Moore’s law has been strengthened and generalized, with frequent assertions that accelerating change isn’t about transistors on chips, but applies to just about *anything* connected to technology. Ray Kurzweil, a prominent computer scientist and futurist, writes:

> An analysis of the history of technology shows that technological change is exponential, contrary to the common-sense ‘intuitive linear’ view. So we won’t experience 100 years of progress in the 21st century—it will be more like 20,000 years of progress (at today’s rate). ... There’s even exponential growth in the rate of exponential growth. Within a few decades, machine intelligence will surpass human intelligence, leading to the Singularity—technological change so rapid and profound it represents a rupture in the fabric of human history. The implications include the merger of biological and nonbiological intelligence, immortal software-based humans, and ultra-high levels of intelligence that expand outward in the universe at the speed of light.34

Kurzweil seems to believe that we have little choice in these matters—it’s just the way of the world. Get on board and enjoy the ride.

I persist in holding out hope that we actually have some choice in these matters—and that the smart choice is to apply the brakes and slow down. It is entirely possible that becoming one of Kurzweil’s *immortal software-based humans*, say, is *not* the best future for humanity. Not something to aspire to.

There is a caveat to move-slow-and-fix-things: we can’t afford to move slowly on that which imperils us. In particular, we need to promptly stop doing things that are destroying life on earth.

16.9 Another imperative in the program for radical CS is to pay attention to your employer’s social and environmental impact. It is hard to fathom how such a belief could be seen as radical. Yet I have seen from decades of teaching and talking to students that whether a prospective employer is doing something good or bad in the world is rarely a student’s concern.

16.10 Now here’s a radical suggestion: that we stop all the Orwellian double-speak that has come to pervade discourse in CS. Deceptive language has become so common we fail to even notice it. Terminology often seems *designed* to deceive—probably for some party’s benefits. Some examples.

An *algorithm* used to be a procedure to compute some particular function. You knew *what* you wanted to compute, but needed a smart way to compute it. Now an algorithm (new-use) means

---

33 Moore’s law is the observation that the number of transistors on an integrated circuit has doubled every two years, more or less.

Could we invent more deceptive language were this the explicit goal?

Language designed to deceive or distort its actual meaning, normally for the benefit of those in power.

Algorithm  (a) A program to compute some unknown function. (b) An opinion rendered in code.

Cloud computing  Putting your data on somebody else’s servers so that it can be stored in an unknown jurisdiction and mined by unknown parties for unknown ends. But at least it sounds fluffy and cool.

Crypto  Used to mean cryptography — the art and science of secure communication. Now it refers to a massive Ponzi scheme wrapped in technobabble. (P. Klugman, 5/21/2020)

Deep learning  Learning devoid of depth due to an absence of foundations and domain expertise and sociopolitical thinking.

Smartphone  A phone that is not smart and that pushes its users to be just as stupid. Also, the device should barely function as an actual phone.

Social media  Systems designed to sunder social interactions.

code that computes something, but you don’t know what. The function—if it even is one—has no characterization beyond the code itself. An algorithm computes whatever the hell it computes.

“Algorithms”, Cathy O’Neil explains, “are opinions embedded in code.” But opinions rendered by code are worse than opinions rendered by people. The techy aura of the former provides a false sense of authority, and provides cover to those motivated to minimize accountability.

Cloud computing is not an ethereal computing apparatus floating in the sky. It’s the practice of putting your data on somebody else’s servers—so it can be stored in an unknown jurisdiction and mined for unknown ends by unknown parties. But at least the name sounds cool.

Crypto used to be short for cryptography—the art and science of secure communication. This was my research area, and I was proud of the area. Cryptographers were smart, creative, and mathematically hip. Cryptographic solutions were often beautiful, subtle, and sometimes paradoxical. Now, however, crypto means (Post-Satoshi) cryptocurrency. It’s Bitcoin, blockchains, smart contracts, Web3, NFTs, and all that nonsense. Paul Krugman speaks of crypto (new-use) as a massive Ponzi scheme wrapped in technobabble.

Cryptography lost more than a word in the crypto (old-use) to crypto (new-use) transition: many crypto (old-use) folks were attracted by the prospects for wealth, power, and attention that the crypto (new-use) folks were getting, so we reinvented ourselves as the rightful masters of (new-use) crypto. Before, crypto folks might have been irrelevant or weird—but at least we weren’t players in a trillion-dollar scam.

