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

Nicole A. Ozer[†]

ABSTRACT

The importance of state law and constitutions to protect and promote rights has become even more salient given the reality of a U.S. Supreme Court that is increasingly hostile to privacy and other civil rights. As we face a period of both critical social justice fights and rapid technological change, now is the time to ensure that the California constitutional right to privacy is widely understood and to fight for it to be used as robustly as intended to defend and advance rights, justice, and democracy in the modern digital age.

The California constitutional right to privacy was forged by intersectional social justice movements and integrated advocacy and passed by the voters in 1972 to be a modern right to privacy—to equally address both informational privacy and autonomy privacy and protect against privacy intrusions by both government and private parties. 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 it clear that the California constitutional right to privacy was passed to give people the power in how privacy questions were resolved in the modern digital age.

But this Golden State Sword of the California constitutional right to privacy has been largely latent for the past thirty years, not being used to its full potential to protect against government surveillance and surveillance business models. This Article tells an important story about how the clarion call that the Privacy Amendment's passage served on the courts and policymakers has been improperly muted in recent decades, and how it must now regain its full strength to really work for the people.

This Article contributes to the literature in three ways. First, it recontextualizes the historical and legislative history of the California constitutional right to privacy and how it can inform innovative strategies to drive justice in the digital age. Second, it contributes deep legal

DOI: https://doi.org/10.15779/Z384Q7QR5W

† Nicole A. Ozer is the Technology and Civil Liberties Director at the ACLU of Northern California and a 2024–2025 Technology and Human Rights Fellow at the Carr Center at the Harvard Kennedy School. Affiliation for identification purposes only. This Article is written in the author's individual capacity and represents solely the views of its author. Thank you to Dorothy Ehrlich, Matt Cagle, Jake Snow, Nick Hidalgo, Ellen Gunn, and Noosha Aliabadi for helpful input on this article.

and policy analysis of the successes and failures in using the constitutional right to privacy to defend and promote rights in the digital age and assesses the sociopolitical climate that has influenced these opportunities and challenges. Finally, it charts a path forward for what should happen in the courts and legislature to fully respect the fundamental right to privacy and properly protect rights, justice, and democracy in the modern digital age.

TABLE OF CONTENTS

I. INTRODUCTION

We are at a crossroads. Surveillance has been allowed to run rampant in recent decades—an alliance between government and company profit that has led to heavy costs to rights, safety, and democracy in the modern digital age. Our lives are already shaped by the way technology is built and used; the growth of artificial intelligence will only amplify technology's power to affect equity, access, and justice, especially for already marginalized communities. Social movements must fight for justice on new terrain, where barriers to freedom and opportunity are now both structural and digital. This current period of technological change is happening at a time when reproductive rights and LGBTQ rights, racial justice, and the very fabric of American democracy and rule of law is under assault. Whether technology helps or hinders struggles for freedom and justice depends on decisions about why it is built and how it can be used, which are being made today by companies, communities, policymakers, and the courts. 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.

The California constitutional right to privacy, the first in the nation, was passed by a wide margin of voters in November 1972. This fundamental right to privacy was born of intersectional movement activism and integrated advocacy,[1] forged at a time when diverse Californians viscerally understood the implications of surveillance on movements for justice and could not trust that the federal government would protect their rights, bodies, or lives. The

1. "Integrated Advocacy" is a term used to describe a movement lawyering approach that considers and strategically leverages and layers diverse strategies, both within and outside of formal lawmaking arenas, to both build momentum and better support long-term social change. *See* additional discussion *infra* Part II.

