AI, Encryption, and the Sins of the 90s

Meredith Whittaker

Keynote address delivered to the Network and Distributed System Security (NDSS) Symposium, San Diego, California

Feb 27, 2024

Hello everyone! Thank you so much for having me. I'm Meredith Whittaker. I'm the President of Signal and a longtime scholar and tech worker. It's an honor to be here and to have this opportunity to introduce research I've been developing over the last year as I endeavor to better understand how we can win in the fight for privacy.

So let's get started.

Late last week, the wonderful lawyer and privacy advocate Riana Pfefferkorn hit up our group chat on Signal letting me know that a Nevada AG had filed a motion for a temporary restraining order against Meta, aiming to prevent the company from providing end-to-end encrypted and private messaging via its Messenger service to minors in the state. Yesterday, the court rejected the motion. But that's not the end of the case. And while the legal reasoning is threadbare, with all the hallmarks of a weak PR op, it's also the most direct attack on encryption I've seen in the US since San Bernardino and the iPhone standoff.

And it comes at a bad time, when the stakes are very high and our army is depleted.

In early 2022, Jessica Burgess, a mother living in Nebraska, helped her daughter access reproductive healthcare and contend with the aftermath of this decision in the wake of the US Supreme Court's Dobbs ruling. Nebraska, like many other states, responded to the court's decision by criminalizing abortion.

Burgess is now serving two years in prison thanks to Meta turning over unencrypted Facebook Messenger messages to law enforcement, which provided key evidence used to charge and convict both Jessica and her daughter.

Here we have a single, chilling example of the seriousness of the threat posed by these attacks on privacy. And an object lesson in the real, human costs of our continued failure to secure meaningful privacy.

This failure helped actuate a world where unfathomable amounts of private data reside in the hands of a handful of US-based companies that–being companies–will ultimately comply with government mandates. Whether that government is benevolent, or working to criminalize healthcare, LGBTQ rights, access to literature, and the like.

The Nevada case is just the latest in a string of pernicious anti-privacy litigation, legislation, and rhetoric that has emerged with renewed force over the last 3-5 years, attacking in particular the public deployment and use of strong end-to-end encryption, and working to subtend privacy and expression to the position of second-class rights–if that.

These attacks threaten to effectively eliminate the ability to speak honestly and intimately, to experiment with new ideas, to blow the whistle, engage in rigorous journalism, conduct human rights work under authoritarian regimes, access reproductive healthcare or LGBTQ resources, and generally to live a full and dignified life in a world riven with surveillant digital infrastructures at a time of rising, if unevenly distributed, autocracy.

And while these attacks are often parochial, emanating from a given jurisdiction or province, and used by small-time politicians to score political points, the threat they pose is universal. Every time. Because of course you can't backdoor or undermine a network in one location without corrupting it in all others. This is how a law in the UK could have significant implications for, say, the government-in-exile in Belarus, and others like them who rely on private digital communications for fundamental safety and security.

Now, I and others have sometimes used the term "crypto wars 2.0" to describe this recent spate of attacks. It's an easy analogy. But it's also inaccurate. What we're facing now is worse–in large part because of what's changed in the interim.

Today, in 2024, mass surveillance of a scale and granularity unimaginable in the 1990s has cemented itself as one of the world's most profitable business models, conducted by massive consolidated (and largely US-based) firms like Meta, Google, Microsoft, Amazon, and others in service of targeting and influencing the billions of people who interact with their near-ubiquitous services.

Put another way, the economic engine of the now-mature tech industry is surveillance–either you monetize data via surveillance advertising, or you're providing services and infrastructure to those that do.

Or, yes! You're one of the few, like Signal, swimming against this fierce tide. And in a world that looks like our current tech ecosystem, bastions of real communications privacy–like

Signal–are essential core infrastructure. Undermining these would leave a landscape with no place safe from centralized corporate surveillance.

Sadly, the news gets worse. Because this engine of mass surveillance, far from being questioned and curtailed, is currently being supercharged by the bigger-is-better AI goldrush–which has taken on quasi-theological dimensions, led by these same companies. This has impelled a push for more, and more, and more data–aka surveillance–to train and inform corporate AI systems.