---

35Probabilism, persistent state, Internet access, constant human tuning, even looking up the time of day—all of these things can take us out of classical realm of what a function even is.


I could go on and on. **Deep learning** is a branch of ML that uses neural-nets (which have little to do with networks of neurons) to fashion algorithms (new-sense) devoid of actual depth (due to an absence of domain expertise, sociopolitical thinking, and theoretical foundations). **Smartphones** are a surveillance device that aren’t smart and barely work as phones. Not content with their own lack of smarts, the devices work to make their users less smart, too. **Social media** is the ironic term used for systems that sunder social relations by encouraging people to type stuff into screens instead of having actual, in-person social interactions.

You probably think I’m being flip on all of this. Maybe a little. But it’s no joke that computer scientists and our sponsors end up with terms like those just given because we benefit from all the misleading language. And, rather soon, the misleading language has wormed its way into our thoughts, misleading us. For example, algorithms (new-use) become a legitimate way to settle pesky questions in part because the shadow of mathematical rigor left over from actual (old use) algorithms deceives us into imagining that something of social or intellectual legitimacy is going on.

16.11 My next suggestion is this: don’t sleep with the enemy. Don’t work for or accept money from those whose values you seriously disagree with. You might think that you’ll retain your sensibilities and integrity. You might think that you’re going to change the values of your sponsors. This is not realistic. When you take money from DARPA or Facebook or whatever, you will change, and they won’t.

16.12 Finally, I don’t think radical CS makes sense without trying our best to contextualize that we are not dealing with isolated technical problems. Our problems with technology are entwined with, and largely spring from, the system of industrial-growth capitalism in which modern technology is embedded. In short: it’s the system, and nothing will truly be changed without fundamental changes to our economic system.
The phrase **radical CS** is adapted from the

![Radical AI Network](https://radicalai.net)

**Radical AI Principles**

1. ...
2. ...
3. “We recognize that all technologies rearrange power.”
4. “We are critical of how AI shifts power. In particular, we recognize AI is frequently extractive, exploitative, surveilling, controlling, prescriptive, and reductionist. We recognize AI frequently prevents consent, deliberation, investigation, intervention, resistance, and agency.”
5. ...

**Slide 23** Let me pause for an overdue acknowledgment: that the oxymoronic term **radical CS** isn’t exactly original. I tweaked it from **radical AI**, the phrase chosen by a group of computer scientists who once invited me to give a talk. And perhaps I appropriated more than a name: the viewpoints expressed by the Radical AI Network largely intersect those expressed here. Most importantly, the Radical AI Network keeps a focus on how AI shifts power—rather than interrogating subordinate concerns, like fairness, as most of the ethics-in-AI world focusses on. For example, the group’s “Radical AI Principles” include “We recognize that all technologies rearrange power.” It continues:

> We are critical of how AI shifts power. In particular, we recognize AI is frequently extractive, exploitative, surveilling, controlling, prescriptive, and reductionist. We recognize AI frequently prevents consent, deliberation, investigation, intervention, resistance, and agency.

The quoted principle can be broadened, with **CS** replacing **AI** in the quoted text above.

---

38 See [https://radicalai.net](https://radicalai.net) (visited 16 Feb 2024).
At this point I’d like to shift gears a bit and describe three projects I’ve worked on that were, in retrospect, attempts at radical CS.

Let me start with my essay *The Moral Character of Cryptographic Work*, which was written to accompany a 2015 invited talk.\(^\text{40}\)

I received the invitation for this talk about two months after the Snowden revelations began. By then it was clear to anyone paying attention that the NSA had wormed their way into just about every piece of technology out there for digital communication and storage. They had, their slides explained, adopted a strategy to *collect it all*—so that, subsequently, they could *process it all* and *know it all*.\(^\text{41}\) In this extraordinary program of mass surveillance, cryptographic protections had proven to be barely perceptible speed bumps.

---

\(^\text{40}\) The 2015 IACR Distinguished Lecture, Auckland, New Zealand, Asiacrypt 2015. The essay can be found as ePrint 1162, http://tinyurl.com/tmccow

\(^\text{41}\) Slide from an undated NSA presentation, https://imgur.com/dVCiLz1
**Cryptography** – the science of **secure communications**.

