



CARR-RYAN CENTER FOR HUMAN RIGHTS  
HARVARD KENNEDY SCHOOL

# Putting People Power into US Privacy Law

Learning from the Past to  
Light the Path to True Privacy  
Protection to Advance Rights  
and Democracy in the Age of  
Artificial Intelligence

**Nicole A. Ozer**

---

Carr-Ryan Center  
Discussion Paper

## **Putting People Power into US Privacy Law:**

Learning from the Past to Light the Path to True Privacy  
Protection to Advance Rights and Democracy in the Age of  
Artificial Intelligence

Carr-Ryan Center for Human Rights  
Harvard Kennedy School, Harvard University  
November 6, 2025 | Issue 2025-08  
Publication design by Kyle Faneuff

### **Nicole A. Ozer**

2024-2025 Technology & Human Rights Fellow at the Carr-Ryan Center at the  
Harvard Kennedy School and the Founding Director of the Technology and Civil  
Liberties Program at the ACLU of Northern California

The views expressed in the Carr-Ryan Center Discussion Paper Series are those of the author(s) and do not necessarily reflect those of the John F. Kennedy School of Government or of Harvard University. Carr-Ryan Center Discussion Papers have not undergone formal review and approval. Such papers are included in this series to elicit feedback and to encourage debate on important public policy challenges. Copyright belongs to the author(s).  
These papers may be downloaded for personal use only.



## ABSTRACT

With the current political climate and advances in artificial intelligence (AI), the stakes are higher than ever to advance new laws that make technology work for the people and promote access, equity, and justice in the digital age. When we were last at a similar historical crossroads in the early 1970s—at the cusp of massive technological change with the rise of computerization and fights for the future of this country raging across movement issues—the people of California passed the constitutional right to privacy. It is the last truly comprehensive privacy law passed in the United States. This modern right to privacy, enacted in 1972, addresses both autonomy privacy and informational privacy and protects against privacy invasions by both government and business. At its core is an allocation of power to the people to control how technological advances can invade private lives and undermine fundamental rights. But, by the mid-1970s, political energy for similar robust substantive privacy protections that limited information collection, use, and disclosure had been undermined. United States privacy protections had been pummeled into weak procedural due process frameworks, like notice and choice, that have now occupied the privacy field for decades. It is urgent to explore what we can learn from history and interrogate current US privacy law and movement power to light a path to defend existing protections and enact stronger privacy laws that can properly support rights and democracy in the AI age.

## I. INTRODUCTION

People and democracy are paying the price for a United States vision of privacy law that has been clouded for more than 50 years by powerful efforts intended to utilize new technology to perpetuate political, economic, and social power structures, not support greater access, equity, and justice. The social justice community lost the fight for robust, substantive privacy law in the mid-1970s and has never been able to rebuild the power necessary to get privacy law back on track.

The year 1972 is a pivotal year in the trajectory of US privacy law. There was support in the late 1960s and early 1970s, at the dawn of the modern computer age, to push robust substantive privacy protections and be able to channel how personal information was collected and used, and how advances in technology impacted people and democracy. The California constitutional right to privacy was enacted in November 1972 and the federal HEW Committee,<sup>1</sup> which convened in April 1972, grappled with power and how to protect people in the modern digital age. But the 1970s ended with no comprehensive federal privacy law and the entrenchment of a national privacy narrative focused on weak procedural safeguards that ignored power and accommodated business profit and government surveillance. US privacy law has now been locked in this five-decades long experiment to rely on process safeguards to counterbalance the new powers of computerization. It has been like bringing a pocketknife to the fight, when the other side has a fully loaded tank. Now Big Tech is recycling the same playbook to attempt to eviscerate existing local and state law protections, and prevent any meaningful regulation for the mass technological advancements of artificial intelligence.

The costs of current United States' privacy law (or lack thereof) of the last 50 years have already been incredibly high. Technology is used by the government to fuel immigration deportation, racist systems of policing, and track activists. The corporate sector is rife with surveillance business models and biased algorithms that are allowed to prioritize profit over people's lives, health, and safety and to externalize costs to people and democracy. If it was not already abundantly clear that how technology is built and used has immense power to control our daily lives, manipulate our system of governance, and be a dire threat to democracy and rights, the Trump administration's recent political actions have made these truths fully evident.

While there has been a consistent march of public concern about privacy and technology issues since the 1970s,<sup>2</sup> the United States has no comprehensive federal privacy law and most current privacy laws lack substantive provisions that limit or prevent information collection. On the government surveillance side, federal privacy laws that supplement Fourth Amendment constitutional rights are ancient. The Privacy Act of 1974,<sup>2</sup> which is being relied on to fight the so-called Department of Government Efficiency (DOGE),<sup>3</sup> was inadequate even when it was enacted 50 years ago. Its "soft spots,"<sup>4</sup> in the form of loopholes, like its routine use exception and weaknesses in enforcement provisions, have become particularly

salient with recent Trump administration actions. "The federal privacy law that is supposed to limit government surveillance of electronic communications, the Electronic Communications Privacy Act (ECPA),<sup>6</sup> has not been meaningfully updated since 1986, when cell phones were the size of bricks and the World Wide Web did not even exist.<sup>7</sup> The events of September 11 derailed efforts to strengthen privacy laws for the digital age<sup>8</sup> and undermined existing protections like the Foreign Intelligence Surveillance Act (FISA).<sup>9</sup> Important state laws, like the California Electronic Communications Privacy Act (CalECPA), have filled some gaps.<sup>10</sup> But as technology has advanced, government surveillance has become ever more pervasive and powerful.<sup>11</sup>

**"The social justice community lost the fight for robust, substantive privacy law in the mid-1970s and has never been able to rebuild the power necessary to get privacy law back on track."**

On the consumer side, sectoral laws on the federal-level, like the Fair Credit Reporting Act (FCRA),<sup>12</sup> the 1996 Health Insurance Portability and Accountability Act (HIPAA),<sup>13</sup> and many laws on the state-level, like the California Consumer Privacy Act (CCPA),<sup>14</sup> have few substantive limitations on information collection. The majority of privacy laws enacted in the digital age are largely based on a weak procedural notice and choice framework. These "wet napkin privacy laws"<sup>15</sup> put an impossible burden on individuals to try to eke out some privacy.<sup>16</sup> They fail to protect people, especially people who are not already in the top echelons of power and privilege.<sup>17</sup> Studies of the psychology of compliance have long demonstrated that people vastly underestimate how hard it is to say no.<sup>18</sup> Further, whether people feel they really have a choice connects to privilege<sup>19</sup> and many current privacy laws lack an adequate focus on the experiences of marginalized populations, such as the compounding vulnerabilities of excessive and discriminatory surveillance and targeted exclusion experienced by African Americans.<sup>20</sup> Community members describe ever-present power dynamics and the experience of "being forced to engage with intrusive and unsecure data-driven systems because of their membership in groups that have historically faced exploitation, discrimination, predation, and other forms of structural violence..."<sup>21</sup> The notice and consent paradigm in the digital space, replete with check boxes galore that are usually defaulted to "agree" by businesses, most often translates to accommodating, rather than preventing privacy-invasive practices.

The current political climate and pace of technological advances with AI makes it even more critical to understand the past and the

“  
People and democracy are paying the price for a United States vision of privacy law that has been clouded for more than 50 years by powerful efforts intended to utilize new technology to perpetuate political, economic, and social power structures, not support greater access, equity, and justice.

context of US privacy law, and how to work strategically on the local, state, national, and international-level to pass substantive privacy law that actually prevents privacy intrusions and protects people. This is the time to focus on further building the social movement power necessary to make AI and other emerging technology work for the people.

When we were last at a similar historical crossroads in the early 1970s—at the cusp of massive technological change with the rise of computerization and with fights for the future of this country raging across movement issues—the people of California passed the constitutional right to privacy.<sup>22</sup> Its “moving force” was a focused privacy concern “relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society.”<sup>23</sup> At the core of the California constitutional right to privacy is an allocation of power. In 1972, the California legislature and the people of California recognized that the combination of government, corporate, and technological power was going to stack the decks against people’s rights. The Privacy Amendment’s legislative history, both as it initially moved through the California legislature, and then the ballot argument itself, makes clear that the California constitutional right to privacy was passed to give people the power to guide how privacy questions were resolved in the digital age. It was intended to robustly limit how technological advances and the surveillance ecosystem of both business and government actions could invade private lives and undermine fundamental rights.<sup>24</sup>



Altair 8800, the first commercially successful personal computers.  
Image: Wikipedia Commons - Tim Colegrove

The 1972 California constitutional right to privacy is the last truly comprehensive privacy law to pass in the United States. It is the last law enacted to protect both autonomy privacy and informational privacy, to safeguard against both government and business intrusions, and not be limited to a single type of privacy issue or sector.<sup>25</sup> How can this be? Why have no other truly comprehensive privacy laws ever been enacted in the United States? As technology has advanced exponentially and people now live digital lives, why have strong substantive laws in the United States that limit how technology can be used to invade people’s personal lives largely languished in the digital dark ages for more than 50 years? How did privacy law lose its path forward? And how can the United States get back on the path to true privacy protection?

Part I of this article uses archival research and oral history to demonstrate that bold actions related to channeling the power of technology and addressing information collection, retention, and use of information are not new ideas. In fact, these are original ideas of the 1960s and early 1970s at the dawn of the modern computer age. An understanding of the intersections of information collection and use, power and democracy, and the need to take decisive action to account for the advances of computerization pre-date the far weaker notice and choice frameworks that have now occupied the privacy law field for decades. In the late 1960s and early 1970s, there was significant public discussion about the need for many of the public and private sector privacy interventions that are being discussed today.

Part II explores what happened to privacy law starting in the mid-1970s and how law in the United States was pummeled from an early trajectory of providing real power to the people into weak notice and choice frameworks when intersectional movement power was undermined and political opportunity paths were blocked by political, social, and economic factors. The current political climate, the mass undermining of democratic institutions, blatant attacks on the rule of law by the Trump administration, and efforts to undermine existing local and state laws for the AI age, make it all the more urgent to understand the history of how we ended up here and the lessons that that can be learned about how to build intersectional power to advance enduring change.

The article concludes by lighting a potential path for how to make it politically possible to pass new robust privacy law. It discusses steps that the public interest community should take to build the social movement power and create the climate to be able to defend existing protections and be in a position to enact strong privacy law that makes technology work for the people and advance access, equity, and justice in the AI age.

### **PART I: ROBUST SUBSTANTIVE PRIVACY LAW IDEAS AND PLANS FOR ACTION AT THE DAWN OF THE COMPUTER AGE**

By the late 1960s, the impact of computerization had entered the US legal, political, and public consciousness. It was already well understood that bold steps were needed to address the new powers of technology and how it affected people, communities, and movements. The potential privacy interventions discussed during that time included substantive laws and policies that prohibited what personal information could be collected and how it could be used.

As early as the spring of 1967, there were important discussions about technology and privacy issues at both the state- and federal-level,<sup>26</sup> including “grave concern[s]” with a proposed National Data Center<sup>27</sup> and the need to take prompt and robust action to address the advances of technology and its impact on rights and democratic society.<sup>28</sup> At a 1967 conference hosted by the ACLU of Northern California, United States Supreme Court Justice William O. Douglas spoke about “Computerized Man” and Alan Westin<sup>29</sup> discussed that without meaningful interventions in the United States, there was a “menacing prospect” that “authorities in government and

private organizations will convince the public that new surveillance methods are necessary in order to build a stronger democratic society.” Westin feared that “[i]ntrusions would be made in the name of social values,” with the right to privacy never “openly challenged,” but “found to be less important ‘in this particular area’ than society’s need for disclosure or surveillance.”<sup>30</sup>

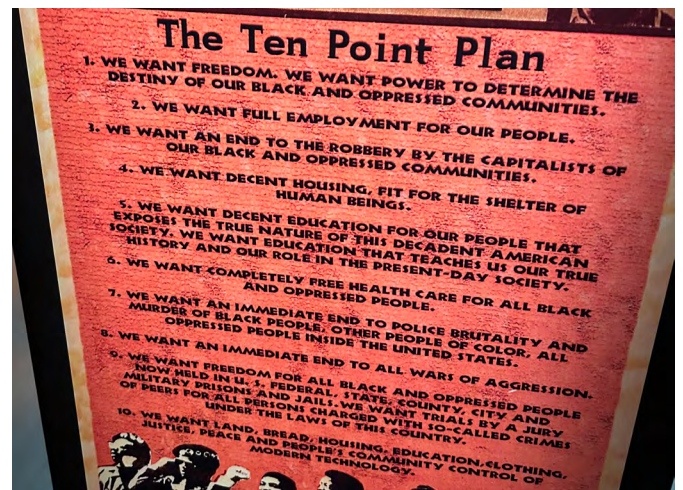
By 1968, deeper conversations were happening about the intersection of both government surveillance and business practices. The ACLU Executive Director, John Pemberton, speaking at a symposium on Computers, Databanks, and Individual Privacy, highlighted the need to address issues related to both government and business information collection, use, and disclosure. He noted that we can no longer rely on corporate and government inefficiency to protect our privacy and protect us from dangers. Rather, the “presence of new techniques in data gathering and dissemination warrants regulation of private and government data gathering and dissemination as well as government data banks.”<sup>31</sup> He cautioned that dangers will persist until “we take steps to discriminate about the kinds of information that are gathered and stored”<sup>32</sup> and would “have to be dealt with by legislation” and could not be left to the slow pace of judicial decisions.<sup>33</sup>

Arthur Miller,<sup>34</sup> presenting at the same symposium, asserted that “we need a total and complete revamping of our legislative approach to informational privacy” and one that includes “all phases of the regulations regarding governmental and nongovernmental information gathering, processing, manipulating, and storing.” He reinforced the need to take into account “the massive shifts in information technology and the new threats they pose.”<sup>35</sup> Miller stressed, “[f]irst and foremost, we need controls on input”<sup>36</sup> and he emphasized that we must “regulate the character of information that private agencies can collect.”<sup>37</sup> Further, Miller predicted that “there is so much information that we could collect, and in time it will be economical to collect it in view of the fact that computer costs are constantly declining. But in the case of certain types of sensitive data, we just shouldn’t collect it—period!”<sup>38</sup> Miller also highlighted the “proliferation of non-federal data systems” including those in the insurance and credit fields<sup>39</sup> and cautioned that data centers would present “really significant problems of computer-based information and privacy in the future.”<sup>40</sup>

**" Technology and privacy were also intersecting with race and class in this era in complex ways and there was also elite support for privacy."**

#### A. Intersectional Movements Supported Calls for Robust Privacy Law in the Late 1960s

There was support from both social movement actors and elite communities for robust privacy law during the late 1960s and early 1970s. Intersectional liberation movements of this important time in history understood technology’s power to support or undermine their efforts and democracy as a whole. Many activists understood that they were being heavily surveilled, including by new technologies like electronic wiretapping, later confirmed by the 1971 public exposure of the FBI COINTELPRO Program.<sup>41</sup> The government’s surveillance targets included Martin Luther King Jr.,<sup>42</sup> the Black Panthers, the women’s movement, LGBTQ leaders, Native American leaders, antiwar groups, and many other organizations and activists. Many of these movement leaders and activists personally understood how advances in technology could exacerbate threats to movement work and personal safety. In Dr. King’s final public sermon before his assassination, he highlighted both the “technological revolution with the impact of automation and cybernation” and “the human rights revolution with the freedom explosion that is taking place all over the world.”<sup>43</sup> The Black Panther Party<sup>44</sup> was one of the most heavily surveilled activist organizations at the time<sup>45</sup> and made direct connections between technology and the fight for liberation. The Black Panther Party’s Ten Point Plan of ideals included an explicit provision about “people’s community control of modern technology” in addition to “land, bread, housing, education, clothing, justice, peace.”<sup>46</sup>



A poster of the Black Panther Party’s “Ten Point Plan,” taken at the National Museum of African American History and Culture.