Privacy Amendment created an inalienable right to privacy, and it also ensured that all fundamental rights were equally extended to every person in California, by adding three words to Article I, Section 1 of the California Constitution, replacing the word, "men," with "people," and inserting "and privacy."[2] The right to privacy equally addressed both informational privacy and autonomy privacy.[3] It also protected against privacy intrusions by government and business, with its "moving force" 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."[4]

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 in how privacy questions were resolved in the digital age. As California Assemblymember Kenneth Cory, the legislative author of the amendment, discussed, "[t]he concern that our privacy is increasingly becoming a mere myth and that individuals are powerless to control it led to the introduction of [the Privacy Amendment]."[5] Cory also observed that in the "era of computerized data banks [and] increased government surveillance . . . a clearer statement of our rights is needed."[6] As the ballot argument in support of the constitutional amendment further articulated, "[a]t present there are no

2. 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." CAL. CONST. art. I, § 1.

3. There are many conceptions of privacy, but the California constitutional right to privacy is "the right to be left alone . . . . It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose." *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), at 26–27, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props. It equally recognizes privacy interests in what is generally considered to be informational privacy—interests in precluding both the dissemination or misuse of information—and autonomy privacy—interests in making intimate personal decisions or conducting personal activities without observation, intrusion, or interference. *See* Hill v. Nat'l Collegiate Athletic Assn., 865 P.2d 633 (Cal. 1994).

4. White v. Davis, 533 P.2d 222, 233 (Cal. 1975).

5. Letter from Kenneth Cory to the Legislative File, (1972), https://www.aclunc.org/sites/default/files/Letter%20Response%20to%20Chairman%20Ignazio%20Vella%20from%20Hon.%20Kenneth%20Cory.pdf.

6. *Id.*

effective restraints on the information activities of government and business."[7] The Privacy Amendment created a legally enforceable, inalienable right to privacy, which "should be abridged only when there is a compelling public need."[8] The passage of the Privacy Amendment built a constitutionally mandated baseline to protect privacy, and it placed the legal and policy burden on the government or business to demonstrate a compelling interest to override that fundamental right.

The California constitutional right to privacy reached a historic, fifty-year milestone in 2023—five decades since it was passed by the voters and went into effect.[9] Its anniversary was an important time to take stock of California privacy law, where it should be, and how to generate paths forward.[10]

We currently experience a modern digital world where the proliferation of surveillance capitalism,[11] its deep partnership with government surveillance, and the consolidation of power of the technology companies has externalized deep costs to both people and democracy. From the Cambridge Analytica scandal, to misinformation, to the health and safety concerns of families and children, it has become increasingly clear that individual rights and democracy have borne the costs of the "free" business models of surveillance capitalism. We experience a modern digital world where there is a startling disconnect between the constitutional privacy rights that Californians are guaranteed and the current reality of rampant surveillance.

The California Supreme Court issued strong early rulings in the 1970s and early 1980s like *White v. Davis*, which ensured that Californians could utilize the California constitutional right to both pursue and obtain privacy.[12] But with changes in the California Supreme Court in the "War on Drugs" era, the Court

7. *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), at 26–27, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props.

8. *Id.*

9. *Id.*

10. In October 2023, I worked with students to help spearhead a symposium at Berkeley Law School—*California Constitutional Privacy at 50: Power of State Law and Promoting Racial Justice in the Digital Age*. This symposium brought together more than 200 leading academics and practitioners to discuss the California constitutional right to privacy at age fifty and discuss new creative and intersectional uses of state constitutional rights to privacy to defend and promote justice in the modern digital age. This article was developed as a complement to the symposium. Recordings and other resources from the symposium are available at https://www.law.berkeley.edu/research/bclt/bcltevents/4th-annual-btlj-bclt-fall-symposium/.

11. Surveillance capitalism is a concept in political economics which denotes the widespread collection and commodification of personal information by corporations. *See generally*, SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (Jan. 15, 2019).