**Mass surveillance** – the spectacular **failure** to **secure communications**.

So you might **think** that **cryptographers** would be **ashamed** and **aghast** about **mass surveillance** revelations.

**You’d be wrong.**

My community thinks things are going **great**, and that mass surveillance is **not our concern**.

---

**Slide 25**  
I felt that this ought to be a huge embarrassment for cryptographers. I mean, cryptography is, first and foremost, the science for enabling people to communicate or store things privately. The Snowden revelations had made clear that ordinary people had virtually no communication or storage privacy. Whatever cool stuff we might be doing as cryptographers, cryptography’s most **basic** real-world aim had gone spectacularly unachieved.

Yet few cryptographers saw it that way. In fact, most felt that the Snowden revelations were professionally irrelevant.

The first question I wanted to answer was *why*. My first talk in this space was titled: *Why most academic cryptographers don’t care about real-world protocols, mass-surveillance, or anything else that impacts your privacy or security*. The answer, in brief: *It’s the culture*. Our job, as we saw it, was to write cool papers. The rest was on somebody else. **In contrast**, I felt that our professional obligations went further, and that, as a community, we should be doing more to try to create a world in which ordinary people can and do communicate privately.

---


43 I would also point out that the Summer of Snowden was also, to the cryptographic community, the Summer of iO (Indistinguishability Obfuscation). This concerns turning a computer program into an obfuscated program in such a way that functionally equivalent and equally efficient programs $P_0$ and $P_1$ will give rise to computationally indistinguishable obfuscated programs $\tilde{P}_0$ and $\tilde{P}_1$. The 2013 paper that formalized this goal and evidenced that this it might be achievable came out about a month after the initial Snowden revelations. It is: S. Garg, C. Gentry, S. Halevi, M. Raykova, A. Sahai, and B. Waters: Candidate Indistinguishability Obfuscation and Functional Encryption for all circuits (capitalization preserved). 21 July 2013, ePrint, [https://ia.cr/2013/451](https://ia.cr/2013/451)
Suggestions from the essay

1. Do more crypto-for-privacy / anti-surveillance research.
2. Attend to problems' social value.
3. Be introspective as to why you’re working on what you are.
4. Look to current security practice and privacy needs as a source of probs.
5. Be open to diverse models. Regard all models as suspect and dialectical.
6. Think twice before accepting military funding.
7. Regard ordinary people as those whose needs you aim to satisfy.
8. Figure out what research would frustrate the NSA. Then do it.
9. Stop with the cutesy pictures. Take adversaries seriously.
10. Use the academic freedom you have.
11. Get a systems-level view.
12. Learn some privacy tools. Use them. Improve them.
13. Design and build a broadly useful cryptographic commons.

Slide 26  While much of the Moral Character essay was written from a 30,000-foot view, I did enumerate explicit suggestions (slide 26). For example, I urged people to stop drawing all those cutesy pictures of adversaries as little devils. I suggested that colleagues stop accepting DARPA money. I encouraged people to do whatever they thought would annoy the NSA.
I didn’t know what sort of reception my talk and essay would receive, so I was delighted when, within hours of posting it, friendly emails started pouring in. Rather soon, it was more emails than I had received about all the technical papers I had every written—combined.

Now, nearly a decade later, the emails still come in. They come from students, recent grads, and old-timers; from cryptographers and non-cryptographers; from academics and folks in industry. And the emails are overwhelmingly positive. Quite a few have told me that the essay changed their career trajectory.

I realized that the only way that I could be receiving this volume of positive emails was that I put words to ideas that thousands of people already believed. People like to see their ideas articulated, especially if they haven’t been seeing it.

I knew there were some people who hated the essay—yet I received only three critical emails: an NSA cryptographer (the “SIGINT Philosopher”) whom I had picked on a bit in the essay; a right-wing crazy; and a well-known colleague whom I won’t name. The last fellow was so angered that, he said, he couldn’t talk about it. But, in preparation for this talk, I reached out to him again. His response said that my teaching ethics was itself immoral; that he would never write about his politics and morals to me (so why was I writing about mine?); and that he thought it absurd that I would treat someone like Marcuse (a communist) or Einstein (a self-centered twerp) as moral exemplars. [W]hen you’re not morally/politically preaching you’re being idiosyncratic, he explained. *This would be fine in a paper entitled: “My Personal Tastes in Crypto Research”* (but not for a paper that claimed to be more).