Technology and privacy were also intersecting with race and class in this era in complex ways and there was also elite support for privacy. As economist Richard Ruggles explained in 1968, the “present concern with the right to privacy” had two different aspects—one being the fight for civil rights and the other being the libertarian concerns of the wealthy.<sup>47</sup> First, the increased concern about civil rights made it “glaringly evident that in the past the normal process of operation of the society has violated the privacy of many individuals.”<sup>48</sup> Second, the rich “resent[ed]” reporting information to the government about their financial dealings, safety standards, fair employment practices and more.<sup>49</sup> They felt that it was “an invasion of privacy” to not be “free” to run affairs as they saw fit without government interference.<sup>50</sup>

## B. Political Energy for Substantive Privacy Laws

By the early 1970s, there was both state and national political energy to address computerization and privacy issues. By the winter of 1971, Senator Sam Ervin was chairing a series of eleven Congressional hearings on “Federal Data Banks, Computers, and the Bill of Rights.”<sup>51</sup> Senator Ervin reflected that “Americans in every walk of life are concerned about the growth of government and private records on individuals.”<sup>52</sup> In fact, by 1971, about one-third of the American public felt that “invasions of privacy” were a matter of concern and 83% of college-age respondents agreed with the statement “[p]eople’s privacy is being destroyed.”<sup>53</sup> Senator Ervin contended that, “[i]f Americans can harness computers to get to the moon, surely we can harness them to protect our liberty.”<sup>54</sup>

**"About one-third of the American public felt that 'invasions of privacy' were a matter of concern."**

The Congressional hearings brought together expert testimony on privacy concerns and the need for new protections. Burt Neuborne, in a statement on behalf of the ACLU, highlighted how innovation in computer technology had eviscerated the practical deterrents of cost and storage space that checked the growth of national dossiers. People now lived “imprisoned in a web of imperishable data” and we now faced the dilemma of how to control the “technological Frankenssteins we have created.”<sup>55</sup>

Gerhard Casper<sup>56</sup> highlighted both the importance of remedies against both the government and private parties and the need to understand the connection between privacy and First Amendment protections.<sup>57</sup> Casper noted how the development of computers had changed the landscape and “the threats posed by unlimited data storage and data recall.” He reasoned those remedies “both as against the government and as against as equally inescapable private institutions” should be “developed with an understanding that the First Amendment as correlated with the Fourth demands far-reaching protection of personal privacy, with the burden of justifying intrusions clearly placed upon the intruder. The ‘central meaning’ of the First Amendment requires no less.”<sup>58</sup>

Arthur Miller discussed the “spiraling pattern of data collection in this country.”<sup>59</sup> That “whether someone knows it or not” he is “likely to leave distinctive electronic tracks in the memory of a computer that can tell a great deal about his activities, his movements, his habits and associations.”<sup>60</sup> He discussed the intersections between privacy and chilling of free association and expression. He also highlighted stunningly similar issues to what we are still grappling with today, particularly with current debates on AI, including how the power of data integration changes the context of privacy issues.<sup>61</sup>

Testimony was also submitted by Computer People for Peace (CPP), a grassroots organization of people who worked in the early years of the computer industry.<sup>62</sup> CPP noted that, as “computer technicians,” they felt they had the “responsibility to inform the public of misuses and dangerous applications of computers.”<sup>63</sup> CPP articulated needed protections that put the burden on the data collector rather than the individual, robust limitations on collection, use, and disclosure, and transparency rights paired with the right to data deletion. It also recommended limits on what was considered public information, prohibiting pay for service with privacy/personal information, and requiring anonymization.<sup>64</sup>

During the same time period of the Congressional hearings, the widespread surveillance by the FBI’s COINTELPRO program was first publicly exposed.<sup>65</sup> Public awareness of privacy issues and political energy undergirded the passage of the California constitutional right to privacy in 1972.



California State Capitol, Sacramento. Image: Wikimedia Commons- Henri Sivonen

## **PART II: WHY AND HOW DID PRIVACY LAW GO SIDEWAYS AND MOVE FROM POWER TO THE PEOPLE TO PROTECTING PROFIT AND GOVERNMENT SURVEILLANCE?**

The 1972 California constitutional right to privacy was solidly about power to the people, an effort motivated by the desire to protect people in the digital age and not accommodate government surveillance or business profit at the expense of people’s rights and safety.<sup>66</sup> It was purpose-built to “meet the new dangers”<sup>67</sup> of the “technological revolution”<sup>68</sup> and address the rising surveillance ecosystem.<sup>69</sup> It guaranteed an affirmative right to privacy<sup>70</sup> intended to “prevent[] government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us.” Further, it created a constitutional baseline that privacy was a “fundamental and compelling interest” and “should be abridged only when there is compelling public need.”<sup>71</sup> California voters passed the constitutional right to privacy in 1972 by a substantial majority, with 62.9% of the vote.<sup>72</sup> With its passage, California became the first constitution in the nation—either federal or state—to include an explicit right to privacy<sup>73</sup> that applied to both government and private parties, and it put California on the vanguard of protecting both informational privacy and autonomy privacy in the digital age.<sup>74</sup>

But the California constitutional language of inalienable and fundamental privacy rights and power to the people to prevent information collection and use by both government and business was never replicated on the federal-level. The California constitutional right to privacy is the last truly comprehensive privacy law passed in the United States. By 1973, narrative frames like “safeguards” that “balanced” the “needs” of computerization while managing risk to individual liberties had taken hold.<sup>75</sup> The burden on the privacy invader to demonstrate compelling interest, as was required by the California constitutional right to privacy, morphed into a national narrative about far more nebulous due process safeguards that put a heavy burden on the individual to try to suss out what was happening to their information and attempt to ameliorate the risks. The primary driver in US privacy law became accommodating information collection, government surveillance power, and potential business profit—not people power.

The year 1972 was a turning point. It is both a high-water mark for modern privacy law in the United States with the passage of California’s constitutional right to privacy and also the year where there is a visible turn away from comprehensive privacy laws that directly addressed the power of new technology and towards procedural due process that would accommodate government surveillance and surveillance business models. Three W’s: (1) the War on Drugs; (2) Alan Westin—the author of 1972’s *Databanks in a Free Society*;<sup>76</sup> and (3) Willis H. Ware, chair of the HEW Committee<sup>77</sup> and vice-chair of the Privacy Protection Study Commission (PPSC),<sup>78</sup> were significant factors in shifting political energy away from supporting substantive privacy law limits related to information collection, use, and disclosure, and had a profound effect on power and democracy in the digital age.

**"By 1972, on the federal-level, conservative Southern politicians had reframed their desired backlash to civil rights as a law and order agenda."**

A. The First “W” – War on Drugs and Impact on Privacy Law in the Digital Age

When the California constitutional right to privacy was passed in 1972, interest in comprehensive privacy law in California still had the tail end of support in the state by both social movement groups<sup>79</sup> and elite financial interests.<sup>80</sup> But diverse support for privacy efforts more broadly was already very much on the rocks due to larger political and social contexts in the country. As the civil rights movement increasingly turned its attention to economic justice, changes that could challenge the economic dominance and position of elites, elite alliances moved into a position of defense, backlash, and retrenchment.<sup>81</sup> By 1972, on the

federal-level, conservative Southern politicians had reframed their desired backlash to civil rights as a law and order agenda.<sup>82</sup> They had leveraged fear of crime and racial uprisings, particularly after the assassination of Dr. Martin Luther King Jr.,<sup>83</sup> to build support for punitive policies while avoiding overtly racist language.<sup>84</sup> Conservatives had been able to push through the 1968 Safe Streets Act<sup>85</sup> despite President Johnson’s concerns.<sup>86</sup> The new law marked a sharp turn in federal crime policy,<sup>87</sup> fueled increased policing and surveillance,<sup>88</sup> and diverted activist energy from advancing privacy protections to fighting new surveillance laws.<sup>89</sup> Nixon further intensified the assault with the “War on Drugs” when he was elected President in 1968. Nixon’s advisor John Ehrlichman has admitted that the War on Drugs was “really all about” an assault on Black and Brown people, activists, and social justice movements organizing for change.<sup>90</sup>

The federal courts were also an active front for efforts to stifle privacy rights and further the War on Drugs playbook. While technology was continuing to advance, and government at all levels had more tools at its disposal for surveillance and searches, Fourth Amendment law was generally being undermined. When the United States Supreme Court decided the seminal stop and frisk case, *Terry v. Ohio*, in 1968, “the era of Black Power was at its zenith as a social movement.”<sup>91</sup> But after *Terry*, there was a deep erosion of privacy rights,<sup>92</sup> further powering racially biased policing and massively disproportionate imprisonment and related disenfranchisement of incarcerated Black and Brown community members.<sup>93</sup>



The Earl Warren Building and Courthouse home to the Supreme Court of California. Image: Wikimedia Commons-Coolcaesar

The California Supreme Court also became increasingly conservative through the War on Drugs years and these changes had a profound impact on the California constitutional right to privacy. Most notably, three Democratically appointed California Supreme Court Justices lost their 1986 retention elections (the only Justices ever ousted by voters in nearly 100 years of California retention elections),<sup>94</sup> after being targeted by a multi-million dollar campaign that they were “soft on crime” and too often voted to overturn death sentences.<sup>95</sup> After these election losses, Republican Governor Deukmejian appointed three new Associate Justices, creating the first conservative majority on the California Supreme Court since the Great Depression.<sup>96</sup> It was this new conservative majority California Supreme Court, which after nearly 20 years

of existing jurisprudence on the California constitutional right to privacy,<sup>97</sup> decided the 1994 *Hill v. NCAA* case about drug testing in the private context. In the *Hill* case, the majority deviated from the language and intent of the California constitutional right to privacy. The majority decision subverted the burden and required plaintiffs to demonstrate multiple elements for their claims to go forward. The majority decision also undermined a consistent compelling interest standard for privacy claims.<sup>98</sup> The new *Hill* test for constitutional privacy claims made it very difficult for people to actually obtain their fundamental right to privacy going forward.<sup>99</sup> Justice Stanley Mosk, a veteran Justice on the California Supreme Court, issued a blistering dissent. He chastised his fellow Justices for abrogating an “express” right where “nothing is left to implication” and disregarding the “people’s constitutional policy declaring a right to privacy.”<sup>100</sup> Justice Mosk concluded his dissent in *Hill* by connecting the dots on the War on Drugs narrative and contended, “I think it obvious that this justification is unacceptable.”<sup>101</sup>

### B. The Second “W” – Alan Westin and Influence on Privacy Law in the Digital Age

Alan Westin, described by some as the father of modern privacy law,<sup>102</sup> is another influential force in shifting attention away from supporting substantive limits related to collection, use, and disclosure, and towards a far weaker guardrail framework that included notice and consent as a significant lever. In 1972, Westin published *Databanks in a Free Society: Computers, Recordkeeping, and Privacy*. In *Databanks*, Westin promoted a “balanced” framework that accepted widespread information collection and offered procedural safeguards rather than substantive limits.<sup>103</sup> Though Westin had previously warned in 1967 against compromising privacy in the name of social good, by 1972, Westin contended that there was a “need for data.”<sup>104</sup> The report’s foreword, written by the president of the Foundation which funded the work, asserted that the current debate was a “fundamental conflict between the individuals’ right to privacy and society’s right to know”<sup>105</sup> and that “intelligent formulation of public policy” and “monitoring social change demands the collection and analysis” of data.<sup>106</sup>

**"Westin promoted a 'balanced' framework that accepted widespread information collection and offered procedural safeguards rather than substantive limits."**

Westin also largely rejected public fears about computerization.<sup>107</sup> He disregarded the interconnectedness and power dynamics that civil rights leaders articulated at the time between

computerization and liberation,<sup>108</sup> and instead, attributed concern to misunderstanding.<sup>109</sup> The foreword of *Databanks* also contended that “there has been, and still is, much confused thinking about databanks in our society” and characterized those speaking out about privacy issues as “doomsday prophets crying out about national data centers...anecdotes about credit-card society...and plenty of wild and misinformed testimony at congressional hearings.”<sup>110</sup> In fact, many of the speakers at the Congressional hearings were constitutional law and civil rights experts and technologists who presciently described what was at stake (and it is striking just how much of this testimony could now be utilized again word-for-word today at an AI hearing).

Westin’s work did face some critique at the time, including from Mary Kay Kane,<sup>111</sup> who argued that, despite its impressive credentials, *Databanks* in a Free Society suffered from inconsistencies and an overly trusting stance toward data handlers.<sup>112</sup> James Rule and others criticized Westin’s reliance on legal-procedural protections, warning that such measures might legitimize intrusive practices and obscure deeper power imbalances created by surveillance systems.<sup>113</sup> While critics contended Westin’s framework lacked the rigor to address growing systemic risks and that his misplaced optimism could lead to far-reaching consequences,<sup>114</sup> Westin’s ideas strongly influenced national privacy policy moving forward. His work helped sideline more robust protections and entrench the notice and consent model despite growing structural concerns about surveillance and organizational power.

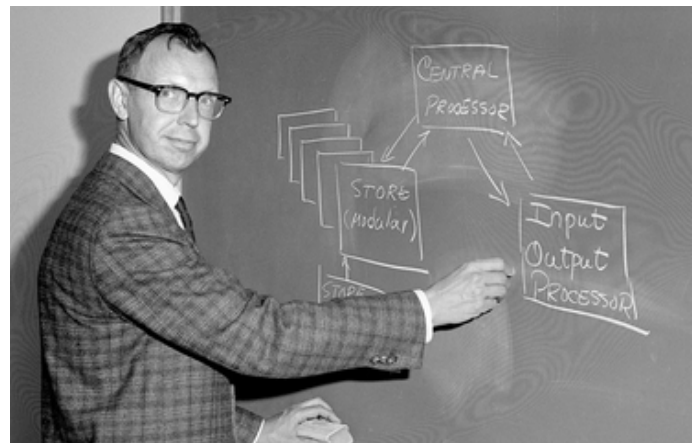


Photo of Willis Howard Ware. Image: Rand Corporation

### C. The Third “W” – Willis Ware and Impact on Privacy Law

Willis Ware, an engineer who worked for the RAND Corporation, played another significant role in the trajectory of privacy law. Ware was both the chair of the HEW Committee and a vice-chair of the PPSC,<sup>115</sup> the two primary federal committees to assess privacy risks and develop recommendations for US privacy law in the 1970s.