12. White v. Davis, 533 P.2d 222 (Cal. 1975).

did not continue to enforce the full reach of the constitutional right. The Court erected regrettable roadblocks in cases like *Hill v. NCAA* that made it difficult for Californians to utilize the fundamental privacy right for its intended purpose.[13]

California policymakers have also generally lost the thread of the California constitutional right to privacy. They have certainly been more productive than their federal counterparts in passing new privacy laws in recent decades. But California policymakers often fail to fully uphold the fundamental privacy rights of Californians and ensure that the onus is on government and business to justify a privacy invasion, rather than putting the burden on people to try to protect their rights. California policymakers often fail to support robust statutory interventions that truly help to operationalize the California constitutional right to privacy by preventing privacy invasions from ever occurring and ensuring that Californians are not forced to wait to go to court for redress. Instead, policymakers too often allow policy efforts to go forward that not only fail to prevent privacy harms, but often even seek to legalize or otherwise legitimize privacy invasions.

As we find ourselves again at a point of rapid technological change and critical social justice fights, now is the time to rectify these wrongs in the courts and legislature and fully revitalize the reach and intended power of the California constitutional right to privacy. Now is the time to ensure that this right to privacy is widely understood and to fight for this right to be used as robustly as intended to protect and promote rights, justice, and democracy in the digital age.

The California constitutional right to privacy—our Golden State Sword—can and should be protecting against government surveillance and surveillance business models and meet this moment of even greater threats to rights and democracy in the digital age. But this Golden State Sword has been largely latent for the past thirty years, and not been used to its full potential. Why? This fundamental right to privacy, forged by intersectional movements and through integrated advocacy, and passed with a clear purpose in the early 1970s, was unfortunately undermined by pressures of political and social forces. This Article tells this important story about how the clarion call that the Privacy Amendment's passage served on the courts and policymakers has been improperly muted in recent decades, and how it now must regain its full strength.

13. Hill v. Nat'l Collegiate Athletic Assn., 865 P.2d 633 (Cal. 1994); s*ee also* ACLU NEWS, VOL. 58, NO. 2, (Apr. 1994), https://digitallibrary.californiahistoricalsociety.org/object/17286; Rodolfo R. Aquino, *California's Constitutional Privacy Guarantee Needs a Reset*, SCOCABLOG (Apr. 9, 2021), https://scocablog.com/californias-constitutional-privacy-guarantee-needs-a-reset/.

This Article contributes to the literature in several ways. First, it contributes new analysis of the historical and legislative history of the California constitutional right to privacy. Second, it contributes deep legal and policy analysis of the successes and failures in using the constitutional right to privacy to defend and promote rights in the digital age and assessing the sociopolitical climate that has influenced these opportunities and challenges. Finally, it charts a path forward for what courts and policymakers need to do to fully respect the fundamental right to privacy and properly protect rights, justice, and democracy in the digital age.

Part II recontextualizes the historical and legislative record to understand how the explicit right to privacy in the California Constitution was developed and passed in 1972. It examines how the right was informed by intersectional justice movements and integrated advocacy and how it was intended to defend and support fundamental rights, justice, and democracy in the digital age. Understanding this history and identifying what we can learn from it is critical to building movement power and developing innovative strategies to drive real justice in the digital age.

Part III engages in a legal and policy analysis of the successes and failures in using the right to privacy. It explores how the political and business climate affected the trajectory of privacy law. It delves into how faulty premises and manufactured legal distinctions unsupported by the language and legislative history of the California constitutional right to privacy promulgated in the 1994 *Hill v. NCAA* case have kneecapped the force of the constitutional right and undermined how it was intended to protect rights and democracy in the digital age.

Part IV charts a path forward for ensuring that the California constitutional right to privacy can be used as robustly as intended to protect people and society in the modern digital age. It includes steps that can and should be taken by the courts and policymakers to fully respect the fundamental right to privacy; prevent the widespread collection, retention, and use of personal information by both government and business; and protect rights, justice, and democracy. California courts should carefully reexamine the 1994 *Hill* decision and ensure that Californians can actually obtain their fundamental right to privacy. Policymakers should both protect existing privacy rights from industry attacks like federal preemption and pass new, robust laws that prevent privacy intrusions.