I do not think this colleague’s critique aligns with that of others. What I have heard is, more, that cryptography is just not related to mass surveillance. And, also, that flagrantly political matters ought not to be addressed by scientists. Because it isn’t our role or our expertise. And—what goes unsaid—that getting involved could ultimately diminish our power and authority to speak out on technical matters.
My self-critique of the essay aligns with none of the above. The essay’s real problem, I’d say, was that it didn’t change a damn thing. When one looks at the body of academic cryptographic work before and after Snowden, nothing is different. In IACR conferences, it remains the case that almost nothing is motivated by curtailing mass-surveillance. Crypto-for-privacy, as I called it in the essay, is as marginalized as before. And since the primary motivation of the Moral Character essay was to increase the cryptographic community’s involvement in anti-surveillance work, I would have to give the paper a poor grade. Maybe a B-.

Don’t get me wrong: the Moral Character essay is the paper I’m proudest of (if it even counts as a paper). I never regretted the time, anguish, or angst it took to write it. All the same, the essay didn’t have the impact I hoped. It wanted it to help shift the ethos of my field. It didn’t.
“Our initial reason for developing ADSS was to address use cases involving journalists and whistleblowers. We were motivated by a conversation with journalist Laurent Richard [36,22], by the Snowden revelations [24], and by the development of Sunder [39]. We recognized that unadorned Shamir secret-sharing [40] wouldn’t do ...”

Slide 28 Let me move on to a second effort at radical CS, my 2020 paper *Reimagining Secret Sharing*. It wasn’t my first piece of technical work inspired by the Snowden revelations but it was the work most directly related to its mechanics.

---


Secret Sharing

[Blakely 79], [Shamir 79]

Slide 29  Secret sharing is a classical cryptographic problem independently invented, and solved, by Bob Blakley and Adi Shamir. The setup for classical secret-sharing (classical-SS) is like this. A dealer has some secret $M$ that he’d like to split up among a few shareholders. He applies some algorithm $\text{share}$ to $M$, getting a vector of shares, one for each shareholder. At some later point in time, some of the shareholders can reconvene and contribute their shares. If the requisite number of shares are provided then an algorithm, $\text{recover}$, will reconstruct the originally shared-out secret $M$. If fewer than the required number of shareholders get together then, even if they pool all their information, they’ll still learn nothing of $M$.

In this picture (slide #29) the message $M$ is broken into three shares any two of which enable the reconstruction of the secret: a 2-out-of-3 secret-sharing scheme. The access structure specifies which sets of parties are authorized to reconstruct the secret.

Shamir’s solution for classical-SS is simple and elegant, using polynomials over a finite field.

There are multiple ways that secret-sharing could potentially be used by whistleblowers and journalists. A party with a highly sensitive document or archive $M$ could share it out to colleagues so that each could cross international borders without possessing data that would, by itself, implicate $M$ and endanger the traveller. Or a journalist or whistleblower might try to protect himself from assassination by ensuring that, if he is killed, shared-out materials will be reconstructed and further developed by colleagues.


47 Returning to the old-use of the word algorithm.

48 The idea was expressed to me my journalist Richard Laurent in a meeting organized by J. Alex Halderman, October 2016. A subsequent conversation with the staff at the Freedom of the Press Foundation helped clarify practical secret-sharing goals.
The post-Snowden project I had in mind was simple: develop a versatile tool, and work out any associated theory, to enable a journalist or whistleblower to secret-share a document or archive $M$, splitting it up according to a user-specified access structure. In fact, the development of a secret-sharing tool, Sunder, was already underway by volunteers at the Freedom of the Press Foundation.$^{49}$ I wanted to create a tool that would be as easy to correctly use as possible. As with symmetric encryption, this meant that we should target strong definitions.

$^{49}$However, this project was eventually mothballed. See [https://tinyurl.com/meet-sunder](https://tinyurl.com/meet-sunder)
A lot. Classical-SS has a ton of unexplored problems that wreck its utility for what it’s ostensibly for.