The HEW Committee met between April 1972 and May 1973 and developed the 1973 *Records, Computers and the Rights of Citizens*, Report of the Secretary’s Advisory Committee on Automated Personal Data Systems (HEW Report).<sup>116</sup> Its 30 members represented a wide diversity of backgrounds and sectors<sup>117</sup> and the HEW Committee was given a broad mandate<sup>118</sup> to respond to “growing concern about the

harmful consequences that may result from uncontrolled application of computer and telecommunications technology to the collection,<sup>119</sup> storage, and use of data about individual citizens” in both the “public and private sectors....”<sup>120</sup>

The diverse HEW Committee recognized the dangers of privacy incursions by both government and business and grappled with the intersections of privacy, power, politics, and lived experience in the face of emerging computerization.<sup>121</sup> Internal discussions reflected a strong awareness of the coercive dynamics inherent in information collection practices—particularly for low-income individuals—and the unequal distribution of privacy based on socioeconomic status. Members, like Arthur Miller, discussed how power and socioeconomics affected who can afford to negotiate to protect their privacy<sup>122</sup> and how that should “raise the question to what degree should the system extract that information, knowing, first, in some amorphous, constitutional sense the cost of privacy is being unequally distributed across the nation.”<sup>123</sup> External presenters underscored how information asymmetries reinforced institutional power and that the “possession of all this information increases the power...to control and manipulate, and this accretion of power to institutions caused by the accumulation of information has not been accompanied by any compensating accretion of power to individuals.”<sup>124</sup> There was advocacy from various members for bolder constraints, like limiting information collection,<sup>125</sup> a recognition that existing norms and computer systems entrenched subtle policy choices,<sup>126</sup> and concerns raised that the Fair Credit Reporting Act (FCRA) notice and disclosure model was already failing to effectively protect privacy.<sup>127</sup> But, the Committee still settled on more modest due process recommendations aimed at preventing further harms that did not fundamentally address power or challenge the “collect it all” ethos.<sup>128</sup>

The HEW Committee’s recommendation of the Fair Information Principles (FIPS),<sup>129</sup> which is now often seen as its central contribution to the development of privacy law,<sup>130</sup> utilized a safeguards approach that largely accommodated existing databases by focusing on ensuring overall transparency and fairness, and generally not limiting information collection.<sup>131</sup> The HEW Committee was clear-eyed that “this formulation does not provide the basis for determining a priori which data should or may be recorded and used, or why, and when.”<sup>132</sup> Miller recognized that the procedural safeguards would not restore “equality in power between the individual and the institution,” but hoped that they could be a “prophylactic structure so that whatever there is today, it doesn’t grow tomorrow” by constraining “the ways in which that institution can use the data bank.”<sup>133</sup>

The lack of final meeting transcripts makes it unclear why the Committee ultimately embraced a due process model. Though Ware, the HEW chair, reflected that FIPS was “a reasonable way to go.” He understood his goal for the Committee to be “to steer toward a sense of reality, toward a set of solutions that made sense, could be accepted by the real world, could be effective in the real world.”<sup>134</sup> What is clear is that the HEW Committee intended that FIPS comprehensively apply to both government and business practices and ensure “minimum standards”<sup>135</sup> that would be enforceable “legal protection against

unfair information practice.”<sup>136</sup> But the FIPS were never implemented as intended.

The Privacy Act of 1974, which was influenced by the HEW Report and enacted in the wake of the Watergate scandal, did not create a comprehensive privacy framework for both government and the private sector as the HEW Committee recommended.<sup>137</sup> Rather, a “compromise” took place between Congress and the Ford White House to obtain passage of the Privacy Act.<sup>138</sup> The deal that was struck established procedural safeguards for government agencies,<sup>139</sup> but kicked the can on any private-sector regulation to a future federal commission.<sup>140</sup> This later commission, the PPSC, was tasked with evaluating the Privacy Act and considering ways to update and augment it in the future, including any privacy protections for private sector information collection, use, and disclosure.<sup>141</sup> Willis Ware returned again as a major player, this time as the vice-chair of the PPSC. The PPSC inherited the research products and some of the staff from an earlier Ford Presidential privacy task force.<sup>142</sup> Ultimately, the PPSC continued its work under the Carter administration, issued its final report in July 1977 titled *Personal Privacy in an Information Society*,<sup>143</sup> and closed-up shop. The PPSC lacked diverse committee membership—it was only seven members, who were all men, appears to have had no members of color, and was largely comprised of elected officials and individuals related to business.<sup>144</sup> Its recommendations were very industry-oriented and strongly favored notice and self-regulation over individual rights. Most striking is how the PPSC report elevated costs to business as the “most compelling competing interest” and reflected early weaponization of the First Amendment against privacy protections.<sup>145</sup> The PPSC did not recommend any meaningful private-sector privacy protections and any additional progress for privacy reforms stalled out during the Carter administration.<sup>146</sup>

**"It is recognized that consent in privacy is beyond broken, it is a complete fiction."**

The 1970s had started with the passage of constitutional rights to privacy and apparent political momentum for additional privacy change in both the government and consumer context. But the decade ended without comprehensive federal privacy law, a relatively hamstrung Privacy Act that only applied to government agencies, and increasing efforts by elites to realign government actions with global economic interests. Once President Reagan took office in January 1981, there was not only no path forward, but consumer advances in any arena were being actively undermined and the political opportunity for comprehensive privacy law was slammed shut for many years to come.<sup>147</sup>

### PART III: PAVING PATH TO POSSIBLE

The public interest community lost the fight for comprehensive privacy laws that would actually protect people in the digital age by

“  
Now history is replaying.  
Like during debates about  
early computerization in the  
1970s, business interests are  
recycling the same narratives  
about AI and how it will  
be used to benefit ‘all of  
society’ while opposing any  
substantive regulation.global  
economic interests.

## "People who are most impacted need to have an active role in decision-making and there must be AI impact assessments that include evidence-based evaluation of whether the risks outweigh the benefits."

1973. While the 1972 California constitutional right to privacy focused on power and an inalienable right to privacy that could prevent information collection and use by both government and business, an important political opportunity to push for comprehensive US privacy protection was squandered when influential efforts like the HEW Committee focused on procedural safeguards that were already showing their seams, even in 1972.

US privacy law has now been locked for 50 years in a safeguards approach largely reliant on notice and choice that scholars, including Barocas and Nissenbaum,<sup>148</sup> Schwartz,<sup>149</sup> Richards and Hartzog,<sup>150</sup> Solove,<sup>151</sup> Zuboff,<sup>152</sup> and Turow, Lelkes, Draper and Waldman,<sup>153</sup> have derided for its inadequacy. It is recognized that "consent in privacy is beyond broken, it is a complete fiction."<sup>154</sup> The notice and consent regime is plagued with challenges and invites "unwitting and coerced consent."<sup>155</sup> People care about protecting their privacy, but can often be "nudged and manipulated by powerful companies against their actual interests,"<sup>156</sup> with consent "deployed in ways and in contexts to do more harm than good, and in ways that have masked the effects of largely unchecked (and sometimes unconscionable) power."<sup>157</sup>

Now history is replaying. Like during debates about early computerization in the 1970s, business interests are recycling the same narratives about AI and how it will be used to benefit "all of society" while opposing any substantive regulation.<sup>158</sup> Industry lobbyists tout "trustworthy" AI<sup>159</sup> that is limited only by guardrails related to transparency and ineffectual notice and choice frameworks.<sup>160</sup> If technology and democracy is going to work for the people in the AI age, there must be substantive laws that create robust rules of the road for how AI is developed and used, not just weak process safeguards that do nothing to address power structures. There must be multi-level governance, including at the local and state-level, that centers people, not profit.<sup>161</sup> People who are most impacted need to have an active role in decision-making and there must be AI impact assessments that include evidence-based evaluation of whether the risks outweigh the benefits. Further, some uses of AI need to be off the table. AI should never be trusted to make high stakes decisions in our criminal, immigration, and policing systems, including prohibitions on its use for face surveillance and other biometric surveillance systems.

To be in a position to protect existing rights and enact stronger privacy laws, this time of Trump must be used to double down on offense and focus on fostering social movement's core building blocks of relationship, narrative, strategy, action, and structures, and build the power for the technology future that people need and want.<sup>162</sup> Fortunately, there has been considerable progress along the continuum of social movement organization related to issues at the intersection of privacy and technology since I last considered and wrote about this issue in 2012.<sup>163</sup> The face surveillance campaign<sup>164</sup> is just one example of successful work in the last decade that reflects

social movement growth, particularly in developing stronger relationship, strategy, and action. But the public interest community remains particularly weak on narrative and structures that would support a true social movement. Technology has continued to advance, and government and corporations are closely partnered to broaden surveillance powers. It is time to get serious about interrogating ways that the public interest technology community is successfully building power and how it continues to fall short in supporting a true social movement to defend and advance justice in the AI age.



Diverse community coalition press conference at Amazon headquarters pushing back on face surveillance. Image: ACLU of Washington

### A. Growth in Social Movement Building Blocks – Relationship, Strategy, and Action

Public interest technology leaders have made significant progress in the past decade on some of the core building blocks of social movement power, including building relationships, developing integrated advocacy plans across strategy, and translating plans into concrete action. Now is an urgent time to continue to solidify and further augment these advances.

#### 1. Growth in Building and Nurturing Relationships

There has been marked growth in building and nurturing relationships across issue areas and across the local, state, national, and international-level. When I started working on the intersection of technology and public interest law in the early 2000s, there was still very little connective tissue between technology issues and other movement work, and it was a relatively hard sell to engage grassroots organizations on technology issues. Now, most organizations no longer need to be convinced of the interconnection of their work with technology. In spring 2018, when the ACLU of Northern California Technology and Civil Liberties team publicly blew the whistle on Amazon Rekognition, releasing the results of a public records act investigation showing that Amazon was marketing facial recognition

to law enforcement as a tool of mass surveillance,<sup>165</sup> it was possible to quickly mobilize a large coalition of more than 85 diverse racial justice, faith, and civil, human, and immigrants' rights groups on the local, state, national, and international-level to work on a very successful integrated advocacy campaign to stop facial surveillance.<sup>166</sup> There were also existing relationships with academics, and legal and policy work could be informed by important early research<sup>167</sup> and other academic voices.<sup>168</sup> The relationships were sustained and continued to grow through many years of both proactive and defensive work, including pushing major technology companies, including Amazon and Microsoft, to stop selling facial surveillance to law enforcement, the enactment of dozens of local laws prohibiting government use of facial surveillance,<sup>169</sup> and successfully opposing California bills in three consecutive legislative years that would have greenlighted police use of this dangerous surveillance technology.<sup>170</sup>

By 2019, both traditional civil society and digital policy organizations saw a "common, intertwined fate for the future of democracy, human well-being, and essential rights" as well as a recognition of the power of connection and a desire to have support to develop more and new ways to work together.<sup>171</sup> Especially with recent advances in AI, civil society has an even deeper understanding that barriers to freedom and opportunity are now both physical and digital, and social movements must fight for access, equity, and justice on multiple terrains. There are now consistent coalition spaces where diverse organizations meet

to share information, plan strategy, and collaborate on both defense and offense. These include the California Privacy Coalition, a multi-state call that brings together people working on state-level privacy work across the country, and Civil Rights Table working groups, like the Police Surveillance Working Group (PSWG) and the Immigration Surveillance Working Group (ISWG).<sup>172</sup> On the local-level, there is the Bay Area Tech Table (BATT),<sup>173</sup> a model developed in the fall of 2024 to bring together diverse hyper-local organizations from racial justice, policing, economic and housing justice, immigrants' rights, youth justice, digital rights, and more to build a stronger, more connected network to better protect people and advance access, equity, and justice in the technology age. Public interest technology-related clinics and centers at universities around the world, conferences like RightsCon<sup>174</sup> and the Privacy Law Scholars Conference,<sup>175</sup> and international fellowship cohorts<sup>176</sup> play a particularly important role in further developing relationships and fostering collaborative work on emerging issues across regions.

Now is the time to continue to focus on building more and deeper relationships across movement work, connecting work on the local, state, national, and international-level, and nurturing the opportunities for intersectional collaboration. Movement leaders

need to focus in on relationships so that people are willing to move from silos of seeing difference, into solidarity of connection and commonality, and be in a position to actively and consistently work together for change and to defend advances.<sup>177</sup> It is hard to imagine a more important moment than now for the public interest community to stand together in shared interest and purpose to collectively use its power to defend and continue to advance access, equity, and justice in the AI age.

## 2. Growth in Strategizing and Integrated Advocacy

There have also been significant development in the public interest technology space in strategizing, with particular growth in the effective use of integrated advocacy and working both within and between many organizations to channel resources into purposeful plans. Integrated advocacy is a big picture, strategic approach to powering social change that considers and strategically leverages and layers diverse strategies across institutional domains, both inside and outside of formal lawmaking arenas (courts, legislatures, agencies, companies, and communities) and at multiple levels (local, state, federal, and international), to better support long-term social change.<sup>178</sup> The facial surveillance campaign is a strong

example of effective strategizing and integrated advocacy at work, with the campaign powering on all cylinders and using practically every type of integrated advocacy strategy since the movement work started in earnest in

**"It is hard to imagine a more important moment than now for the public interest community to stand together in shared interest and purpose to collectively use its power to defend and continue to advance access, equity, and justice in the AI age."**

2018.<sup>179</sup> The integrated advocacy across legislative work, corporate advocacy, litigation, organizing, communications, and other strategies also reinforced intersectional connection and further created networks of people across issues areas and the public and private sectors who could contribute different types of expertise and support campaign goals.<sup>180</sup> The strategic work across domains and levels also created virtuous cycles, embedding change at one level that created "positive feedback loops" in others and could produce "a widening circle of democratic transformation."<sup>181</sup> Support to reinforce creative strategy and effectively utilize integrated advocacy to create opportunities for continued change at the local and regional-level is particularly important in this political climate—where positive action in Congress and at the US Supreme Court is largely foreclosed.

## 3. Growth in Translating Strategy into Action

There has also been important growth in developing a deeper bench of public interest technology expertise that can effectively turn plans into "clear, measurable, recognizable action."<sup>182</sup> Twenty years ago, there were only a small handful of public interest technology clinics and centers, including at Berkeley Law, Harvard University, and

Oxford. Now, there are more than 50 universities from across the United States as well as international institutions that are in the public interest technology university network (PIT-UN).<sup>183</sup> Many of these institutions have taken on substantial new research, and developed centers and institutes that bring together students and academics from across disciplines to grapple with issues at the intersection of technology and policy.<sup>184</sup> The facial surveillance campaign provides a strong example of how many of the people trained at these institutions who are now working in the public interest technology community (including me at Berkeley Law) both developed and led integrated advocacy strategies that led to successful action on facial surveillance. The integrated advocacy campaign spurred high levels of engagement by the public and policymakers,<sup>185</sup> and clear, tangible change in local law, state law, and corporate policy. It drove the passage of twenty local facial surveillance bans,<sup>186</sup> the enactment of important state laws limiting facial surveillance,<sup>187</sup> successful lawsuits against companies<sup>188</sup> and police departments,<sup>189</sup> and moratoriums on sales by Amazon, IBM, and Microsoft.<sup>190</sup> The Federal Trade Commission also took action against facial surveillance.<sup>191</sup>

The pipeline has grown in the public interest technology community. But there is still much more that is needed to bring together work across disciplines, including public policy, data science, information science, computer science, law, and the broader social sciences to generate cutting-edge research, develop intellectually-rigorous, evidence-based interventions, and educate a new generation of students who are capable of leading the interdisciplinary work to address the challenges and opportunities of technological advances in the AI age.