II. HISTORY

A. CALIFORNIA CONSTITUTIONAL PRIVACY WAS DEEPLY CONNECTED TO INTERSECTIONAL SOCIAL JUSTICE AT THE DAWN OF THE MODERN DIGITAL AGE

The California constitutional right to privacy, the first such right in the nation, was drafted and passed in 1972. Both its origins and purpose are deeply connected to intersectional social justice and the fights for racial justice, gender justice, antiwar activism, and other important social movements. Many activists involved in these social movements had developed a very personal understanding about how the government and private actors could use surveillance to weaponize information about their private life. They viscerally recognized how already powerful actors could take advantage of new technology to attack and undermine social movements, protect the status quo and further expand government and corporate power, and criminalize gender, sexuality, and reproductive care. The years immediately surrounding the passage of the constitutional right to privacy were a particularly pivotal time for many of these intersectional movements and the growth of understanding of both activists and the general public about the power of technology to support or undermine these fights.

In March 1971, the Citizens' Commission to Investigate the FBI, a group of antiwar activists, broke into an FBI field office and left with more than a thousand documents.[14] These documents first publicly exposed the widespread secret surveillance of the FBI and its COINTELPRO program. The exposure of COINTELPRO confirmed what activists and others had suspected for years—there was widespread, unconstitutional wiretapping and other surveillance and infiltration intended to disrupt and sabotage activist leaders and movement groups engaged in protest, dissent and social change. Its targets included Martin Luther King Jr.,[15] the Black Panthers, the women's

14. *The Burglary That Exposed COINTELPRO: Activists Mark 50th Anniversary of Daring FBI Break-in* (Democracy Now! television broadcast Mar. 9, 2021), 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*, WASH. POST (Sept. 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 (Jan. 15, 2014), https://www.aclu.org/news/national-security/i-broke-fbi-office-and-took-every-document-heres-why.

15. *Federal Bureau of Investigation*, MARTIN LUTHER KING, JR. RSCH. & EDUC. INST., STAN. UNIV. (Mar. 16, 1909), https://kinginstitute.stanford.edu/federal-bureau-investigation-fbi#:~:text=In%20the%20following%20months%2C%20Hoover,SCLC)%20offices%20in%20October%201963; *Fresh Air: Documentary Exposes How FBI Tried to Destroy MLK With*

movement, LGBTQ leaders, Native American leaders, farm worker rights leaders, antiwar groups, and many other organizations and activists. The government surveillance of these movements and leaders was meant to infiltrate and undermine the immense energy to advance social change happening both within and amongst these movements in the 1960s and early 1970s. Many movement leaders and activists, including a significant number of activists based in California, personally experienced being surveilled by the government and understood how advances in technology could exacerbate these threats to movement work and personal safety.

At the time the California constitutional right to privacy was being developed and passed, movements for gender and reproductive justice were at a critical juncture and many of its activist leaders knew they were being heavily surveilled. Women's rights activists were working in high gear to enact the Equal Rights Amendment (ERA), which Congress passed in 1972 and then sent to the individual states for ratification.[16] In 1972, Ruth Bader Ginsburg founded the ACLU's Women's Rights Project and began its work to systematically break down the legal regime allowing sex discrimination and practices that denied true equality to women.[17] As gender activism was in full swing, many of the women's rights activists were under heavy surveillance.[18] A surveillance report on the Baltimore Liberation Movement that was sent not only to the FBI, but also to three military agencies, made it clear that the government had no legitimate purpose surveilling the women's rights activists. The surveillance reports on the activists had "nothing to do with violence, nothing to do with these labels of subversion and extremism."[19] Rather, the women's rights activists were focused on how to obtain "equal opportunities that men have in the working society," and not "being only a wife and mother."[20]

Wiretaps, Blackmail, NPR (Jan. 18, 2021), https://www.npr.org/2021/01/18/956741992/documentary-exposes-how-the-fbi-tried-to-destroy-mlk-with-wiretaps-blackmail.