Given where I am speaking this Tuesday morning, I doubt many in the audience are hugely antagonistic to this stance, although I'm sure we can debate the specifics. In my experience, those close to these systems are the people who recognize how–and for whom–they work.

Meaning that these folks–that all of you–are essential in the fight to preserve and, crucially, extend the tools and spaces of meaningful privacy. We need you involved, speaking out, and working together to strategize to win.

I've briefly sketched the peril of our situation, and why fighting to gain back the privacy ground we've ceded is so important. Now I want to make the case that in order to keep the ground we have, and from there to gain more, we CANNOT rinse and repeat the 1990s crypto wars playbook. We need to refuse the dated, market-centric folk wisdom that is content to leave the governance of significant choices about fundamental rights–like expression and privacy–to a handful of private companies, assuming the invisible hand will work some B-Corp magic. And we cannot focus on technology in a vacuum, ignoring the social, political, and historical forces within which it is produced and deployed.

Because making these strategic mistakes in the 1990s–in particular, the mistake of trusting industry and "the free market" while viewing the government as the sole threat to fundamental rights–is a big part of how we got here.

■ ■ ■

With that, let's turn to this history, starting with a revision of the story we tell about the crypto wars.

Here, I draw on the work of Dr. Sarah Myers West, Dr. Chris Gilliard, Dr. Karina Rider, and Dr. Matthew Crain, among other scholars who've spent time on these issues and in these archives, and come out with brilliant analyses. I am grateful to their work, in addition to germinal research by people like Simone Browne and Seda Gurses. When I post this video

on various platforms, I'll include links to relevant papers for those of you interested in digging deeper and learning together.

Now, let's start at the beginning with some definitions for the young people. What are the crypto wars? Well, children, the crypto wars refer to a series of legal battles, campaigns, and policy debates that played out in the US across the 1990s. Here, questions about who should be allowed to develop and deploy strong encryption, and whether that encryption should be adulterated to enable government access, were fought, litigated, and more or less resolved. In decades prior, the government had asserted an effective monopoly on encryption, so much so that the academic field of cryptographic research was starved, as the NSA and others claimed the right to control and obscure work on cryptosystems. While this loosened somewhat in the 1970s, the government's desire to control the output of this research continued to put significant roadblocks in the way of wide dissemination. Moving into the 1990s, cryptosystems were still classified as munitions and subject to strict export controls. And in order to integrate them into products or services and distribute them broadly, you needed government permission.

This regime of secrecy and restriction ended, more or less, with the liberalization of strong encryption in 1999. Following that, companies and practitioners could develop and use strong encryption without being subject to controls, and academics could freely publish their encryption implementations without fear of government reprisal if someone in Europe downloaded their package. This was a win. And it was thanks to much creative and good work by technologists and advocates–Matt Blaze, Dan Bernstein, Cindy Cohen, EFF, EPIC, and the advocacy group Computer Professionals for Social Responsibility all played a part!–alongside powerful tech corporations whose interests, when it came to liberalizing encryption, aligned with theirs.

Liberalizing strong encryption was an important win. But the result of this win was not privacy. Indeed, the legacy of the crypto wars was to trade privacy for encryption–and to usher in an age of mass corporate surveillance.

To understand how this happened, we need to bring the process of commercializing networked computation into scope–the creation and regulation of what we ended up calling the internet.

Emerging from the mid-1980s, and gaining speed in the early 1990s, a vision of prosperity focused on what would become the internet seeded itself in US political circles, particularly among Democrats.

A potted account of this history goes something like this: following a sustained economic downturn related to manufacturing decline in the US, powerful members of the Democratic party followed the neoliberal spirit of the 1980s and shifted their base, from

labor and the white working class, to professional workers and the high-tech industry. The term “Atari Democrats” was coined at the time to refer to those leading this charge. And they promoted a vision of economic prosperity yoked to the high-tech sector.

It was this vision that fueled the Clinton administration’s drive to privatize and commercialize networked computation at exactly the time this appeared increasingly possible–given the rise in personal computing, and the fact that databases and networking were becoming powerful enough to support the aspiration.

The hopes pinned on the emerging commercial internet were big. We see this in contemporaneous projections. For example, in 1998 the OECD projected “a $1 trillion economic commerce market by 2005,” while in the mid-1990s Business Week estimated that “electronic commerce could boost the U.S. gross domestic product by $10-20 billion by 2002.” In 1996, meanwhile, the Commerce Department affirmed that “the total value of electronic commerce…will be close to $1.4 trillion by 2003.” And remember, they’re talking 1990s dollars.