## B. Challenges to Social Movement and Supporting Robust, Substantive Privacy Law – Narrative and Structures

While there has been some critical growth in supporting social movement power, the public interest community continues to be plagued by a weakness in robust narrative and inadequate structures that makes it very difficult to advance protections in the AI age.

### 1. Public Interest Community Is Woefully Weak at Narrative

The weakest link in the public interest technology community's work to support robust, substantive privacy law is narrative development and discipline. Leading with a powerful, consistent meta-narrative that can tell a story that inspires, builds connection, and instills hope, possibility, and a sense of group power is a linchpin in supporting positive change.<sup>192</sup> It is imperative to be able to effectively counter the opposition narratives—increasingly apocalyptic—that are designed to undermine connection and power.<sup>193</sup>

There has been some progress on developing a positive meta-narrative and moving from dry and disconnected mission and narratives to a focus on connection, group power, and hope and possibility. Compare language from the ACLU of Northern California Technology and Civil Liberties from 2004—“as technology advances, civil liberties will keep

pace” to 2024, “[t]ogether, we can harness the power of technology to free our communities, nurture our connections, and create equity and justice for all.”<sup>194</sup> Or as MediaJustice articulated, “a future where we are all connected, represented and free.”<sup>195</sup> As Fight for the Future said, “a future where technology is a force for liberation—not oppression.”<sup>196</sup> The Athena Coalition talks about rights and liberties, health and the planet, and hopes and dreams,<sup>197</sup> Mijente about the need to “free our future,”<sup>198</sup> and Just Futures Law has its mission right in its name—“Just Futures.”



Facebook CEO Mark Zuckerberg at Facebook's developer conference. Image: Wiki Commons - Anthony Quintano

But generally, from the mid-1970s to today, the public interest community has been consistently and woefully weak at narrative, and been outplayed by both the government and industry. Too many public interest advocates speak in legal or computer science jargon and get in the weeds about the specific details of a particular law or technical issue and end up reinforcing difference between issues, rather than supporting a throughline about an overall effect on people and society. The public interest community is too rarely able to communicate persuasively about what is at stake across different issues and effectively neutralize the narratives that have consistently been used by the government and industry since the mid-1970s. Government narratives focused on crime waves and policing and surveillance as safety have been largely consistent from the 1968 Safe Streets Act, to 2001,<sup>199</sup> to today.<sup>200</sup> National security and world order narratives that have been ever-present since the 1960s just took on another flavor post-September 11<sup>201</sup> and are now being used in another form with the AI race against China. The government mantra of “nothing to hide” has also not skipped a beat.<sup>202</sup> Pervasive corporate narratives work hand-in-hand along with the government narratives to undermine movement efforts to address how technology can impact individuals and society.<sup>203</sup> These narrative standbys include: (1) technology and technology companies are inherently good for the world; (2) anyone who challenges technology is a backwards luddite; (3) technology and any potential uses of it are inevitable and people are powerless; and (4) technology is too complicated—you don't understand it. Finally, if the first four narratives are not getting adequate traction, then industry regroups to a narrative that is seemingly in contradiction to the social good narrative and claims that (5) technology is just a neutral tool and the companies who develop, build it, or deploy it are not responsible for how technology is used or how it impacts people or society. To pass robust privacy law, the

public interest community must have a greater focus on narrative that calls out the government and industry playbook, and dedicate more resources to seed a powerful and consistent social justice narrative that replaces people's feelings of powerlessness with intersectional power and that transforms resignation to indignation.

#### Industry Narrative #1 – Good for Technology Companies, Good for the World

Industry has been particularly successfully in employing a narrative that is basically “what is good for them is also good for the world.”<sup>204</sup> That any costs to the company are actually bad for people and society. While the 1973 HEW Report included a strong, proactive argument that organizations must not be allowed to externalize the costs of computerization to individuals and society,<sup>205</sup> by the 1977 PPSC report, the narrative of what is good for business is good for society had become entrenched and that “costs of privacy” could not be allowed to be burdensome to business.<sup>206</sup> Facebook's use of this good for society narrative is one of the most aggressive, with its founder long claiming that it was “built to accomplish a social mission,”<sup>207</sup> while internal memos revealed the “ugly truth.”<sup>208</sup> This “technology-equals progress narrative” has to be consistently challenged by movement leaders and exposed for what it is, “a convenient myth propagated by a huge industry.”<sup>209</sup>

#### Industry Narrative #2 – Resisters Are “Luddites”

A second, consistent narrative in the corporate arsenal is the backwards “luddite.” Anyone who dares to challenge the premise that technology and technology companies are always inherently good for people and the world is a luddite who is stuck in the past and is stifling innovation. This narrative was present as early as 1971, when Arthur Miller grappled with it during the Ervin congressional hearings and defended against being characterized as a “19th century luddite who is out to smash the machines.” Miller analogized to then-recent developments in car safety and how it would be worthwhile to have the same type of in-depth perception, analysis, and study of the computer.<sup>210</sup> The implied message of this luddite narrative (as well as the direct contention of industry lobbyists that consistently argue, regardless of the topic of the legislative bill, that it will “stifle innovation”) is that they “should be allowed get on with their habits of ‘creative destruction’...without being troubled by regulation.”<sup>211</sup> This narrative must finally be toppled to advance protections for people.

#### Industry Narrative #3 –Technology Is Inevitable and People Should Feel Powerless

The third consistent narrative that is used to undermine movement power is that technology is inevitable and people should feel powerless to control it. Often this narrative takes the form of phrases, such as “the train has left the station” or “the genie is out of bottle.” It extols the futility of actually taking a moment to thoughtfully consider the “why” of using the technology and doing a deeper inquiry into whether using the technology will have greater costs than benefits, before just jumping to the “how” of using a technology in every instance. The importance of countering a narrative of powerlessness

related to advances in technology was specifically discussed in the legislative materials for the 1972 California Privacy Amendment<sup>212</sup> and it is even more important today. As of 2023, a majority of Americans believed they have “little to no control” over what the government or companies do with their data<sup>213</sup> and that what companies know about them can hurt them, but that they are “powerless to stop it.”<sup>214</sup> While the facial surveillance campaign is an example of what can be accomplished when there is a people-centered narrative of principled refusal,<sup>215</sup> industry is tenacious in its use of the inevitability narrative to attempt to belittle and undermine any challengers. It has reached a fever pitch in the AI hype cycle, with the “father of AI” saying the “rise of artificial intelligence is inevitable but should not be feared”<sup>216</sup> and article upon article characterizing it as “inevitable.”<sup>217</sup> But as Margaret Heffernan discusses, “[a]ll assertions of inevitability have an agenda. Anyone claiming to know the future is just trying to own it.”<sup>218</sup> The goal of “that tone of inevitability” is not “participation, but submission” and the “language of inevitability has to be called out for the propaganda that it is.”<sup>219</sup>

**"The public interest community needs to counter the industry's AI-washing, tech exceptionalism narrative with a strong spin cycle that centers the needs of people and society."**

#### Industry Narrative #4 – Technology Issues Are Too Complicated

The fourth consistent narrative that is particularly detrimental to intersectional social movement power is that technology issues are just too complicated for mere mortals to understand—or as the technology industry has so often shorthanded it—You'll Break the Internet. The technology industry promulgates a narrative that technology is too confusing, that it is too hard for regular people and elected officials to understand. The goal of this narrative is to make people feel that their knowledge of important community issues, how technology may be impacting these issues, and their thoughts about what should be done to address the concerns, are not valid. That “we aren't smart enough to have choices. And any questions we ask, we aren't smart enough to understand.”<sup>220</sup> Industry is now regularly engaging in what I term “AI-washing”—slapping the term AI on an issue or product to attempt to intimidate people against speaking up about how it affects their lives.<sup>221</sup> It is not a coincidence that while most politicians are not experts on any subject matter, it seems to primarily be technology hearings that produce flack for legislators as “clueless,”<sup>222</sup> and statements that technology is “prone to over regulation” and “misunderstanding,”<sup>223</sup> despite the fact that the US has not enacted a substantial technology law in more than 30 years.

## "It is critical for advocates to be working together and ensuring that the public interest community can aggressively, consistently, and collaboratively counter narratives that are meant to undermine fights for justice"

But just like the liberation movements in the 1970s understood the potential impact of computerization, people today, particularly already marginalized communities, continue to clearly comprehend how advances in technology can impact access, equity, and justice. The public interest community needs to counter the industry's AI-washing, tech exceptionalism narrative<sup>224</sup> with a strong spin cycle that centers the needs of people and society.

### Industry Narrative #5 – Technology Is Neutral and Technology Companies Are Not Responsible for its Use

If any of the first four narratives are pierced in any way and there is traction for change, then one can often see industry regroup to a narrative that is actually the flip side of its narrative of social good—that technology is actually just a neutral tool and the technology companies who develop, build, or deploy it are not responsible for how it is used or how it impacts people or society. This played out with the facial surveillance fight when Amazon was in the hot seat for its dangerous Rekognition system. Widespread advocacy had changed the national dialogue on facial surveillance, with significant media discussing its dangers, letters of concern sent by prominent lawmakers about its impact on African Americans, immigrants, and activists, as well as opposition letters from employees and shareholders.<sup>225</sup> Amazon CEO Jeff Bezos attempted to defend against the successful coalition advocacy by saying that new technologies should not be viewed as good or bad. While he acknowledged his company's products might be put to "bad uses," he said the solution was to wait for society's eventual "immune response" to take care of the problems.<sup>226</sup> Amazon's employees disagreed and issued a letter demanding that the company stop selling facial recognition services to law enforcement. The letter highlighted that "technology like ours is playing an increasingly critical role across many sectors of society. What is clear to us is that our development and sales practices have yet to acknowledge the obligation that comes with this...we refuse to contribute to tools that violate human rights...The time to act is now..."<sup>227</sup> Amazon employees did not buy the industry narrative hype and neither should anyone else.

Big picture, whatever the flavor of the fight, the other side does not fight piecemeal, with disconnected efforts. It fights with coordinated efforts and narrative discipline. It is critical for advocates to be working together and ensuring that the public interest community can aggressively, consistently, and collaboratively counter narratives that are meant to undermine fights for justice and for social movement narratives to hold sway in the minds of decisionmakers—whether that be in court, legislatures, or the court of public opinion.

Movement leaders also need to be more aware of how and why the public interest community often gives opposition narratives

more power, not less, by its reactions. When opposition narratives seem to be initially swaying the public or policymakers, the public interest community too often responds by negotiating against itself on the policy position, which can also undermine core relationships and coalition trust that are essential to the growth of the social movement. If a policymaker initially reacts that a bill, an ask, or an issue is not "reasonable" or is "not politically feasible," that should not be the cue for the public interest community to backtrack on a substantive position. Rather, it should be the cue that there is work that needs to be done to develop greater relationships, build a more diverse coalition, engage in more effective public organizing, and change the power calculus. It should also signal to the public interest community that there is a real need to reinforce the strategic communications work to advance the positive narrative and effectively undermine the opposition narratives that are keeping the issue from advancing. Whether any change is seen as radical or reasonable, fringe, or political feasible, are just constructs of power. Whoever holds the power in public opinion—whoever owns the narrative—can push change.



The Amazon Spheres, part of Amazon's headquarters campus in Seattle, Washington, United States. Image: Wiki Commons - SounderBruce

### 2. Public Interest Community Needs More Sustainable Structures, Training, and Support

It is also more critical than ever for there to be consistent structures and resources, including funding and training resources, to support sustained relationships, coordination, collaboration, and intersectional power building. There has been an increased focus on measurable outcomes for public interest work. While it is important to have actions that lead to tangible change, a focus on measurement must not undermine the need for foundational relationships, connection, and solidarity. For "when measurement consumes our civic imagination, everything that can't be measured—the relationships and collective experiences that uphold democracy—is liable to wither."<sup>228</sup> Without a pipeline of leaders who have the formal and informal training and support to both come into and stay in movement work and lead diverse efforts across strategy, the movement cannot continue to build and sustain constituencies.<sup>229</sup>



Civil Rights March on Washington, D.C., August 28, 1963. Image: Wiki Commons - Warren K. Leffler

The Ford Civil Rights Table and its focus on supporting a “network for cross-sector collaboration and learning” has been instrumental in supporting deeper relationships and fostering cross-sector vehicles for change that “can be greater than the sum of their parts.”<sup>230</sup> There are newer funding streams, like the CS Fund’s Just Transitions Program, which has been supporting global organizations in having the resources to break down silos with digital justice and support movement power building across sectors.<sup>231</sup> Models like BATT are supporting hyper-local cross sector collaboration and learning that helps to build a widening circle of confidence and expertise in issues at the intersection of technology, rights, and democracy.<sup>232</sup> It is particularly important to continue to have more support for structures that enable the public interest technology community, especially grassroots organizations and diverse voices at the local and state-level, to have the training and resources to engage in strategic communications and weave robust, people-centered narratives across strategies and time.

PIT-UN has been supporting structures in academic institutions to build the public interest technology field, but there is still a dearth of the cross-disciplinary curriculum and integrated advocacy skills training necessary to effectively lead and implement work on technology issues. Working effectively on fast-moving public interest technology issues requires a broad set of skills far beyond what is often taught in graduate programs about how to litigate a case, draft a law, or how to code. It requires the ability to recognize the realities of complex systems and the problem-solving skills necessary to integrate tactical modes.<sup>233</sup> It requires moving from the “narrow lens” of technical skill to the “broader art of persuasion” and being able to tell compelling stories to those with decision-making power and the wider public and “exert pressure and build support for political and cultural change.”<sup>234</sup> It requires being a leader—someone who can inspire people to come together and take responsibility for enabling

others to achieve shared purpose under uncertain conditions.<sup>235</sup> It also requires leaders who have the people and project management skills to be able to effectively plan, coordinate, and move work forward across strategy and time.

Law schools generally lack adequate training in how to develop and implement integrated legal advocacy across strategies and lead cross-disciplinary efforts that are necessary for public interest technology work. Few public policy programs offer sufficient training in how to analyze and establish strategies for designing, procuring, implementing, using, and regulating AI technologies and other systems that are growing across the private and public sectors. Computer science schools—data science, information science, and a few similarly interdisciplinary-oriented technical programs—may include some social, legal, and ethical training, but largely do not expose students to public policy methods and processes. Cross-disciplinary curriculum in integrated advocacy and technology policy should be reinforced and expanded in law school and other graduate disciplines, like information science, data science, computer science, public policy, public health, medicine, and other areas to train and support leaders who can properly address how AI and other emerging technologies are impacting diverse people and communities.