16. *Equal Rights Amendment (ERA) of 1972*, NAT'L ARCHIVES FOUND. (1972), https://www.archivesfoundation.org/amendingamerica/equal-rights-amendment-era-of-1972/.

17. *FAQs: The ACLU Women's Rights Project and Women's History Month*, ACLU (2007), https://www.aclu.org/documents/faqs-aclu-womens-rights-project-and-womens-history-month; *About the ACLU Women's Rights Project*, ACLU (1996), https://www.aclu.org/documents/about-aclu-womens-rights-project.

18. Roberta Sapler, *U.S. Government Surveillance and the Women's Liberation Movement, 1968-1973: A Case Study*, 34 FEMINIST STUD. 431 (2008).

19. *Intelligence Activities, Senate Resolution 21, Hearings Before the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate*, U.S. SELECT COMM. ON INTEL., 94th Cong. 15 (1975).

20. *Id.*

The LGBTQ movement was also gaining important momentum in the same period and its activists were also under heavy surveillance. In June 1969, the Stonewall protest helped ignite a public LGBTQ movement. It was followed closely by a Halloween 1969 protest in San Francisco, where members of the Gay Liberation Front penned "Gay Power" messages around the city that brought additional important public attention. The 1970 march in New York to commemorate the one-year anniversary of Stonewall is considered America's first gay pride parade; gay pride marches also took place in Los Angeles, while the first "Gay-in" was held in San Francisco.[21] By 1972, Democratic presidential candidate George McGovern had endorsed gay rights.[22] San Francisco, California also became one of the first cities in the United States to pass a gay rights ordinance and prohibit employment discrimination based on sexual orientation by the city and by companies doing business with the city.[23] Early LGBTQ activists were the target of extensive and abusive surveillance and raids by the FBI and other government agencies.[24] There were extraordinary efforts to try to undermine gay Black civil rights leader, Bayard Rustin, who was a primary organizer of the historic 1963 March on Washington. Just days before the march, segregationist Senator Strom Thurmond verbally attacked Rustin on the Senate floor for being a communist, a draft dodger, and a homosexual. Thurmond's actions backfired, and instead became a rallying point for the civil rights movement, building even more momentum for the upcoming march.[25]

It was during these same years in the late 1960s and early 1970s that Northern California became an important center for activism, particularly for the Black Power movement, antiwar movement, and Red Power movement. Unfortunately, it was also a center for government surveillance of activists.

---

21. *Milestones in the American Gay Rights Movement*, PBS, https://www.pbs.org/wgbh/americanexperience/features/stonewall-milestones-american-gay-rights-movement/.

22. Mark Walston, *First Gay Rights Legislation Enacted*, MARK WALSTON: EXPLORING THE AM. EXPERIENCE (Mar. 27, 2012), https://markwalston.com/2012/03/27/first-gay-rights-legislation-enacted/.

23. *The 1970s*, SF GAY HISTORY, https://www.sfgayhistory.com/timeline/the-1970s/.

24. *ACLU History: Earliest Advocacy on Behalf of LGBT People*, ACLU (Sept. 10, 2010), https://www.aclu.org/documents/aclu-history-earliest-advocacy-behalf-lgbt-people; Ian S. Thompson, *Abusive Surveillance Is an LGBTQ Rights Issue*, ACLU (July 12, 2014), https://www.aclu.org/news/national-security/abusive-surveillance-lgbtq-rights-issue; Eric Cervini, *Spying Before Stonewall: How the FBI Secretly Tracked Gay Activists in the 60s*, VICE (June 8, 2020), https://www.vice.com/en/article/xg8dzn/-the-fbi-secretly-tracked-gay-activists-in-the-60s.