These projections paint a representative picture, showing simply that there was a lot riding on the success of the commercial internet–including booming financial markets driven by frenetic speculation on the so-called dot-com sector.

Importantly, this ambition was also global in nature. The goal was not simply to create an internet to serve people in the US, but to nurture a US tech industry that could dominate the global market, setting the terms and standards that would define “the internet” for everyone. And as we see, everywhere around us, this largely worked.

This drive to commercialize the internet provided a catalyst for the crypto wars. The push to commercialize forced the issue of encryption, and brought it to a head.

Because in order to commercialize networked computation and fulfill these visions of riches and reach, confidentiality and authenticity are essential–particularly in the context of commerce and financial transactions. And, as we have it, ensuring confidentiality and authenticity in the context of networked computation is, quite literally, the set of problems that Whit Diffie and Martin Hellman developed public-key cryptography to solve–something we see clearly in their germinal paper, New Directions in Cryptography, published in 1976.

Or, as technology writer Peter Wayner put it in 1997, “cryptography is a crucial technology for preserving computer privacy and making commerce possible on the Internet.”

So, encryption was essential for the commercial internet. But law enforcement and security services saw any network resistant to government surveillance as a threat and a problem.

So how to square this circle–particularly the conundrum of achieving global technological dominance, while giving US law enforcement access, without losing non-US customers understandably reticent to invest in technology that provided a foreign government with a backdoor?

There were many failed, even laughable attempts throughout the 1990s, and I will not spend time reviewing them in detail–from the busted Clipper chip proposal that Matt Blaze popped only months after the spec was published, to the various plans for corporate-run key escrow schemes whose naming conventions changed across the decade but whose premise remained more or less the same, to the performance-art-cum-lawsuit that was Dan Bernstein's attempt to publish his crypto algorithm, Snuffle, without State Department permission, and which brought EFF to his defense in a historic lawsuit. All of this history is worth visiting, and is also well-documented elsewhere.

So I'll leave it for another time, and focus here instead on the bigger picture, and how it got us where we are today.

■ ■ ■

As Matthew Crain details in his excellent book, Profit over Privacy, the process of commercializing the internet–which catalyzed and played out alongside the crypto wars–ultimately resulted in unfettered private-sector surveillance.

In 1997, as Crain documents, the Clinton administration published The Framework for Global Electronic Commerce, laying down the rules of the road for commercializing the internet. This framework endorsed advertising as the revenue source for internet commerce, which it argued would "allow the new interactive media to offer more affordable products and services to a wider, global audience." And it put no restrictions on surveillance by private companies.

It's important to understand this as the US government not only permitting, but also incentivising mass commercial surveillance. Because of course the more you surveil people, the more you 'know' about the potential customers you're advertising to, and the more ably you can classify them, make inferences about them, and target them with

messaging and images that will shape their opinions and behavior. Or, at least that's the theory, and that theory moves billions of dollars.

We should note as well, as Crain lays out, that the embrace of unlimited surveillance advertising was not inevitable. Nor was it the only option on the table. Indeed, throughout the 1990s the surveillance business model and its potential harms were being actively examined and debated, and many alternatives–from publicly funded networked computation, to subscription models–were on the table simultaneously. Nor were the privacy harms unforeseen. Technical experts, civil society groups, and even the government's own advisors and agencies warned that permitting unfettered commercial surveillance could be unconstitutional, and lead to significant infringements.

Nonetheless, as Crain puts it, "The legacy of…[the 1990s] is the concentration of surveillance capacity in corporate hands and the normalization of consumer monitoring across all digital media platforms."

■ ■ ■

Now let's bring these threads together.

It was 1997 when the Clinton administration published their framework, permitting and endorsing surveillance advertising. And just after that, in 1999, the US government finally liberalized strong encryption, all but eliminating export controls and making it legal to create and disseminate strong cryptosystems broadly without government interference or permission.