Problems?

Simple, elegant, 45-year-old notion and technique—what could possibly be wrong or unsaid?

Slide 30 Classical-SS is almost 45 years old and there are, by now, thousands of papers in this domain, and dozens of definitional variants. Given that, one might imagine that there should be no theoretical work needed, just some programming, to create the desired tool. Surely secret-sharing would be found in numerous cryptographic libraries and tools.

Yet this wasn’t remotely the case. First, my colleagues and I soon saw that there were multiple reasons that an implementation of classical-SS wouldn’t work well for a safe and general-purpose tool. And secret-sharing variants in the literature didn’t seem to fare better. It was as though paper after paper had explored secret sharing without any paper being motivated by the obvious: create a safe, versatile, easy-to-use tool for a human user to share out a secret.

The gaps between that which classical-SS provided and that which human users would want weren’t especially subtle; multiple issues would be noticed right away. Let’s look at some.
Scenario #1

Shareholders must know their “position” — shares have implicit metadata

Slide 31  Here’s a first example to illustrate the gap. In classical-SS the recovery algorithm takes in a vector of shares, which means that every shareholder must knows her “position” relative to everyone else. But, in the real world, people don’t come numbered; a shareholder might not she’s person-3. Conceptually, it should be a set of shares that are input for message recovery, not a vector.\footnote{A reader could reasonably counter: this is overblown; you just put a number in each share. First, it’s not quite that trivial, as multiple (adversarially-provided) shares could claim to be share-i. Regardless, the issue isn’t how hard it is to fix; it’s whether the real-world setting is well-modelled.}
Algorithm share is randomized, so a share can’t be regenerated without retaining the coins. But the coins can’t be retained without destroying security.

Scenario #2

Here’s a more troublesome sort of problem. Suppose the secret the dealer wants to share out a strong passphrase kept only in his head. Suppose also that he’s going to meet up with shareholders on different days. Then, already, classical-SS has a problem. To achieve its privacy guarantee share needs to be probabilistic—the dealer must provide unpredictable bits to the algorithm—and the dealer will either need to retain those bits, or the undistributed shares, until he sees the last shareholder. Either gives rise to a serious security vulnerability. The hardware (e.g., the laptop computer) storing the coins or undistributed shares becomes an attractive adversarial target—and a target not modelled in the definition. In essence, classical-SS requires an all-at-once distribution of shares, which might not reflect what happens in practice.
Scenario #3

You’ll recover something — and get no indication anything is wrong.

Slide 33  Here (slide #33) is a different sort of problem with classical-SS. Suppose that one of the shares gets accidentally corrupted, or that a shareholder accidentally provides the share from some “other” sharing. Such mishaps are inevitable. But classical-SS guarantees nothing about what will happen if a share is wrong; the model assumes that shares will be accurate or missing. If a share is wrong then, typically, one will recover garbage—with no indication that anything bad has happened. But it could be worse: substituting a single share with an adversarially chosen one could allow the adversary to induce the recovery of any message it wants. Why shouldn’t secret sharing guarantee a shareholder that received a share from an honest dealer that it will recover either the originally shared-out secret or nothing at all? And, for that matter, why shouldn’t we guarantee recovery of the correct value, despite bad shares, if the remaining shares implicate a unique secret?
Such issues can be fixed, of course, which is what adept SS aims to do.

But your ending point — definitions, properties, and constructions — will be quite unlike classical secret sharing.

Just from taking seriously that you are trying to craft a practical too to actually split up a secret.

How did this work out?

The paper was technically successful; it solved everything it aimed to solve.

It was ignored. 6 citations. Even the journalists who brought the problem to our attention didn’t really seem to really need a technical solution.

Grade: C-

Slide 34  Problems like those I’ve described can be addressed with stronger definitions. The primitive we call adept secret-sharing (adept-SS) does this. Sharing is made reproducible, corrupted shares are detected, and so on. The move from classical-SS to adept-SS rather directly recapitulates the move from privacy-only symmetric encryption to authenticated-encryption, a change that transformed cryptographic practice. I was hopeful that adept-SS might spur the same sort of progress. How has that fared?