## CONCLUSION

In the current political climate and with exponential advances in AI, there is no more urgent time to learn from the past and not replicate the missteps of the 1970s. Now is the time to work strategically on the local, state, national, and international-level to continue to build the social movement necessary to put real power into privacy law and make AI and other technology work for the people.

## REFERENCES

- 1 The Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems (HEW Committee) met between April 1972 and May 1973 and developed the 1973 Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems (HEW Report).
- 2 United States House of Representatives, Privacy Act, 1974, <https://www.congress.gov/bill/93rd-congress/house-bill/16373/all-info>.
- 3 Jason Kelly, "EFF Sues DOGE and the Office of Personnel Management to Halt Ransacking of Federal Data," Electronic Frontier Foundation, February 11, 2025, <https://www.eff.org/deeplinks/2025/02/eff-sues-doge-and-office-personnel-management-halt-ransacking-federal-data>.
- 4 Lori Trahan, "Trahan Announces Effort to Reform Privacy Act of 1974, Protect Americans' Data from Government Abuse," Lori Trahan (2025), <https://trahan.house.gov/news/documentsingle.aspx?DocumentID=3491>.
- 5 Nicole A. Ozer, "Will We Let a Digital Coup Against Democracy Prevail?," The Contrarian, February 25, 2025, <https://contrarian.substack.com/p/will-we-let-a-digital-coup-against>.
- 6 United States House of Representatives, Electronic Communications Privacy Act of 1986 (1986), <https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg1848>.
- 7 Declan McCullagh, "Google, Facebook Go Retro in Push to Update 1986 Privacy Law," CNET, October 21, 2011, <https://www.cnet.com/news/privacy/google-facebook-go-retro-in-push-to-update-1986-privacy-law/>.
- 8 Declan McCullagh, "How 9/11 Attacks Reshaped U.S. Privacy Debate," CNET, September 9, 2011, <https://www.cnet.com/news/privacy/how-911-attacks-reshaped-u-s-privacy-debate/>.
- 9 "Surveillance Under the USA/PATRIOT Act," American Civil Liberties Union, October 23, 2001, <https://www.aclu.org/documents/surveillance-under-usapatriot-act>, Accessed June 7, 2025; California Legislature; California Civil Code, Section 1789.90.
- 10 I spearheaded the passage of CalECPA. California Legislature, California Electronic Communications Privacy Act (CalECPA) (2015), [https://leginfo.ca.gov/faces/codes\\_displaySection.xhtml?sectionNum=1546.&lawCode=PEN](https://leginfo.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1546.&lawCode=PEN); "California Electronic Communications Privacy Act (CalECPA) - SB 178," ACLU of Northern California, January 2025; <https://www.aclunc.org/our-work/legislation/california-electronic-communications-privacy-act-calcapa-sb-178>.
- 11 Matt Cagle, Nicole Ozer, and Brady Hirsch, "Seeing Through Surveillance: Why Policymakers Should Look Past the Hype," American Civil Liberties Union of Northern California, July 2024, [https://www.aclunc.org/sites/default/files/Seeing\\_Through\\_Surveillance\\_\\_Report\\_Web.pdf](https://www.aclunc.org/sites/default/files/Seeing_Through_Surveillance__Report_Web.pdf).
- 12 United States Congress, Fair Credit Reporting Act, Public Law 91-508, 84 Stat. 1128 (1970) (codified as amended at 15 U.S.C. § 1681 et seq.).
- 13 United States, Congress, Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, (1996), 110 Stat. 1936.
- 14 California Legislature, California Consumer Privacy Act of 2018, Assembly Bill No. 375, Chapter 55, approved by Governor June 28, 2018.
- 15 Neil Richards and Woodrow Hartzog, "The Vermont Veto Is a Step Backward for Privacy," International Association of Privacy Professionals (IAPP), June 18, 2024, <https://iapp.org/news/a/the-vermont-veto-is-a-step-backward-for-privacy>.
- 16 Solon Barocas and Helen Nissenbaum, "On Notice: The Trouble with Notice and Consent," Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information (2009), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2567409](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567409); Paul M. Schwartz, "Privacy and Democracy in Cyberspace," *Vanderbilt Law Review* 52, no. 6 (1999): 1609–1701, <https://scholarship.law.vanderbilt.edu/vlr/vol52/iss6/2/>; Neil Richards and Woodrow Hartzog, "The Pathologies of Digital Consent," *Washington University Law Review* 96, no. 6 (2019): 1461–1513, [https://openscholarship.wustl.edu/law\\_lawreview/vol96/iss6/11/](https://openscholarship.wustl.edu/law_lawreview/vol96/iss6/11/); Daniel J. Solove, "Murky Consent: An Approach to the Fictions of Consent in Privacy Law," *Boston University Law Review* 104 (2024): 593–641, <https://dx.doi.org/10.2139/ssrn.4333743>; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York, NY: PublicAffairs, 2019); Joseph Turow, Yphtach Lelkes, Nora A. Draper, and Ari E. Waldman, "Americans Can't Consent to Companies' Use of Their Data," University of Pennsylvania Annenberg School for Communication, 2023, <https://perma.cc/J3ZR-RBG6>.
- 17 Roseanna Sommers and Vanessa K. Bohns, "Consent Searches and Underestimation of Compliance: Robustness to Type of Search, Consequences of Search, and Demographic Sample," *Journal of Empirical Legal Studies* 21, no. 4 (2024), <https://doi.org/10.1111/jels.12375>.
- 18 Vanessa K. Sommers, Mahdi Roghanizad, and Amy Z. Xu, "Underestimating Our Influence Over Others' Unethical Behavior and Decisions," *Personality and Social Psychology Bulletin* 40, no. 3 (2013) 348–359, <https://journals.sagepub.com/doi/10.1177/0146167213511825>.
- 19 Richard Mackenzie-Gray Scott, "'Consent or Pay' and the Future of Privacy," Tech Policy Press, July 18, 2024, <https://www.techpolicy.press/consent-or-pay-and-the-future-of-privacy>.
- 20 Anita Allen, "Dismantling the 'Black Opticon': Privacy, Race, Equity, and Online Data-Protection Reform," *Yale Law Journal Forum* 131 (2022): 907–924, <https://www.yalelawjournal.org/forum/dismantling-the-black-opticon>.
- 21 Tawana Petty, et al., "Our Data Bodies: Reclaiming Our Data," Our Data Bodies Project (2018), [https://www.odbproject.org/wp-content/uploads/2016/12/ODB.InterimReport.FINAL\\_7.16.2018.pdf](https://www.odbproject.org/wp-content/uploads/2016/12/ODB.InterimReport.FINAL_7.16.2018.pdf).
- 22 Nicole Ozer, "Golden State Sword: The History and Future of California's Constitutional Right to Privacy to Defend and Promote Rights, Justice, and Democracy in the Modern Digital Age," *Berkeley Technology Law Journal* 39 (2024): 961, <https://ssrn.com/abstract=5013707>.  
*White v. Davis*, 13 Cal. 3d 757, 533 P.2d 222, 120 Cal. Rptr. 94 (1975).

23 *White v. Davis*, 13 Cal. 3d 757, 533 P.2d 222, 120 Cal. Rptr. 94 (1975).

24 Ozer, "Golden State Sword."

25 Ozer, "Golden State Sword."

26 It was one of the few (if only) public interest law organizations working on these issues at the time. The July 15, 1970, notes of the ACLU Privacy Committee included that the 1969–1970 Committee conducted a letter survey of organizations about computers and data collection, storage, and dissemination and the responses indicated "there was no present engagement in a study or similar activity." American Civil Liberties Union Records, MC#001, Box 1091, Folder 10, 1970, Notes of the ACLU Privacy Committee, July 15, 1970 (on file with author).

27 "Lawrence Speiser's Testimony: The Proposed Federal Data Center," *ACLU of Northern California News* 32, no. 4 (April 1967) 3, [https://digitallibrary.californiahistoricalsociety.org/object/15631?islandora\\_paged\\_content\\_page=3](https://digitallibrary.californiahistoricalsociety.org/object/15631?islandora_paged_content_page=3).

28 The Conference included 13 privacy panels, a banquet speech by US Supreme Court Justice William O. Douglas, and an additional keynote speech by Alan Westin.

29 *ACLU of Northern California News* 32, no. 5 (May 1967), [https://digitallibrary.californiahistoricalsociety.org/object/15606?solr\\_nav%5Bid%5D=6f116fdfadb5309128bd&solr\\_nav%5Bpage%5D=0&solr\\_nav%5Boffset%5D=4](https://digitallibrary.californiahistoricalsociety.org/object/15606?solr_nav%5Bid%5D=6f116fdfadb5309128bd&solr_nav%5Bpage%5D=0&solr_nav%5Boffset%5D=4); *ACLU of Northern California News* 32, no. 3 (March 1967), [https://digitallibrary.californiahistoricalsociety.org/object/15636?solr\\_nav%5Bid%5D=394161b2536c2b387f02&solr\\_nav%5Bpage%5D=0&solr\\_nav%5Boffset%5D=3](https://digitallibrary.californiahistoricalsociety.org/object/15636?solr_nav%5Bid%5D=394161b2536c2b387f02&solr_nav%5Bpage%5D=0&solr_nav%5Boffset%5D=3); *ACLU of Northern California News* 32, no. 4 (April 1967): 3, [https://digitallibrary.californiahistoricalsociety.org/object/15631?islandora\\_paged\\_content\\_page=3](https://digitallibrary.californiahistoricalsociety.org/object/15631?islandora_paged_content_page=3).

30 *ACLU of Northern California News* 32, no. 6 (June 1967): 2-3, [https://digitallibrary.californiahistoricalsociety.org/object/15616?islandora\\_paged\\_content\\_page=2](https://digitallibrary.californiahistoricalsociety.org/object/15616?islandora_paged_content_page=2).

31 Richard Ruggles, John Pemberton, and Arthur R. Miller, "Computers, Data Banks, and Individual Privacy," *Minnesota Law Review* 53, (1968): 223, 236, <https://scholarship.law.umn.edu/mlr/2164/>.

32 Ruggles, Pemberton, and Miller, 236.

33 Ruggles, Pemberton, and Miller, 240.

34 At that time, Arthur R. Miller was a professor of law at the University of Michigan. Miller was subsequently the Bruce Bromley Professor of Law at Harvard Law School from 1971-2007. "Arthur R. Miller," Wikipedia, [https://en.wikipedia.org/wiki/Arthur\\_R.\\_Miller](https://en.wikipedia.org/wiki/Arthur_R._Miller), Accessed June 7, 2025.

35 Ruggles, Pemberton, and Miller, 240.

36 Ruggles, Pemberton, and Miller, 244.

37 Ruggles, Pemberton, and Miller, 240.

38 Ruggles, Pemberton, and Miller, 244 (emphasis in original).

39 Ruggles, Pemberton, and Miller, 238.

40 Ruggles, Pemberton, and Miller, 238.

41 "The Burglary That Exposed COINTELPRO: Activists Mark 50th Anniversary of Daring FBI Break-in," *Democracy Now!*, March 9, 2021, [https://www.democracynow.org/2021/3/9/50th\\_anniversary\\_fbi\\_office\\_cointelpro\\_exposure](https://www.democracynow.org/2021/3/9/50th_anniversary_fbi_office_cointelpro_exposure); Tom Jackman, "The FBI Break-in that Exposed J. Edgar Hoover's Misdeeds to be Honored With Historical Marker," *The Washington Post*, September 1, 2021, <https://www.washingtonpost.com/history/2021/09/01/fbi-burglary-hoover-cointelpro/>; Bonnie Raines, "I Broke into an FBI Office and Took Every Document. Here's Why," *ACLU*, January 15, 2014, <https://www.aclu.org/news/national-security/i-broke-fbi-office-and-took-every-document-heres-why>.

42 "Federal Bureau of Investigation," *Martin Luther King, Jr. Research & Education Institute*, Stanford University, March 16, 1909, [https://kinginstitute.stanford.edu/federal-bureau-investigation-fbi#:~:text=In%20the%20following%20months%2C%20Hoover,SCLC\)%20offices%20in%20October%201963](https://kinginstitute.stanford.edu/federal-bureau-investigation-fbi#:~:text=In%20the%20following%20months%2C%20Hoover,SCLC)%20offices%20in%20October%201963), Accessed June 7, 2025.; "Fresh Air: Documentary Exposes How FBI Tried to Destroy MLK With Wiretaps, Blackmail," *NPR*, January 18, 2021, <https://www.npr.org/2021/01/18/956741992/documentary-exposes-how-the-fbi-tried-to-destroy-mlk-with-wiretaps-blackmail>.

43 Martin Luther King, Jr., "Remaining Awake Through a Great Revolution," Sermon at the National Cathedral, March 31, 1968, <https://archive.org/details/MartinLutherKingJrAllSpeeches/Dr.+Martin+Luther+King+Jr.++Complete+Speeches+and+Sermons/1968+03+31+Remaining+Awake+Through+a+Great+Revolution%2C+National+Cathedral+3-31-68.mp3>.

44 "The Black Panther Party," *National Archives*, <https://www.archives.gov/research/african-americans/black-power/black-panthers>, Accessed June 7, 2025.

45 "COINTELPRO," *PBS*, [https://www.pbs.org/hueypnewton/actions/actions\\_cointelpro.html](https://www.pbs.org/hueypnewton/actions/actions_cointelpro.html), Accessed June 7, 2025.

46 First publicized in the second issue of the organization's newspaper, *Black Panther*, on May 15, 1967, the platform and program, titled "What We Want Now! What We Believe," was a set of guidelines written by Newton and Seale that emphasized the Party's ideals and commitment to advancing a revolution that addressed the needs of the Black community. "The Black Panther Party's Ten-Point Program," *UC Press Blog*, February 7, 2024, <https://www.ucpress.edu/blog/25139/the-black-panther-party-ten-point-program/>; Andrew Beale, et al., "The Black Panther Party's Ten-Point Program, 50 Years Later," *Oakland North*, November 4, 2016, <https://oaklandnorth.net/2016/11/04/the-black-panther-party-ten-point-program-50-years-later/>. By 1972, community control over technology was in the Ten Point Plan. "The Black Panther Party's Ten Point Program 1972,"

Black Panther Party Alumni Legacy Network, <https://bppaln.org/10-point-platform>.

47 Richard Ruggles, "On the Needs and Values of Data Banks," *Minnesota Law Review* 53 (1968): 211-212. Ruggles was a member of the economics department at Yale from 1946-1985 and chair of the department from 1969-1972.

48 Ruggles, "On the Needs and Values of Data Banks," 213.

49 Ruggles, "On the Needs and Values of Data Banks," 213.

50 Ruggles, "On the Needs and Values of Data Banks," 213.

51 Committee on the Judiciary, Subcommittee on Constitutional Rights, "Federal Data Banks, Computers, and the Bill of Rights: Hearings Before the Subcommittee on Constitutional Rights of the Committee of the Judiciary," United States Senate, 1971, 6, <https://babel.hathitrust.org/cgi/pt?id=uc1.c051765460&view=1up&seq=19&q1=aclu>.

52 Committee on the Judiciary, Subcommittee on Constitutional Rights, "Federal Data Banks, Computers, and the Bill of Rights," 1.