25. Cervini, *supra* note 24; Cheryl Corley, *Bayard Rustin: The Man Who Organized The March On Washington*, NPR (Aug. 15, 2013), https://www.npr.org/sections/codeswitch/2013/08/15/212338844/bayard-rustin-the-man-who-organized-the-march-on-washington.

The Black Panther Party for Self Defense ("Black Panther Party") was founded in Oakland, California in 1966 as a revolutionary organization with an ideology of Black nationalism, socialism, and armed self-defense, particularly against long-standing police brutality.[26] In the late 1960s, the Black Power movement was at "its zenith as a social movement"[27] and Black Panther members built important social programs for food and housing,[28] protected civil rights protesters from white vigilantes, and marched into the halls of power in California brandishing guns in protest of police killings.[29] In 1968, FBI Director J. Edgar Hoover said the Black Panther Party "without question, represents the greatest threat to the internal security of the country."[30] For Huey P. Newton, one of the founders of the Black Panther Party, government surveillance was pervasive. He recounted that there were "about a million pages of FBI documents with my name on it; they wanted to tear down my character."[31] Of the nearly three hundred documented actions taken by COINTELPRO to disrupt Black groups, two hundred and thirty-three were directed against the Black Panther Party.[32]

These years were also a critical time for Bay Area protests and activism against the war in Vietnam, which had raged with American ground troops since 1965. In June 1971, the *New York Times* began publishing secret government documents leaked by whistleblower Daniel Ellsberg. The documents, which came to be known as the Pentagon Papers, chronicled the decades of failed U.S. policy in Vietnam and deliberate efforts to mislead Americans about the war. The release of these papers helped activists

26. *The Black Panther Party*, NAT'L ARCHIVES, https://www.archives.gov/research/african-americans/black-power/black-panthers.

27. Donald F. Tibbs, *From Black Power to Hip Hop: Discussing Race, Policing, and the Fourth Amendment Through the 'War On' Paradigm*, J. OF GENDER, RACE & JUST. 15, 63 (2012).

28. Interview with Huey P. Newton, WASH. UNIV. ST. LOUIS REPOSITORY (May 23, 1989), http://repository.wustl.edu/concern/videos/gt54ks236.

29. Tibbs, *supra* note 27 at 63–64; *Black Panther Party, Oakland, California, 1968-1972*, STAN. UNIV., https://exhibits.stanford.edu/fitch/browse/black-panther-party-oakland-california-1968-1972.

30. Rund Abdelfatah, Ramtin Arablouei, Jamie York, Julie Caine, Laine Kaplan-Levenson, Lawrence Wu, Parth Shah & Victor Yvellez, *The Real Black Panthers (2021)*, NPR (Feb. 2, 2023), https://www.npr.org/2023/01/31/1152784993/the-real-black-panthers-2021.

31. *COINTELPRO*, PBS, https://www.pbs.org/hueypnewton/actions/actions_cointelpro.html. Publicly available FBI records on Huey P. Newton are available at https://vault.fbi.gov/huey-percy-newton.

32. *Id.*

mobilize for the final push to end the war,[33] and by January 1973, the peace agreement was finally signed, and America officially ended its military involvement in Vietnam.[34]

During this same period, Native American activists, including many in California, founded and joined organizations like American Indian Movement (AIM) and galvanized the Red Power movement. AIM engaged in high profile activism for Native American sovereignty and the protection of Native Americans and their liberties.[35] In November 1969, Richard Oakes and LaNada War Jack, two Native American students studying at Bay Area colleges, led the takeover of Alcatraz Island in the San Francisco Bay.[36] The occupation protest lasted for nineteen months until June 1971, helping the Red Power activists focus the nation's attention on injustices and the need for tribal self-rule.[37]

In addition to heavy surveillance by the FBI and other federal agencies,[38] Black Power, antiwar, and Red Power activists were also actively surveilled by local California police. By 1973, San Francisco police alone had amassed intelligence files on over 100,000 people that the department deemed to be engaged with "subversive groups" or participating in activities that "might threaten the welfare of the community."[39]

---

33. Terry Gross, *How The Pentagon Papers Changed Public Perception Of The War In Vietnam*, NPR (June 18, 2021), https://www.npr.org/2021/06/18/1007573283/how-the-pentagon-papers-changed-public-perception-of-the-war-in-vietnam.