Not well. The paper on adept-SS is probably my most ignored piece of work. Four years after its publication, it has almost no citations.

The irony is not lost on me. This is the only paper I’ve ever written that involved interacting with non-corporate users: a journalist, a whistleblower, and an NGO. The only paper intended to result in a new privacy-protecting tool. But, in the end, cryptographic community didn’t even notice. In the end, even the target audience didn’t seem to need such a tool.

I gave a talk on adept-SS at RWC 2020. Afterwards, some folks approached who were interested in doing implementations. Great, I thought, just what I was hoping for. Then one of them explained his motivation: sharing-out keys for high-value crypto (meaning crypto-currency) wallets. I had made a tool for journalists or whistleblowers who wanted to expose wrongdoing, but the only people expressing an interest in implementing it wanted to help crypto bros protect their gazillions of unearned riches. Great.

I should grade myself again. I still think the adept-SS paper has good definitions, novelty, writing, and schemes. Yet the point of the thing was to pave the way for secret sharing to become a tool for at-risk whistleblowers or journalists. There is no sign of that happening. If this project was supposed to be a model for doing socially conscious cryptographic work, well, publishing ignored

51Real World Cryptography, the name itself a reminder that so little cryptography bridges research and practice that one could have a symposium that makes that its theme.
papers will inspire nobody. In view of that, I’ll say a C-.

It’s possible that it’s just too early; some papers take a long time to get noticed. If that’s the problem I can always file a grade-change request. But I don’t think this is what’s going on. The paper was pragmatic, political, definitionally complex, and without mathematical depth. It’s on a seriously dated topic. This is miles from where the cryptographic community is at.
2 c) A class: Ethics in an Age of Technology (2004-2023)

“I want you to think about **and act upon** the ethical implications of

- your personal **and** professional choices, **and**
- our collective **work** as technologists.”

Slide 35  My last example of trying to do radical CS is the class that I’ve been teaching since 2004, *Ethics in an Age of Technology*. The title is taken from a 1993 book by Ian Barbour, which also set the initial tone for my class.\(^{52}\)

At this point I’ve taught 30 sections of the class, over 18 terms; it has comprised about half of all my teaching for the last two decades. The class is a broad exploration of the human and environmental costs of technology, and a reflection on our personal and collective responsibilities as computer scientists. I invented the class because I became convinced that my university, like most, was mass-producing droves of amoral CS droids. That **itself** seemed phenomenally immoral. In teaching the class I hoped to increase CS students’ inclination to reflect and act upon, their personal and professional choices. Equally, I wanted them to reflect and act upon our **collective** work as technologists.

Teaching the class changed me. Each term I would invite the students to try to grow over the 11 weeks, and to end the class as better people than they started it. I promised that I would try to do the same.

---

20 years of teaching ethics

1. No lectures, just facilitate.
2. Genuinely listen
3. Allow no phones, no laptops
4. Forget moral philosophy
5. Steer far away from methodological approaches to ethical analyses
6. Encourage students to feel, not think
7. Select disturbing films and articles; have disturbing discussions
8. Don’t worry about the students feeling bad
9. Chatham House Rule
10. Urge students to be judgmental
11. Dismantle hyper-individualism, ethical relativism
12. Keep it personal: what we eat, where we work, how we die, ...

Slide 36 Here are some of the things I figured out about teaching ethics in a CS Department—expressed as though you will do that. Might you?

1. Don’t lecture; just sit in a circle and let the students talk. College kids won’t behave differently, or change their basic view on things, by being lectured to. And they won’t care about your opinion if it’s delivered from a position of performative authority.

2. Listen. This is hard when that student you’re interacting with seems to have the moral acumen of a tic-tac-toe program. Still, be gentle, respectful, and listen. Remember that there is generational divide—and the world we have bequeathed to the young is in rapid decay.

3. Strive for a technology-free classroom. Phones and laptops are incompatible, at least in a classroom setting, with enhancing empathy, activism, or introspection.

4. Forget traditional moral philosophy. Studying utilitarianism or deontology won’t make a student more ethical; it may well make them less ethical. One problem is that traditional moral philosophy is strongly rooted in rationalism—but behaving ethically is, I would claim, far more rooted in empathy and emotion. CS students generally rely too much on rationalism already. It’s why they gravitate to ethical altruism like flies to feces. CS students, and CS faculty, will find ways to use their reason to justify whatever they want. And, as if by magic, the rational view will somehow be the view that benefits them and their group. Forget trolley-cars and other fanciful scenarios that act to turns ethics into a puzzle-solving game.