53 Committee on the Judiciary, Subcommittee on Constitutional Rights, "Federal Data Banks, Computers, and the Bill of Rights," 1. These concerns have remained present. A 2015 Annenberg study found that a large pool of Americans remain very concerned and objected to these activities but also feel resigned to the inevitability of surveillance and the power of marketers to harvest their information. A 2023 follow-up Annenberg study found that 91% percent of people wanted to have control over what marketers can learn about them online. Russel Heimlich, "Internet Users Don't Like Targeted Ads," Pew Research Center, March 13, 2012, <https://www.pewresearch.org/short-reads/2012/03/13/internet-users-dont-liketargeted-ads>; Joseph Turow, Michael Hennessy, and Nora Draper, "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation," *SSRN Electronic Journal* (2015), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2820060](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820060); Turow, et al., "Americans Can't Consent."

54 Committee on the Judiciary, Subcommittee on Constitutional Rights, "Federal Data Banks, Computers, and the Bill of Rights," 6.

55 Committee on the Judiciary, Subcommittee on Constitutional Rights, "Federal Data Banks, Computers, and the Bill of Rights," 1, 64.

56 Gerhard Casper is the President Emeritus of Stanford University and the Peter and Helen Bing Professor, Emeritus, Professor of Law, Emeritus, and Professor of Political Science (by courtesy), Emeritus. "Gerhard Casper." Stanford University, <https://gcasper.stanford.edu/>, Accessed April 30, 2025.

57 Committee on the Judiciary, Subcommittee on Constitutional Rights, "Federal Data Banks, Computers, and the Bill of Rights," 64.

58 Committee on the Judiciary, Subcommittee on Constitutional Rights, "Federal Data Banks, Computers, and the Bill of Rights," 64

59 Committee on the Judiciary, Subcommittee on Constitutional Rights, "Federal Data Banks, Computers, and the Bill of Rights," 9.

60 Committee on the Judiciary, Subcommittee on Constitutional Rights, "Federal Data Banks, Computers, and the Bill of Rights," 9.

61 Committee on the Judiciary, Subcommittee on Constitutional Rights, "Federal Data Banks, Computers, and the Bill of Rights," 13.

62 CPP started in 1968 with opposition to the Vietnam War and then became engaged in additional intersectional social justice movements. Privacy was an important Computer People for Peace issue. Shwetha Jayaraj, "A Brief History from Hack Manhattan—An Ode to the 1970's Computer People for Peace," Medium (blog), December 31, 2022, <https://medium.com/@shwethajayaraj/a-brief-history-from-hack-manhattan-an-ode-to-the-1970s-computer-people-for-peace-fe04623d5d21>.

63 Committee on the Judiciary, Subcommittee on Constitutional Rights, "Federal Data Banks, Computers, and the Bill of Rights," 931.

64 CPP specifically articulated (1) that the concept of "public information" needs to be limited to name, address, and social security number. No transfer of data from one agency to another and no sale under any circumstances; (2) Informed about data collected and right to deletion/ destruction of anything more than name, address, and social security number; (3) No person denied any public or private service for refusal to supply personal data; (4) No information collected unless "need to know" and the burden of justifying the "need to know" should rest of with the collection; (5) Anonymization—statistical data necessary for analysis and planning should be collected in such a way that none of it can be traced to any individual; and (6) Retention cycles should be established for the data collection on individuals. Committee on the Judiciary, Subcommittee on Constitutional Rights, "Federal Data Banks, Computers, and the Bill of Rights," 933.

65 "The Burglary That Exposed COINTELPRO"; Jackman, "The FBI Break-in that Exposed J. Edgar Hoover's Misdeeds to be Honored With Historical Marker"; Raines, ry/2021/09/01/fbi-burglary-hoover-cointelpro/; Bonnie Raines."

66 Ozer, "Golden State Sword."

67 Staff of Assembly Constitutional Committee, "Report on ACA 51," California Assembly, 1972, 5, <https://www.aclunc.org/sites/default/files/Staff%20report%20of%20Assembly%20Constitutional%20Committee%20on%20ACA%2051%20%28before%20April%2024%29.pdf>.

68 Staff of Assembly Constitutional Committee, "Report on ACA 51."

69 Ignazio Vella, Letter to Assemblyman Kenneth Cory, January 17, 1972, 1-2, <https://www.aclunc.org/sites/default/files/Letter%20from%20Inter-governmental%20Board%20on%20Electronic%20Data%20Processing%20Chairman%20Ignazio%20Vella%20to%20Hon.%20Kenneth%20Cory.pdf>.

70 Article I, Section 1 of the California Constitution reads: "All people are by nature free and independent and have inalienable rights. Among these

are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.” California Constitution. Article I, Section 1.

71 “Ballot Proposition 11, Constitutional Right to Privacy Amendment,” 1972, [https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca\\_ballot\\_props](https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props).

72 “Ballot Proposition 11, Constitutional Right to Privacy Amendment.”

73 Article I, Section 1 of the California Constitution reads: “All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.” California Constitution. Article I, Section 1.

74 *White v Davis*, 533 P.2d at 224 (first California Supreme Court case to interpret the Privacy Amendment, holding that a spying program of the Los Angeles Police Department, which infiltrated UCLA courses and organizations to create dossiers on students and professors, constituted “a prima facie violation of the explicit ‘right of privacy’ recently added to our state Constitution.”). The full, intended reach of the California constitutional right to privacy was undermined by the 1994 California Supreme Court case, *Hill v. NCAA*. See Ozer, “Golden State Sword,” 1006-1011.

75 Alan F. Westin and Michael A. Baker, *Databanks in a Free Society: Computers, Record-Keeping and Privacy*, (New York, NY: Quadrangle Books, 1972) 405; Privacy Protection Study Commission, Introduction to “Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission” (1977), <https://archive.epic.org/privacy/ppsc1977report/c1.htm>.

76 Westin and Baker, *Databanks in a Free Society*, xiii.

77 HEW Committee, “Records, Computers and the Rights of Citizens.”

78 Privacy Protection Study Commission, Introduction to “Personal Privacy in an Information Society.”

79 For example, there was support from the ACLU of Northern California and women’s rights activists. ACLU of Northern California News 37, no. 7, <https://digitallibrary.californiahistoricalsociety.org/object/16083>; “Testimony of Cheriell Moench Jensen,” Hearing on ACA 51 Before the Assembly Constitutional Amendments Committee, 1972, <https://www.aclunc.org/sites/default/files/Testimony%20before%20Assembly%20Constitutional%20Amendments%20Committee%20%28April%2024%2C%201972%29.pdf>.

80 Hugh Bayless, Support Letter to Hon. Donald L. Grunsky, June 12, 1972, [https://www.aclunc.org/sites/default/files/Letter%20from%20Carmel-by-the-Sea%20City%20Administrator%20Hugh%20Bayless%20to%20Hon.%20Donald%20L.%20Grunsky%20\(June%2012%2C%201972\).pdf](https://www.aclunc.org/sites/default/files/Letter%20from%20Carmel-by-the-Sea%20City%20Administrator%20Hugh%20Bayless%20to%20Hon.%20Donald%20L.%20Grunsky%20(June%2012%2C%201972).pdf).

81 Susan R. Jones, “Dr. Martin Luther King, Jr.’s Legacy: An Economic Justice Imperative,” *Washington University Journal of Law & Policy* 19, no. 1 (2005): 39, [https://openscholarship.wustl.edu/law\\_journal\\_law\\_policy/vol19/iss1/6/](https://openscholarship.wustl.edu/law_journal_law_policy/vol19/iss1/6/). Several prominent civil rights groups were already focused on economic justice and labor exploitation by this time, including Huey Newton and the Black Panther Party, the Nation of Islam, the Student Non-violent Coordinating Committee, the Congress of Racial Equality, and the United Farm Workers, among others. Eldridge Cleaver, “On the Ideology of the Black Panther Party (Part 1),” *The Black Panther Party*, <https://www.freedomarchives.org/Documents/Finder/Black%20Liberation%20Disk/Black%20Power!/SugahData/Books/Cleaver.S.pdf>; Malcolm X, “Twenty Million Black People in a Political, Economic, and Mental Prison,” January 23, 1963, *Malcolm X: The Last Speeches* (Montreal: Pathfinder Press, 1989), 51; Mike Miller, “SNCC—the Student Nonviolent Coordinating Committee—Gathers 50 Years After it Started: A Report on the Reunion,” *Poverty & Race Research Action Council*, August 1, 2010, <https://www.prrac.org/sncc-the-student-nonviolent-coordinating-committee-gathers-50-years-after-it-started-a-report-on-the-reunion/>; “About the Congress of Racial Equality,” *Congress of Racial Equality*, <https://www.thecongressofracialequality.org/about.html>, Accessed May 2, 2025.

82 Vesla M. Weaver, “Frontlash: Race and the Development of Punitive Crime Policy,” *Studies in American Political Development* 21 (2007): 230, <https://www.cambridge.org/core/journals/studies-in-american-political-development/article/frontlash-race-and-the-development-of-punitive-crime-policy/9744286F944F1A250B94CD3AFB1A6021>. 237.

83 Between the evening of Monday, April 4, when Dr. King was shot and killed, and Easter Sunday, April 14, 1968, arson or sniper fire was reported in 196 cities in 36 states plus Washington, D.C. Peter B. Levy, *The Great Uprising* (Cambridge, UK: Cambridge University Press, 2018), 153-188.

84 Melissa Maki and U.Va News Staff, “Political Scientist Traces the Origins of Modern Crime Policy,” *UVA Today*, June 27, 2008, <https://news.virginia.edu/content/political-scientist-traces-origins-modern-crime-policy#:~:text=As%20white%20voters%20watched%20rioting,also%20reinstated%20during%20this%20time.>

85 “Statement by the President Upon Signing the Omnibus Crime Control and Safe Streets Act of 1968,” *The American Presidency Project*, June 19, 1968, <https://www.presidency.ucsb.edu/documents/statement-the-president-upon-signing-the-omnibus-crime-control-and-safe-streets-act-1968>.

86 “Statement by the President Upon Signing the Omnibus Crime Control and Safe Streets Act of 1968.”

87 United States Congress, *The Omnibus Crime Control and Safe Streets Act of 1968*, 18 U.S.C. §§ 2510-22, 1968.

88 Weaver, “Frontlash: Race and the Development of Punitive Crime Policy,” 258.

89 ACLU of Northern California News 37, no. 3 (April 1972).

90 Dan Baum, “Legalize it All: How to Win the War on Drugs,” *Harper’s Magazine*, April 2016, <https://harpers.org/archive/2016/04/legalize-it-all/>.

91 Donald F. Tibbs, “From Black Power to Hip Hop: Discussing Race, Policing, and the Fourth Amendment Through the ‘War On’ Paradigm,” *The*

- Journal of Gender, Race & Justice 15, no. 1 (2012): 63-65, <https://researchdiscovery.drexel.edu/esploro/outputs/journalArticle/From-Black-Power-to-Hip-Hop/991021867239304721>.
- 92 Joseph Caraccappa, "Terry v. Ohio and the Power of the Police to Accost Citizens Absent Probable Cause to Arrest: A Critical Look at the Pennsylvania Experience," *Duquesne Law Review* 16, no. 4 (1977): 499, <https://dsc.du.edu/dlr/vol16/iss4/3> (cited in Tibbs at 65); Lawrence Rosenthal, "Pragmatism, Originalism, Race, and the Case Against Terry v. Ohio," *Texas Tech Law Review* 43 (2010): 299, [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1645436](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1645436).
- 93 Tibbs, "From Black Power to Hip Hop," 65.
- 94 Ben Shatz, "Scrap Retention Elections?," *Southern California Appellate News*, February 26, 2025, <https://social-appellate.blogspot.com/2025/02/scrap-retention-elections.html>.
- 95 Frank Clifford, "Voters Repudiate 3 of Court's Liberal Justices," *Los Angeles Times*, November 5, 1986, <https://www.latimes.com/archives/la-xpm-1986-11-05-mn-15232-story.html>; The Committee on History of Law in California, "Oral History: Justice Joseph R. Grodin," *Hastings Constitutional Law Quarterly* 16, no. 1 (1988): 7, [https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1407&context=hastings\\_constitutional\\_law\\_quaterly](https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1407&context=hastings_constitutional_law_quaterly); Jonathan Simon, *Governing Through Crime: How the War on Crime Transformed American Democracy and Created a Culture of Fear* (Oxford, UK: Oxford University Press, 2007).
- 96 Clifford, "Voters Repudiate 3 of Court's Liberal Justices."
- 97 See *White v. Davis*, 533 P.2d 222 (a spying program of the Los Angeles Police Department, which infiltrated UCLA courses and organizations to create dossiers on students and professors, constituted a prima facie violation of the explicit right of privacy; the amendment "does not purport to prohibit all incursion into individual privacy" but "any such intervention must be justified by a compelling interest.").
- 98 Ozer, "Golden State Sword," 1006-1014.
- 99 Ozer, "Golden State Sword," 1040-1045.
- 100 *White v. Davis* at 679-80 (Mosk, J., dissenting).
- 101 *White v. Davis* at 704 (Mosk, J., dissenting).
- 102 "Tribute to Alan F. Westin," *Patient Privacy Rights*, February 22, 2013, <https://patientprivacyrights.org/tribute-alan-f-westin.html>.
- 103 Alan F. Westin, "Databanks in a Free Society: A Summary of The Project on Computer Databanks," in *Privacy, A Public Concern: A Resource Document*, ed. Kent Larson (Washington, DC: US Government Print Office, 1975), 13-14, 122-128, <https://files.eric.ed.gov/fulltext/ED128007.pdf>.
- 104 Westin, "Databanks in a Free Society," 128.
- 105 Westin and Baker, *Databanks in a Free Society*, xiii.
- 106 Westin and Baker, *Databanks in a Free Society*, xiii.
- 107 Westin and Baker, *Databanks in a Free Society*, 345.
- 108 Westin, "Databanks in a Free Society," 125.
- 109 Westin, "Databanks in a Free Society," 124.
- 110 Westin and Baker, *Databanks in a Free Society*, xiii.
- 111 Mary Kay Kane is one of the trailblazing women in legal education and early privacy and social science research. After graduating from law school, Kane became co-director, with her mentor Arthur Miller, of a National Science Foundation project on privacy and social science research data. She joined the UC Law SF faculty in 1977, where she was the first ladder-ranked woman faculty member. She went on to serve as Chancellor and Dean, a position she held until 2006. UC Law San Francisco, "Mary Kay Kane, 1946-2021," June 3, 2021, [www.uclawsf.edu/2021/06/03/mary-kay-kane-1946-2021/](http://www.uclawsf.edu/2021/06/03/mary-kay-kane-1946-2021/).
- 112 Mary Kay Kane, "Data Banks in a Free Society. By Alan F. Westin and Michael A. Baker. Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems," *Buffalo Law Review* 24, no. 2 (1974): 331-339, <https://digitalcommons.law.buffalo.edu/buffalolawreview/vol24/iss2/5>.
- 113 James B. Rule, et al., *The Politics of Privacy* (Amsterdam: Elsevier, 1980), 73, 80, 101-10.
- 114 James B. Rule, et al., *The Politics of Privacy*, 73, 80, 101-10
- 115 Privacy Protection Study Commission, Introduction to "Personal Privacy in an Information Society."
- 116 "Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems," *Electronic Privacy Information Center*, July 1973, <https://epic.org/privacy/hew1973report/>.
- 117 Its members included both men and women, African American and Latinx members, spanning California to Oklahoma, Tennessee to Puerto Rico, and who worked in local, state, and federal agencies, industry, were elected officials, and academics from numerous disciplines. See *Biographical Notes on Members of the Secretary's Advisory Committee on Automated Personal Data Systems*, "Records, Computers and the Rights of Citizens."
- 118 The HEW Committee was asked to analyze and make recommendations about: (1) harmful consequences that may result from using automated personal data systems; (2) safeguards that might protect against potentially harmful consequences; (3) measures that might afford redress for any

harmful consequences; and (4) a more specific inquiry about policy and practice relating to the issuance and use of Social Security numbers. HEW Committee, "Records, Computers and the Rights of Citizens."