This is generally narrated as the end of the crypto wars and as a win for privacy. And when I was coming up in tech, in the mid-2000s, it was commonsense folk wisdom to view this outcome as the reasonable triumphing over the retrograde, as the moment we secured privacy and at least partially revised the musty US legal code to recognize technology for what it was–borderless, resplendent, and unsuited to regulatory restrictions.

It's not that 1999 wasn't a win, at least in a narrow sense. Indeed, we can craft a counterfactual history in which the liberalization of encryption didn't happen, in which we instead accepted some janky, backdoored, government-standard cryptosystem–some sad Clipper chip DES admixture–and that instead became the thing: a world in which strong cryptosystems did not receive the benefit of many eyes and open scrutiny. But of course the future from then to now would have been very different–not least of all

because the metastatic growth of SSL-protected commerce and RSA-protected corporate databases would not have been possible.

And, as we see now, enabling permissionless creation and use of strong encryption was not at all sufficient when it came to ensuring meaningful privacy for people.

Because the power to enable–or violate–privacy was left in the hands of companies, not those who relied on their services. Companies that were incentivised to implement surveillance in service of advertising and commerce, and that were left to choose where and how, and for whose benefit, they deployed encryption.

Of course, technologies like SSL were rapidly implemented to protect commercial transactions, whereas technologies like PGP that could ensure end-to-end messaging privacy languished outside of the standard functionality implemented by large email providers. Dr. Sarah Myers West puts it succinctly when she states that the legacy of this period was making the internet safe for companies, but not for people.

By conflating encryption with privacy and focusing narrowly on the tech itself–on encryption as the goal, not a means to the goal–while focusing concerns about privacy invasion solely on governments, assumed to be always on the verge of tyranny–while ignoring (or even celebrating) the interests of market actors, the legacy of the crypto wars is one of empowering the burgeoning surveillance-based tech industry to a far, far greater degree than of securing privacy for the vast majority of people.

I am, of course, not the first to lament these dynamics, or to claim a loss. Among the more clear eyed-cum-cynical hacker community, the sentiment that “we lost the war” has been asserted and debated in emotional tones since at least the mid-2000s. Rop Gonggrijp and Frank Rieger voiced this view all the way back in 2005 in a prescient talk at that year’s Chaos Communication Congress, lamenting the incursion of surveillance and the centralized control of technical infrastructures post-9/11.

But what we must add to the average hacker jeremiad is an analysis of the political economy of the tech industry, alongside a skepticism of the market that matches the deep (and warranted) distrust of government and security services, in addition to an understanding of the unevenly distributed gaze of surveillance, and the racialized and gendered disciplinary regimes that surveillance works to underpin–something that Simone Browne, Seda Gürses, and many others have worked to illuminate.

Lacking these analytical underpinnings, such laments often take the form of reprimand and reproach–admonitions to the technical community that assume we are, each of us alone, capable of making individual choices and changes that will create better or worse technological futures. That it’s our fault for using a MacBook, or Gmail, or having a

Facebook account. That it's our responsibility to use encryption, to demand metadata protection, and the like. Of course, no one likes to be scolded, and so these messages often land poorly.

But beyond that, they're not accurate. We don't really have this power, at least not individually, and *that* is the problem to solve.

What we face now is largely a result of our having ceded the right to make decisions about our technological infrastructures and their dimensions to a handful of companies, and the VCs entangled with them, and this problem will require more than righteous individual habits to contest.

■ ■ ■

Now back to history, and the aftermath of the 90s.

Following 1999, an uneasy but stable compromise emerged between law enforcement and private tech companies.

The outcome of the crypto wars and the emergence of the commercial surveillance internet–taken together–created a "have your cake and eat it too" scenario for law enforcement and the emerging internet industry.

As Karina Rider brilliantly documents, companies could proceed in building security and privacy into their products and services in ways that could guarantee commercial transactions, enable authentication, and create a global market. And instead of publicly requiring a backdoor in encryption, the government could quietly turn to industry for help.

Following the 90s, government surveillance of the internet was effectively privatized. In this way both companies and government avoided an extended, public confrontation over encryption and the limits of lawful access. Data created and collected by these firms could be shared with the government quietly, protected from public scrutiny and outrage by the twin concealments of classification and corporate secrecy.