5. Relatedly, steer clear of methodological approaches to ethical analyses. People who behave ethically don’t make lists of interested parties, they don’t study costs and benefits, and don’t
try to compute expected values. Thinking in such ways, I am convinced, drives one away from behaving well.

6. Instead, try to get the students to feel something. CS and engineering students might have forgotten how to do this.

7. How do you get the students to feel something? By forcing them to watch, read, or do disturbing things. I often turn to films. Something is wrong with a person who watches Earthlings (2005), say, and doesn’t feel sickened.

8. Don’t worry if students sometimes feel bad. Confronting uncomfortable truths is uncomfortable; there is no way around that. It is a purpose of higher education It is not the place of higher education to protect students from reality.

9. Try to make the classroom a space where students feel that they can speak in an unguarded way. To help with that, I always adopt the Chatham House rule: nothing that goes on inside the classroom may be attributed to anyone outside the classroom.

10. Encourage students to be judgmental. Contemporary college students have become so loathe to criticize anyone for anything that they can barely form ethical opinions, which routinely assert that someone is doing something wrong. Students gravitate towards ethical relativism, which logically and practically collapses to having no ethical views at all.

11. Similarly, call-out hyper-individualism, that toxic worldview, highly prevalent in the US, that everything revolves around personal choice, personal responsibility, and personal benefit. Hyper-individualism decapitates every analysis involving society, institutions, and collective action.

12. Finally, keep it personal and keep it real. Talk about what we eat, for example; it doesn’t get more personal that that (nor more profoundly at the intersection of ethics, politics, and technology). Talk about the behavior of the particular companies where students go to work. Talk about dying and death. In a world of contemporary, existential, all-too-real problems, talking about the rights of sentient robots, for example, turns sober engagement into sci-fi speculation.
Do basic attitudes shift?  

**Beginning — End (SQ23)**

1. Technology has vastly improved the quality of most people’s lives.
2. Technologically-created problems are usually amenable to technological solutions.
3. Technology itself is value-neutral: it is what people do with the technology that is right/wrong.
4. It’s impossible to accurately predict how a technology will be used, so it makes little sense to try.
5. Technology is driven primarily by human desires, as expressed through the marketplace.
6. There’s a good chance that human society will collapse as a result of anthropogenic climate change.
7. Because of technological advances, I will probably live longer than my same-gender parent.
8. I am generally optimistic about our collective future.
9. In making public-policy decisions involving technology, we should rely on the advice of experts.
10. It is morally acceptable to work at a US nuclear weapons laboratory like LLNL.

**Beginning — End (SQ23)**

11. It is morally acceptable to work for a fossil-fuel company like Chevron.
12. It is morally acceptable to eat factory-farmed beef (e.g. McDonald’s, In-and-Out, Safeway)
13. It is morally acceptable for an able-bodied student who lives in Davis to routinely drive to school.
14. There is no right or wrong in this world; everything is relative to your culture or personal beliefs.
15. Most people behave ethically most of the time.
16. It’s important to me that my life have a net positive influence on the world.
17. When considering my future employer, the societal value of what they do is crucial.
18. I am morally obligated to follow the law even if I don’t agree with it.
19. Well-educated people tend to behave more ethically than less educated people.
20. Major aspects of my moral perspective are unlikely to change at this point in my life.

**Slides 37 and 38**  Does spending a term in the class change anyone? I have reason to think that it does. I often survey student attitudes at the beginning and end of the term, trying to see the extent to which students’ basic views on technology change. I ask how much students agree with statements like: (a) Technology itself is value-neutral: it is what people do with technology
that is right or wrong. (b) There’s a good chance that human society will collapse as a result of anthropogenic climate change. (c) It is morally acceptable to work for a fossil-fuel company like Chevron. (d) it is morally acceptable for an able-bodied student who lives in Davis to routinely drive to school.

The traditional view is that questions like these don’t have right or wrong answers. I’m not so sure that is true. A claim like the first (that technology itself is value-neutral) simply does not hold up to critical analysis. It’s an assertion with which no STS scholar would agree.
How did this work out?