119 HEW Committee, Preface to "Records, Computers and the Rights of Citizens."

120 HEW Committee, Preface to "Records, Computers and the Rights of Citizens."

121 HEW Committee, "Records, Computers and the Rights of Citizens."

122 Chris Jay Hoofnagle, "The Origin of Fair Information Practices: Archive of the Meetings of the Secretary's Advisory Committee on Automated Personal Data Systems (SACAPDS)," UC Berkeley Center for Law and Technology, <https://www.law.berkeley.edu/research/bclt/research/privacy-at-bclt/archive-of-the-meetings-of-the-secretarys-advisory-committee-on-automated-personal-data-systems-sacapds/>, Accessed May 7, 2025.

123 Hoofnagle, "The Origin of Fair Information Practices," 74.

124 Hoofnagle, "The Origin of Fair Information Practices," 211.

125 HEW Committee member, Juan Anglero, from Puerto Rico, discussed that "one of our recommendations could be not to have so much information." He noted that "there should be some kind of rationale, some kind of system design behind it and not having been able to see in any of these presentations that we have had here, the rationale . . . whenever we talk about this, we talk about procedures, we talk about processes. . . . I would like for someone to tell me why the information is gathered and the use being given to that information because that is the only way I think or one of the few ways that we will be able to determine the kind of information to be gathered and where should it be kept." Hoofnagle, "The Origin of Fair Information Practices."

126 Department of Health, Education, and Welfare (HEW), "Transcript of Proceedings for Secretary's Advisory Committee on Automated Personal Data Systems," 1972, 116-117 [https://www.law.berkeley.edu/files/HEW/HEW\\_transcript\\_08171972.pdf](https://www.law.berkeley.edu/files/HEW/HEW_transcript_08171972.pdf) (statement of Professor Joseph Weizenbaum).

127 Department of Health, Education, and Welfare (HEW), "Transcript of Proceedings for Secretary's Advisory Committee on Automated Personal Data Systems Part 2," 1972, 29, [https://www.law.berkeley.edu/files/HEW/HEW\\_transcript\\_05191972.pdf](https://www.law.berkeley.edu/files/HEW/HEW_transcript_05191972.pdf), (statement of Mr. Kenneth McLean).

128 HEW Committee, "Transcript of Proceedings for Secretary's Advisory Committee on Automated Personal Data Systems Part 2," 178.

129 HEW Committee, "Records, Computers and the Rights of Citizens Report."

130 "FTC Fair Information Practice," Wikipedia, [https://en.wikipedia.org/wiki/FTC\\_fair\\_information\\_practice](https://en.wikipedia.org/wiki/FTC_fair_information_practice), Accessed May 7, 2025.

131 The HEW Committee recommendations did include more robust limitations on the collection and use of social security numbers. HEW Committee, "Transcript of Proceedings for Secretary's Advisory Committee on Automated Personal Data Systems."

132 "Safeguards for Privacy, Records, Computers and the Rights of Citizens Report of the Secretary's Advisory Committee on Automated Personal Data Systems," Electronic Privacy Information Center, July, 1973, <https://epic.org/privacy/hew1973report/.pdf>

133 "Safeguards for Privacy, Records, Computers and the Rights of Citizens Report," 220.

134 Willis H. Ware, interview by Jeffrey R. Yost, August 11, 2003, <https://conservancy.umn.edu/bitstream/handle/11299/107703/oh356ww.pdf>.

135 The FIPs established five key minimum standards, including transparency, individual access and correction rights, limits on secondary use, and organizational accountability. Preface, "Records, Computers and the Rights of Citizens."

136 Preface, "Records, Computers and the Rights of Citizens."

137 Fred H. Cate, "The Failure of Fair Information Practice Principles," *Consumer Protection in the Age of the Information Economy* (2006), [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1156972](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972).

138 Cate, "The Failure of Fair Information Practice Principles."

139 Gellman, *Fair Information Practices*, 56.

140 Marc Rotenberg, "Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)," *Stanford Technology Law Review* 1 (2001), <https://journals.law.stanford.edu/sites/default/files/stanford-technology-law-review/online/rotenberg-fair-info-practices.pdf> (summarizing Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified as amended at 5 U.S.C.A. § 552a)).

141 United States Privacy Protection Study Commission, "Introduction in Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission," 1977, <https://archive.epic.org/privacy/ppsc1977report/c1.htm>.

142 Robert Ellis Smith, "Gerald Ford: Privacy's Godfather," *Forbes*, January 5, 2007, [https://www.forbes.com/2007/01/04/privacy-protection-ford-oped-cx\\_res\\_0105privacy.html](https://www.forbes.com/2007/01/04/privacy-protection-ford-oped-cx_res_0105privacy.html).

143 Privacy Protection Study Commission, "Introduction in Personal Privacy in an Information Society."

144 The overall Commission was only seven people. It was both much smaller and far less diverse than the HEW Committee. It was all men, appears to have had no members of color, and was largely comprised of elected officials and individuals related to business. Appendix 4, Privacy Protection Study Commission, "Introduction in Personal Privacy in an Information Society."

145 Privacy Protection Study Commission, "Introduction in Personal Privacy in an Information Society."

146 The only privacy-related law that did move forward during the Carter administration was the enactment of the Right to Financial Privacy Act in

1978. This law responded to the *United States v. Miller* case, and slightly augmented statutory privacy rights to protect against government access to financial records. Gellman, *Fair Information Practices*, 15.
- 147 James Waldo, Herbert S. Lin, & Lynette I. Millett, eds, “Engaging Privacy and Information Technology in a Digital Age,” *National Academy of Sciences, Engineering, and Medicine*, 2007, 155-174, <https://nap.nationalacademies.org/catalog/11896/engaging-privacy-and-information-technology-in-a-digital-age>.
- 148 Barocas and Nissenbaum, “On Notice.”
- 149 Paul M. Schwartz, “Privacy and Democracy in Cyberspace,” *Vanderbilt Law Review* 52, no. 6 (1999): 1607–1701, <https://scholarship.law.vanderbilt.edu/vlr/vol52/iss6/2/>.
- 150 Richards and Hartzog, “The Pathologies of Digital Consent.”
- 151 Solove, “Murky Consent,” 593.
- 152 Zuboff, *The Age of Surveillance Capitalism*.
- 153 Turow, Lelkes, Draper and Waldman, “Americans Can’t Consent to Companies’ Use of Their Data.”
- 154 “16th Annual BCLT Privacy Lecture: Murky Consent.” Berkeley Center for Law & Technology, September 22, 2023, [www.law.berkeley.edu/research/bclt/bclt/events/16th-annual-bclt-privacy-lecture/](http://www.law.berkeley.edu/research/bclt/bclt/events/16th-annual-bclt-privacy-lecture/); see also Solove, “Murky Consent,” 631–632 (“Privacy consent is inescapably fictional”; “[i]n most situations involving technology and personal data, consent can never truly be meaningful, and the law is making things worse by pretending that it is.”).
- 155 Turow, Lelkes, Draper and Waldman, “Americans Can’t Consent to Companies’ Use of Their Data,” 4; see also Richards and Hartzog, “The Pathologies of Digital Consent.”
- 156 Richards and Hartzog, “The Pathologies of Digital Consent,” 1461–1462.
- 157 Daniel J. Solove, “Privacy Self-Management and the Consent Dilemma,” *Harvard Law Review* 126, no. 7 (2013): 1880-1894.
- 158 “U.S. Chamber of Commerce AI Principles,” US Chamber of Commerce, [www.uschamber.com/assets/archived/images/chamber\\_ai\\_principles\\_-\\_general.pdf](http://www.uschamber.com/assets/archived/images/chamber_ai_principles_-_general.pdf), Accessed June 8, 2025.
- 159 “U.S. Chamber of Commerce AI Principles.”
- 160 It only articulates that businesses should be transparent about the collection, use, and sharing of consumer data and provide consumers with clear privacy notices that businesses will honor and some support for narrow risk-based data security and breach notification provisions. “U.S. Chamber of Commerce Privacy Principles,” US Chamber of Commerce, September 6, 2018, [www.uschamber.com/assets/archived/images/9.6.18\\_us\\_chamber\\_-\\_ctec\\_privacy\\_principles.pdf](http://www.uschamber.com/assets/archived/images/9.6.18_us_chamber_-_ctec_privacy_principles.pdf).
- 161 Matt Cagle, Nicole Ozer, and Carmen-Nicole Cox, “ACLU Comment on GenAI Executive Order,” ACLU of Northern California, May 6, 2024, [www.aclunc.org/sites/default/files/ACLU%20Comment%20on%20GenAI%20Executive%20Order.pdf](http://www.aclunc.org/sites/default/files/ACLU%20Comment%20on%20GenAI%20Executive%20Order.pdf).
- 162 Marshall Ganz, *People, Power, Change: Organizing for Democratic Renewal* (Oxford UK: Oxford University Press, 2024); see also *Supporting a Movement for Health and Health Equity: Lessons from Social Movements: Workshop* (Washington DC: National Academies Press, 2014).
- 163 Nicole Ozer, “Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change,” *NYU Review of Law & Social Change* 36 (2012): 215-240, <https://socialchangenyu.com/review/putting-online-privacy-above-the-fold-building-a-social-movement-and-creating-corporate-change/>.
- 164 I helped develop and lead the face surveillance campaign, along with Staff Attorneys Matt Cagle and Jake Snow, at the ACLU of Northern California, and Technology and Liberty Directors at the ACLU of Washington and ACLU of Massachusetts. It later also became nationwide campaign work of the ACLU. See Nicole Ozer, Kate Ruane, and Matt Cagle, “Grassroots Activists are Leading the Fight to Stop Face Recognition,” ACLU, June 17, 2021, [www.aclu.org/news/privacy-technology/grassroots-activists-are-leading-the-fight-to-stop-face-recognition-its-time-for-congress-to-step-up-too](http://www.aclu.org/news/privacy-technology/grassroots-activists-are-leading-the-fight-to-stop-face-recognition-its-time-for-congress-to-step-up-too).
- 165 Matt Cagle and Nicole Ozer, “Amazon Teams with Government to Deploy Dangerous New Surveillance Technologies,” ACLU, May 22, 2018, [www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new](http://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-teams-government-deploy-dangerous-new).
- 166 “Pressure Mounts on Amazon, Microsoft, and Google Against Selling Facial Recognition to Government,” ACLU, January 15, 2019, [www.aclu.org/news/privacy-technology/pressure-mounts-on-amazon-microsoft-and-google-against-selling-facial-recognition-to-government](http://www.aclu.org/news/privacy-technology/pressure-mounts-on-amazon-microsoft-and-google-against-selling-facial-recognition-to-government).
- 167 Larry Hardesty, “Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems,” MIT News, February 11, 2018, [news.mit.edu/2023/study-finds-gender-skin-type-bias-commercial-ai-systems-0211](http://news.mit.edu/2023/study-finds-gender-skin-type-bias-commercial-ai-systems-0211).
- 168 Woodrow Hartzog, “Facial Recognition Is the Perfect Tool for Oppression,” Stanford Center for Internet and Society, August 2, 2018, <https://cyberlaw.stanford.edu/publications/facial-recognition-perfect-tool-oppression/>.
- 169 “The Fight to Stop Face Recognition Technology,” ACLU, June 7, 2023, <https://www.aclu.org/news/topic/stopping-face-recognition-surveillance>.
- 170 Becca Cramer-Mowder, “Once Again, California Refused to Endorse Face Surveillance. Now it’s Time to Ban it,” ACLU of Northern California, August 21, 2024, <https://www.aclunc.org/blog/once-again-california-refused-endorse-face-surveillance-now-it-s-time-ban-it>.