And it's arguable that this was no coincidence–although I have no hard proof here. Reading between the lines, it makes sense that law enforcement and the security services ultimately realized that giving up control over encryption would be OK in a context where the Clinton administration permitted private sector monitoring of online activity, and where they could work with these companies to access this data. Indeed, Rider's work shows companies arguing as much throughout the crypto wars.

We also have Snowden to thank for helping us align these histories, and adding ballast to this hypothesis. The revelations his courage brought to light show that, as if on cue, in the year 2000, just after encryption was liberalized, the NSA established a program codenamed BULLRUN.

As Rider notes, BULLRUN was dedicated to brokering relationships with private tech companies to gain access to surveillance data and, where access was not forthcoming, to use other means to undermine encryption. Documents reveal that the NSA went as far as allegedly paying RSA $10 million to add a vulnerability to core encryption software that they sold to customers. The agency also, allegedly, convinced Microsoft to add vulnerabilities to their Outlook email client–among much else. And lest we think it's just the NSA, the UK's GCHQ had a similar program, codenamed EDGEHILL, which also worked to gain access to private surveillance data.

And, thanks to the Clinton Administration's decisions to place no guardrails on commercial surveillance, this data was far more extensive and comprehensive than anything the government could have dreamed of previously–or could even legally collect, in many cases.

It was the Snowden revelations themselves, in 2013, that troubled this equilibrium.

Following evidence of their complicity in often illegal government mass surveillance, tech companies scrambled to regain trust, pointing fingers at the government while working to shore up their privacy bona fides. This wasn't a bad thing. It increased use of HTTPS and other privacy-preserving techniques, and saw strong encryption added to the iOS and Android operating systems–among other measures that enabled very important expansions of security and privacy for the people reliant on corporate tech systems. It also propelled the use of the Signal Messaging app, and the application of the Signal Protocol. But the post-Snowden privacy moment still left the power to make these decisions largely in the hands of companies, whose business models continued to rely on surveillance.

In my view, the ferocity of the current attack on e2ee, and other privacy-preserving technologies, is very much related to a desire by some in government to return to the less fettered access to surveillance that they see as having lost post-Snowden.

I'll get back to this spate of attacks in a moment. But first, and finally, I want to touch on

how this all relates to AI. And how an awareness of the role of AI in the current tech landscape ties into the strategy we must adopt if we're to fight for and win meaningful privacy here and now.

■ ■ ■

Because of course AI didn't just happen. The field of AI is over 70 years old, and the term itself was coined in 1956. Over the course of its existence, it has been applied to a heterogeneous mix of technical approaches that share, perhaps, a common aspiration, but very little else. So, AI is best understood as a marketing term. Certainly not a technical term of art.

Why, then, has it come to dominate tech in the last decade? The answer to that question is also rooted in the 1990s, and the surveillance business model.

In brief, in the early 2010s researchers showed that AI techniques from the late 1980s could perform new feats when matched with significant amounts of data and significant computational resources. This kicked off the current AI boom.

The companies at the forefront of the surveillance advertising business–the Googles and the Metas and the like–recognized quickly that their wealth of data, and their computational infrastructures, gave them a significant advantage. Or, that what was new in AI were exactly the resources they, and few others, had access to.

They also recognized that these AI techniques could be productively applied to refining ad targeting, news feeds, and other core elements of the surveillance advertising business model. It's no accident that all of the authors of the germinal AlexNet paper that kicked off this boom were almost immediately hired by Google, nor that Yann LeCun, whose work in the 1980s underpinned the AlexNet approach, was quickly hired by Meta.

With this in mind, the AI we're talking about today needs to be seen as an extension of this surveillance business model–a way to expand the reach and profitability of the massive amounts of data and infrastructural monopolies that these large companies possess, and that due to the self-reinforcing nature of networked business models, few others can or do. And that in this current bigger-is-better paradigm, where the few companies that possess these resources are competing to create and deploy increasingly data- and compute-intensive models, AI is exacerbating and entrenching corporate mass surveillance.

It’s incentivizing the expanded creation and collection of data about people, their communities, their habits, politics, locations, faiths, kinks, health conditions, financial health, family ties and ruptures…and so much more in service of training and informing these models.

And let us not forget, once trained and deployed, these AI models create MORE data–forminganother vector of mass surveillance that, while generated via inference not by, say, triangulating a ping to a cell tower to deduce location, nonetheless has power over us and creates narratives about us.