Many students do change. Course seems to have a profound impact on values of many, perhaps most.

But ... ~24 per class. Not remotely commensurate with the problem. And I have never known how to scale this up ... if that is possible at all.

Grade: B+

Slide 39  While I might hope for larger changes, I have seen that students’ basic views on technology do change. For at least a few students each term, the STN has begun to slip from an obvious truth to a contested narrative. Students tell me that they have changed. They say so at the end of the term, or write me an email years on.

Having a major impact on even one person’s life is meaningful; it should not be minimized. But teaching upper-division students at a rate of 24 per eleven-week class—it is, in the end, a little thing. In my 20 years of teaching ethics, I’ve taught my ethics class to about 650 students, while my Department has graduated about 5,000. I was unable to institutionalize my class; when others teach it, it’s a very different thing. When I retire, the class will mostly die.

It is curious: why would a class so critical of CS be tolerated by a CS Department? First, professors still do have some autonomy over what goes on in their classrooms. But, more than that, nobody at the university really cares enough about what happens in a small undergraduate class to complain. And it is understood that, in the context of a student’s total experience in CS, a bit of techno-skepticism is little more than noise.

For a grade, I’ll give myself a B+. Inflated relative to the last one, perhaps, but grade inflation continues apace. Anyway, teaching has different goals than writing; connecting with some students is defined as success.
Concluding remarks

CS, and technology more broadly, is full of smart people that are ethical morons. Don’t be one.

My efforts at radical CS haven’t been very successful. But you can do better. There is a community of people who care about these things. And a rich history of waxing and wanning efforts to make technology more responsive to human needs.

“In dark times, it does no good to pretend that you are not living in dark times”

Ira Glass, This American Life, 781: Watching the Watchers, 7 Oct 2022

Slide 40  It is time to wrap up with a few final comments.

First, I would express that, over my long career, I have observed no correlation between how good someone is in their technical field and how good a person they are. It is possible to be an excellent researcher or scientist and, at the same time, an ethical moron. Don’t be like that. It’s a bad combination.

There are reasons, of course, why my attempts at radical CS failed to earn top grades. One reason is that the course is crazy hard. Nothing one can do about that. But another problem is that I worked too much in isolation. Social change comes from communities; if you want to change the culture within CS, you need to be a part of a community that wants the same thing, something I have never been good at. My advice, if you’re similarly positioned but at an earlier stage in life: get better at this.

Third, I want to acknowledge the absurdity of suggesting that there is anything genuinely “radical” in any of the the projects or ideas I’ve described. And yet, somehow, we inhabit a world in which it actually is somewhat radical for a computer scientist to write a political essay, to teach a course outside his lane, or to rework a basic concept in his field because of political concerns. We should not lose sight of how absurd that is.

Finally, let me come full-circle to the first claim I enumerated on Slide #16. Expressed less gruffly than before: In dark times, it does no good to pretend that you are not living in dark times. As our the world continues its slide into environmental, social, and political ruin, we should stop retelling ourselves the same threadbare stories that propelled us to this point.

54 Well, nothing beyond a general expectation that richer individuals tend to behave less ethically. See, for example, P. Piff, D. M.Stancatoa, S. Côtebm, R. Mendoza-Dentona, and D. Keltner: Higher social class predicts increased unethical behavior. PNAS, 109(11), pp. 4086–4091, 2012.

54 Ira Glass, This American Life (radio program), episode 781: Watching the Watchers. October 7, 2022.
Acknowledgements

Mihir Bellare and I have been discussing the invisibility phenomenon for decades. Mihir even taught a class with this as its theme, and using almost the same term: *Seeing the Invisible*, he called it.\footnote{Mihir Bellare, UCSD course CSE 209B (Winter 2021), \url{https://tinyurl.com/mihir-seeing-the-invisible}}

A short precursor of this talk was given at a hackathon event, HackDavis, on 20 May 2023. I likewise titled that talk *Radical CS*.

Many thanks to Morris Dworkin for the invitation that led to this essay and talk. And thanks to all of the kind folks who converged at NIST on that autumn day—even the NSA people hiding in the back—who made that workshop a pleasant memory.