- 171 Lucy Bernholz, Nicole Ozer, Kip Wainscott, and Wren Elhai, "Integrated Advocacy: Paths Forward for Digital Civil Society," Stanford Center on Philanthropy and Civil Society (PACS), January 2020, 3, <https://pacscenter.stanford.edu/publication/integrated-advocacy-paths-forward-for-digital-civil-society/>.
- 172 Lori McGlinchey, "Lessons from the Table: Civil Rights, Technology, and Privacy," Ford Foundation, November 12, 2019, <https://www.fordfoundation.org/work/learning/learning-reflections/lessons-from-the-table-civil-rights-technology-and-privacy/>.
- 173 I developed the Bay Area Tech Table (BATT) with Nathan Sheard of the Electronic Frontier Foundation and James Burch of the Anti-Police Terror Project.
- 174 "Home," RightsCon, <https://www.rightscon.org/>, Accessed June 8, 2025.
- 175 "Privacy Law Scholars Conference," PLSC, <https://privacyscholars.org/>, Accessed June 8, 2025.
- 176 "Technology and Human Rights Fellowship," Carr-Ryan Center for Human Rights, <https://www.hks.harvard.edu/centers/carr/opportunities/fellowship-opportunities/technology-and-human-rights-fellowship>, Accessed June 8, 2025.
- 177 Sidney Tarrow, *Power in Movement: Social Movements and Contentious Politics* (Cambridge, UK: Cambridge University Press, 1998), 5-6.
- 178 Ozer, "Golden State Sword," 990; Bernholz, Ozer, Wainscott, and Elhai, "Integrated Advocacy: Paths Forward for Digital Civil Society"; see Scott L. Cummings, "Movement Lawyering," *University of Illinois Law Review* 2017, no. 5 (2017): 1645, [ssrn.com/abstract=3067562](https://ssrn.com/abstract=3067562).
- 179 "Fighting High-Tech Government Surveillance," ACLU of Northern California, <https://www.aclunc.org/fighting-high-tech-government-surveillance>, Accessed June 8, 2025; see also Ozer, Ruane, and Cagle, "Grassroots Activists are Leading the Fight to Stop Face Recognition"; "The Fight to Stop Face Recognition Technology."
- 180 Cummings, "Movement Lawyering," 1703.
- 181 Cummings, "Movement Lawyering," 1715.
- 182 National Academies Press, *Lessons from Social Movements*.
- 183 "Public Interest Technology University Network," Wikipedia, [https://en.wikipedia.org/wiki/Public\\_Interest\\_Technology\\_University\\_Network](https://en.wikipedia.org/wiki/Public_Interest_Technology_University_Network), Accessed June 8, 2025.
- 184 "Public Interest Technology University Network 2019-2024," PIT-UN, <https://pit-un.org/2019-2024/>, Accessed June 8, 2025.
- 185 Twenty-five members of Congress, including Representative John Lewis, wrote to Jeff Bezos demanding a meeting to discuss Amazon's face surveillance product and civil rights. See Jimmy Gomez, "Rep. Jimmy Gomez Leads Bipartisan Letter to Jeff Bezos Expressing Civil Rights Concerns About Amazon's Facial Recognition Technology," *United States Representative Jimmy Gomez*, July 27, 2018, <https://gomez.house.gov/news/documentsingle.aspx?DocumentID=371>. Senators Wyden, Booker, and Markey sent a letter to thirty-nine federal law-enforcement agencies seeking information about their use of facial recognition. Ron Wyden, "Wyden, Booker, Markey Question 39 Federal Law-Enforcement Agencies About Facial Recognition Policies," *United States Senator Ron Wyden*, July 27, 2018, <https://www.wyden.senate.gov/news/press-releases/wyden-booker-markey-question-39-federal-law-enforcement-agencies-about-facial-recognition-policies>; Ed Markey, "After False Matches by Facial Recognition Technology, Senator Markey and Representatives Gutiérrez, DeSaulnier Question Amazon About its Sale of 'Rekognition' to Law Enforcement," *United States Senator Ed Markey*, July 26, 2018, <https://www.markey.senate.gov/news/press-releases/after-false-matches-by-facial-recognition-technology-senator-markey-and-representatives-gutierrez-desaulnier-question-amazon-about-its-sale-of-rekognition-to-law-enforcement>.
- 186 Ozer, Ruane and Cagle, "Grassroots Activists are Leading the Fight to Stop Face Recognition."
- 187 The Body Camera Accountability Act (AB 1215), ACLU of Northern California, <https://www.aclunc.org/our-work/legislation/body-camera-accountability-act-ab-1215>, Accessed June 8, 2025.
- 188 "In Big Win, Settlement Ensures Clearview AI Complies With Groundbreaking Illinois Biometric Privacy Law," ACLU, May 9, 2022, <https://www.aclu.org/press-releases/big-win-settlement-ensures-clearview-ai-complies-with-groundbreaking-illinois>.
- 189 "Williams v. City of Detroit," ACLU, <https://www.aclu.org/cases/williams-v-city-of-detroit-face-recognition-false-arrest>, Accessed June 8, 2025.
- 190 Ozer, Ruane, and Cagle, "Grassroots Activists are Leading the Fight to Stop Face Recognition."
- 191 "Statement of Commissioner Alvaro M. Bedoya On FTC v. Rite Aid Corporation & Rite Aid Headquarters Corporation Commission," *United States Federal Trade Commission*, December 19, 2023, [www.ftc.gov/system/files/ftc\\_gov/pdf/2023190\\_commissioner\\_bedoya\\_riteaid\\_statement.pdf](http://www.ftc.gov/system/files/ftc_gov/pdf/2023190_commissioner_bedoya_riteaid_statement.pdf); "Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards," *United States Federal Trade Commission*, December 19, 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without>.
- 192 Ganz, *People, Power, Change*.
- 193 Naomi Klein and Astra Taylor, "The Rise of End Times Fascism," *The Guardian*, April 13, 2025, <https://www.theguardian.com/us-news/ng-interactive/2025/apr/13/end-times-fascism-far-right-trump-musk>.
- 194 "Privacy and Technology," ACLU of Northern California, [www.aclunc.org/tech](http://www.aclunc.org/tech), Accessed June 8, 2025; "Building a Just Digital Age," ACLU of Northern California, <https://www.aclunc.org/building-just-digital-age>, Accessed June 8, 2025.
- 195 "Who We Are," MediaJustice, [www.mediajustice.org/who-we-are/](http://www.mediajustice.org/who-we-are/), Accessed June 8, 2025.

- 196 “Fight for the Future,” Fight for the Future, [www.fightforthefuture.org/](http://www.fightforthefuture.org/), Accessed June 8, 2025.
- 197 “What We’re Fighting For,” Athena, <https://athenaforall.org/#s1>, Accessed June 8, 2025.
- 198 “#NoTechforICE.” No Tech for ICE, [www.notechforice.com/](http://www.notechforice.com/), Accessed June 8, 2025.
- 199 Graham Boyd, “The Drug War: The New Jim Crow,” ACLU, July 31, 2001, [www.aclu.org/documents/drug-war-new-jim-crow](http://www.aclu.org/documents/drug-war-new-jim-crow).
- 200 Cagle, Ozer, and Hirsch, “Seeing Through Surveillance.”
- 201 Susan N. Herman, “Ordinary Americans and the War on Terror,” ACLU, September 20, 2011, [www.aclu.org/news/national-security/ordinary-americans-and-war-terror](http://www.aclu.org/news/national-security/ordinary-americans-and-war-terror).
- 202 Daniel J. Solove, “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy,” *San Diego Law Review* 44, no. 4 (2007), [https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1159&context=faculty\\_publications](https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1159&context=faculty_publications).
- 203 Anna Wiener, “Does Tech Need a New Narrative?” *The New Yorker*, June 15, 2021, <https://www.newyorker.com/news/letter-from-silicon-valley/does-tech-need-a-new-narrative>.
- 204 John Naughton, “Power and Progress Review – Why the Tech-Equals-Progress Narrative Must Be Challenged,” *The Guardian*, May 7, 2023, [www.theguardian.com/books/2023/may/07/power-and-progress-daron-acemoglu-simon-johnson-review-formidable-demolition-of-the-technology-equals-progress-myth](http://www.theguardian.com/books/2023/may/07/power-and-progress-daron-acemoglu-simon-johnson-review-formidable-demolition-of-the-technology-equals-progress-myth).
- 205 “Records, Computers and the Rights of Citizens.”
- 206 Privacy Protection Study Commission, “Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission,” 1977, <https://archive.epic.org/privacy/ppsc1977report/c1.htm>.
- 207 Mark Zuckerberg, “Founder’s Letter, 2012,” Facebook, 2012, [https://m.facebook.com/nt/screen/?params=%7B%22note\\_id%22%3A261129471966151%7D&path=%2Fnotes%2Fnote%2F&refsrc=deprecated&\\_rdr](https://m.facebook.com/nt/screen/?params=%7B%22note_id%22%3A261129471966151%7D&path=%2Fnotes%2Fnote%2F&refsrc=deprecated&_rdr).
- 208 Ryan Mac, Charlie Warzel, and Alex Kantrowitz, “Growth at Any Cost: Top Facebook Executive Defended Data Collection in 2016 Memo,” *BuzzFeed News*, March 29, 2018, [www.buzzfeednews.com/article/ryanmac/growth-at-any-cost-top-facebook-executive-defended-data](http://www.buzzfeednews.com/article/ryanmac/growth-at-any-cost-top-facebook-executive-defended-data). Facebook’s long-time executive, Andrew Bosworth, wrote an internal memo saying “[t]he ugly truth is that we believe in connecting people so deeply that anything that allows us to connect more people more often is de facto good. . . . Maybe it costs a life by exposing someone to bullies. Maybe someone dies in a terrorist attack coordinated on our tools. And still we connect people. . . . That’s why all the work we do in growth is justified. All the questionable contact importing practices. All the subtle language that helps people stay searchable by friends. All of the work we do to bring more communication. . . .”
- 209 Naughton, “Power and Progress Review.”
- 210 Committee on the Judiciary, Subcommittee on Constitutional Rights, “Federal Data Banks, Computers, and the Bill of Rights,” 10–16.
- 211 “Creative destruction” is a phrase popularized by Joseph Schumpeter, one of the most influential economists of the early 20th century. “Joseph Schumpeter,” *Wikipedia*, [en.wikipedia.org/wiki/Joseph\\_Schumpeter](http://en.wikipedia.org/wiki/Joseph_Schumpeter), Accessed June 8, 2025; see also Naughton, “Power and Progress Review.”
- 212 Letter by Kenneth Cory to the ACA 51 Legislative File, ACLU of Northern California, 1972, [www.aclunc.org/sites/default/files/Letter%20Response%20to%20Chairman%20Ignazio%20Vella%20from%20Hon.%20Kenneth%20Cory.pdf](http://www.aclunc.org/sites/default/files/Letter%20Response%20to%20Chairman%20Ignazio%20Vella%20from%20Hon.%20Kenneth%20Cory.pdf).
- 213 Colleen McClain, Michelle Faviero, Monica Anderson, and Eugenie Park, “How Americans View Data Privacy,” *Pew Research Center*, October 18, 2023, <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/>.
- 214 Turow, Lelkes, Draper, and Waldman, “Americans Can’t Consent to Companies’ Use of Their Data,” 13.
- 215 “ACLU Statement on Amazon Face Recognition Moratorium,” *American Civil Liberties Union*, June 10, 2020, [www.aclu.org/press-releases/aclu-statement-amazon-face-recognition-moratorium](http://www.aclu.org/press-releases/aclu-statement-amazon-face-recognition-moratorium).
- 216 Josh Taylor, “Rise of Artificial Intelligence Is Inevitable but Should Not Be Feared, Father of AI Says,” *The Guardian*, May 6, 2023, [www.theguardian.com/technology/2023/may/07/rise-of-artificial-intelligence-is-inevitable-but-should-not-be-feared-father-of-ai-says](http://www.theguardian.com/technology/2023/may/07/rise-of-artificial-intelligence-is-inevitable-but-should-not-be-feared-father-of-ai-says).
- 217 Daniel Shapiro, “Artificial Intelligence: It’s Complicated and Unsettling, but Inevitable,” *Forbes*, September 10, 2019, [www.forbes.com/sites/danielshapiro1/2019/09/10/artificial-intelligence-its-complicated-and-unsettling-but-inevitable/?sh=66f90b6d26f2](http://www.forbes.com/sites/danielshapiro1/2019/09/10/artificial-intelligence-its-complicated-and-unsettling-but-inevitable/?sh=66f90b6d26f2).
- 218 Margaret Heffernan, “The Myth of Inevitability,” *A Point of View*, BBC, October 11, 2019, [www.bbc.co.uk/sounds/play/m0009522](http://www.bbc.co.uk/sounds/play/m0009522).
- 219 Heffernan, “The Myth of Inevitability.”
- 220 Heffernan, “The Myth of Inevitability.”
- 221 “Nicole Ozer,” *Stanford PACS Center*, [pacscenter.stanford.edu/person/nicole-ozier/](http://pacscenter.stanford.edu/person/nicole-ozier/), Accessed June 8, 2025.
- 222 Shara Tibken, “Some Senators in Congress Just Don’t Get Facebook and Mark Zuckerberg,” *CNET*, April 11, 2018, [www.cnet.com/news/politics/](http://www.cnet.com/news/politics/)

some-senators-in-congress-capitol-hill-just-dont-get-facebook-and-mark-zuckerberg/.

223 U.S. Chamber Staff, "Americans Think AI Is 'Inevitable' but Aren't Sure Exactly What It Is," US Chamber of Commerce, October 4, 2017, [www.uschamber.com/technology/americans-think-ai-inevitable-aren-t-sure-exactly-what-it](http://www.uschamber.com/technology/americans-think-ai-inevitable-aren-t-sure-exactly-what-it).

224 Arvin Narayanan and Sayash Kapoor, "Tech Policy Is Only Frustrating 90% of the Time," AI Snake Oil, April 3, 2024, [www.aisnakeoil.com/p/tech-policy-is-only-frustrating-90](http://www.aisnakeoil.com/p/tech-policy-is-only-frustrating-90).

225 Letter to Jeffrey Bezos Regarding Amazon Rekognition, Congressional Black Caucus, May 21, 2018, [cbc.house.gov/uploadedfiles/final\\_cbc\\_amazon\\_facial\\_recognition\\_letter.pdf](http://cbc.house.gov/uploadedfiles/final_cbc_amazon_facial_recognition_letter.pdf).

226 Matt Day, "Amazon Officials Pitched Their Facial Recognition Software to ICE," The Seattle Times, October 21, 2018, [www.seattletimes.com/business/amazon/amazon-officials-pitched-their-facial-recognition-software-to-ice/](http://www.seattletimes.com/business/amazon/amazon-officials-pitched-their-facial-recognition-software-to-ice/); see also Nicole Ozer, "Amazon, Google, and Microsoft Are at Odds on the Dangers of Face Recognition. One of Them Is on the Right Path.," ACLU, January 25, 2019, <https://www.aclu.org/news/privacy-technology/amazon-google-and-microsoft-are-odds-dangers-face>.

227 Kate Conger, "Amazon Workers Demand Jeff Bezos Cancel Face Recognition Contracts," Gizmodo, June 21, 2018, [gizmodo.com/amazon-workers-demand-jeff-bezos-cancel-face-recognition-1827037509](http://gizmodo.com/amazon-workers-demand-jeff-bezos-cancel-face-recognition-1827037509).

228 Aaron Horvath, "Philanthropy by the Numbers, Measurable Impact and its Civic Discontents," The Hedgehog Review, Fall 2024, <https://hedgehogreview.com/issues/in-need-of-repair/articles/philanthropy-by-the-numbers>.

229 National Academies Press, *Lessons from Social Movements*.

230 McGlinchey, "Lessons from the Table."

231 "Building Translocal, Transnational, Interdependent Community-Level Social and Ecological Justice," CS Fund, <https://csfund.org/just-transitions>, Accessed June 8, 2025.

232 BATT's tiered support structure responds to a need identified by a year-long research study conducted by the Stanford Digital Civil Society Lab and helps to maximize the use of available resources to broaden the people and organizations who feel confident engaging in public interest technology work across strategy. Bernholz, Ozer, Wainscott, and Elhai, "Integrated Advocacy: Paths Forward for Digital Civil Society," 3.

233 Cummings, "Movement Lawyering," 1703.

234 Cummings, "Movement Lawyering," 1703.

235 Marshall Ganz, "Leading Change: Leadership, Organization, and Social Movements," in *Handbook of Leadership Theory and Practice*, ed. Nitin Nohria and Rakesh Khurana (Brighton, MA: Harvard Business School Press, 2010), 509-550.

**Carr-Ryan Center for Human Rights  
Harvard Kennedy School  
79 JFK Street  
Cambridge, MA 02138**

Statements and views expressed in this report are solely those of the author and do not imply endorsement by Harvard University, the Harvard Kennedy School, or the Carr-Ryan Center for Human Rights.

Copyright 2025, President and Fellows of Harvard College  
Printed in the United States of America

---

This publication was published by the Carr-Ryan Center  
for Human Rights at the John F. Kennedy  
School of Government at Harvard University

Copyright 2025, President and Fellows of Harvard College  
Printed in the United States of America



[hks.harvard.edu/centers/carr-ryan](https://hks.harvard.edu/centers/carr-ryan)

79 JFK Street | Cambridge, MA 02138  
[carr-ryan-center@hks.harvard.edu](mailto:carr-ryan-center@hks.harvard.edu)