So here we are.

We’ve just taken a rapid, abbreviated tour through relevant history, which shows that we cannot view the crypto wars as an unequivocal win for privacy. That in fact this legacy is more accurately understood as helping enable mass corporate surveillance, empowering companies (and with them governments) but not the people subject to their tech.

Now, I want to be clear. I do not offer this in the spirit of a gotcha, or a reprimand–and certainly not to argue defeat. I’m in this fight! And I believe that protecting e2ee, and defending and expanding the places it’s implemented is a key plank in a critical struggle to gain ground on meaningful privacy and autonomy–a struggle that couldn’t be much more important, given the context we’re living in.

Which is why I spend time putting this history under a blacklight, in order to see what we missed, learn from the past, and build strategies now that avoid these traps.

Because we’re facing some very real, and very severe threats, and we cannot rinse and repeat old tactics in this context.

These threats to privacy frequently build on the back of justifiable concerns relating to surveillance advertising platform practices and affordances. The outcry against these practices is often referred to as the tech-lash, and focuses on harms like doxxing, influence operations, and targeted vitriol that surveillance advertising platforms have facilitated, and that gained significant attention following the 2016 election.

Starting around 2018, reasonable and misguided proposals to address and curtail these harms emerged from academics, think tanks, and legislators–calling on governments and companies to, for example, monitor and make a distinction between real and fake content,

or to stop putting algorithmic weights on the newsfeed scale, or to age-gate and censor content deemed inappropriate. And many of these focused on children, real or imaginary, who were centered as victims of these harms.

Now, Big Tech accountability, in general, is something I'm a big fan of! But in many cases, when you look under the hood, that's not what we're getting.

Under the banner of accountability, we're seeing proposals like the UK's Online Safety Bill, the EU's CSAM act, Australia's eSafety industry codes, and most recently Nevada's embarrassing but dangerous motion to restrain Meta's application of e2ee.

These proposals share a common, and deadly misstep: they leave the fundamental business models and surveillance practices of these companies untouched. Sometimes, they even mandate expanding it. And instead of perturbing the business model, they propose increased monitoring, gatekeeping, and control of content, behavior, and access. More oversight boards, more editorial rules, more precarious workers in the majority world trawling through our digital sewer cleaning up the mess that one-size-fits-all advertising platforms created!

To add to the problem, this is happening at a time when weariness and frustration with arguments for privacy and free expression have gained some purchase, weakening our coalition. Exasperation at the way the US First Amendment, and Section 230 have been deployed to shield these companies combines with a sense among some that arguments for privacy and speech are being wielded simply as socially acceptable pretexts leveraged by those who want to maintain the status quo, not challenge it.

This environment has left the army of those fighting for meaningful privacy, and against the centralized corporate and government control of expression, very thin.

And this helps explain, in my view, how proposals to backdoor, and even eliminate e2ee made their way into policy and legislation that is purportedly aimed at holding big tech to account. In the name of protecting children. In the name of illuminating the crimes done in the dark. Ironically couching a move that would drastically expand the capabilities of authoritarian social control and corporate and government surveillance in benevolent terms, under the ironic umbrella of accountability.

Put another way, far from addressing the core problem, many of these proposals work to expand the surveillance practices of these companies to governments and NGOs at a time when our muscle to fight them is significantly atrophied.

So, what do we do? Most importantly, we need to refuse the framing we're given.

We need to reject the false binary–refusing *both* the tactics and narratives of the 1990s crypto wars, *and* the current trend of surveillance wine packaged in accountability bottles. And we need to recognize the role that AI hype is playing in further entrenching the tech industry's invasion of privacy, and incorporate this into our strategies.

We do not want to become nannies and overseers of these same companies, leaving their concentration and surveillance practices intact. And we cannot frame encryption as our goal–rather than a tool to achieve our goal, while failing to recognize and critique the commercial business models that have made encryption, left to the discretion of a handful of companies, so ineffective at securing meaningful privacy for people.

This means, in my view, that we must broaden our aperture, and refocus on what we're fighting for.

We want e2ee. But we also recognize that e2ee is not going to deploy itself, and that the business incentives in place currently do not allow for the kind of broad privacy protections I believe we need.

To atone for the sins of the 90s, and the path that got us here, we must have the dignity to refuse the options we're being given and to instead demand meaningful privacy. We want not only the right to deploy e2ee and privacy-preserving tech, but the power to make determinations about how, and for whom, our computational infrastructures work.

This is the path to privacy, and to actual tech accountability. And we should accept nothing less.

THANK YOU!

Selected sources

- *Dark Matters: On the Surveillance of Blackness*,
  Simone Browne.
  https://www.dukeupress.edu/dark-matters
- *Profit over Privacy: How Surveillance Advertising Conquered the Internet*,
  Matthew Crain.
  https://www.upress.umn.edu/book-division/books/profit-over-privacy
- *Political Manipulation and Internet Advertising Infrastructure*,
  Matthew Crain and Anthony Nadler.
  https://doi.org/10.5325/jinfopoli.9.2019.0370
- *New Directions in Cryptography*,
  Whitfield Diffie and Martin E. Hellman.
  https://www-ee.stanford.edu/~hellman/publications/24.pdf
- *Atari Democrats*,
  Lily Geismer.
  https://jacobin.com/2016/02/geismer-democratic-party-atari-tech-silicon-valley-mondale
- *Luxury Surveillance: People pay a premium for tracking technologies that get imposed unwillingly on others*,
  Chris Gilliard and David Golumbia.
  https://reallifemag.com/luxury-surveillance/
- *Digital Redlining, Access, and Privacy*,
  Chris Gilliard and Hugh Culik.
  https://www.commonsense.org/education/articles/digital-redlining-access-and-privacy
- *We lost the war: welcome to the world of tomorrow*,
  Rop Gonggrijp and Frank Rieger.
  https://media.ccc.de/v/22C3-920-en-we_lost_the_war
- *Crypto and empire: the contradictions of counter-surveillance advocacy*,
  Seda Gürses, Arun Kundnani, Joris Van Hoboken.
  https://doi.org/10.1177/0163443716643006
- *A history of crypto-discourse: encryption as a site of struggles to define internet freedom*,
  Z. Isadora Hellegren.
  https://doi.org/10.1080/24701475.2017.1387466
- *The Framework for Global Electronic Commerce: A Policy Perspective*,
  Ira C. Magaziner, Senior Advisor to the President for Policy Development,

Interviewed on 24 November 1997 by Ann Grier Cutter and Len A. Costa for the Journal of International Affairs.
https://www.jstor.org/stable/24357514

- *Cryptography as information control*,
Sarah Myers West.
https://doi.org/10.1177/03063127221078314
- *Renegade Infrastructures: Commerce and Policy in the Crypto Wars 1.0*,
Sarah Myers West.
https://spir.aoir.org/ojs/index.php/spir/article/view/13525/11470
- *The Privacy Paradox: Privacy, Surveillance, and Encryption*,
Karina Rider.
http://hdl.handle.net/1773/37248
- *The Privacy Paradox: how market privacy facilitates government surveillance*,
Karina Rider.
https://doi.org/10.1080/1369118X.2017.1314531
- *Centering Race in Analyses and Practices of Countersurveillance Advocacy: Mythologies of the Racialized Other in the Crypto Wars*,
Karina Rider and S. L. Revoy.
https://www.taylorfrancis.com/chapters/edit/10.4324/9781003173335-2/centering-race-analyses-practices-countersurveillance-advocacy-karina-rider-revoy
- *Computational Power and AI*,
Jai Vipra and Sarah Myers West.
https://ainowinstitute.org/publication/policy/compute-and-ai
- *The Steep Cost of Capture*,
Meredith Whittaker.
https://doi.org/10.1145/3488666
- *The Origin and Early History of the Computer Security Software Products Industry*,
Jeffrey R. Yost.
https://ieeexplore.ieee.org/document/7116464
- *The Framework for Global Electronic Commerce*,
The Clinton Whitehouse.
https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html
- *Encryption and the 'Going Dark' Debate*,
Congressional Research Service, Updated January 25, 2017.
https://crsreports.congress.gov/product/pdf/R/R44481
- *Going Dark, Going Forward: A Primer on the Encryption Debate*,
House Homeland Security Committee Majority Staff Report, June 2016.
https://irp.fas.org/congress/2016_rpt/hsc-encrypt.pdf