34. *The Pacifica Radio/UC Berkeley Social Activism Recording Project: Anti-Vietnam War Protests*, UNIV. OF CAL., BERKELEY, https://guides.lib.berkeley.edu/c.php?g=819842&p=5850986.

35. *American Indian Movement*, UNIV. OF GA., https://digilab.libs.uga.edu/exhibits/exhibits/show/civil-rights-digital-history-p/american-indian-movement.

36. *Richard Oakes, Native American Activist*, SFSU STUDENT CTR., https://sfsustudentcenter.com/richard-oakes-native-american-activist/; *Home*, DRWARJACK.COM, https://drwarjack.com/ (last visited May 3, 2024).

37. Charles L. Chavis, Jr., *Today in History: "We Hold the Rock": The Occupation of Alcatraz and the Native American Fight for Sovereignty in the Age of Fracture*, PBS (Nov. 16, 2021), https://www.pbs.org/wnet/exploring-hate/2021/11/16/today-in-history-occupation-of-alcatraz/; *Red Power: Perspectives 50 Years Later*, NAT'L PARK SERV., https://www.nps.gov/goga/redpower50.htm.

38. SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS; FINAL REPORT OF THE SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTEL. ACTIVITIES, S. REP. NO. 94-755 (1976).

39. Mark Schlosberg, *The State of Surveillance, Government Monitoring of Political Activity in Northern & Central California*, ACLU OF N. CAL. (2006), https://www.aclunc.org/sites/default/files/asset_upload_file714_3255_0.pdf, (citing Carol Pogash, *Getting Rid of 'Garbage'*, S.F. EXAM'R (Apr. 23, 1975), https://www.aclunc.org/docs/The_San_Francisco_Examiner_Wed__Apr_23__1975_%20ARTICLE.pdf).

While a wide variety of social justice movements were solidifying and gaining momentum across the country, this same historical period was also a particularly significant inflection point for computerization and the exponential growth of electronic technology—and California was an epicenter for much of this growth. In 1969, computer scientists successfully created the world's first computer network connection, transmitting the first internet message from a research lab at the University of California, Los Angeles to another at Stanford University in Palo Alto.[40] By 1971, the first microprocessor had been developed and sold.[41] By 1972, the C programming language was starting to be widely used and a group of engineers in Sunnyvale, California had founded Atari, developed Pong, and were testing this first video game in local bars.[42] The first mobile phones were also in development, with the earliest mobile phone call being made by April 1973.[43]

The California constitutional right to privacy was also developed and passed at a time when the federal courts were actively grappling with privacy, and despite some strong constitutional privacy decisions in the U.S. Supreme Court, local activists recognized the need for additional strategies. The Court decided *Griswold v. Connecticut* in 1965, striking down the state's anti-contraceptive statute on grounds that it violated a couple's right to privacy.[44] It also decided both *Berger v. New York* and *Katz v. United States* in 1967, holding that Fourth Amendment protection against unreasonable search and seizure extends to the interception of communications.[45] The Court later refined the right to privacy and right to "be let alone" in *Stanley v. Georgia* in 1969, holding that it was unconstitutional to criminalize private possession of obscene material.[46] Writing for the majority, Justice Thurgood Marshall made it clear that the rights to receive information and to personal privacy were fundamental to a free society.[47]

40. *1969: The Internet's First Message Sent From UCLA*, UCLA 100, https://100.ucla.edu/timeline/the-internets-first-message-sent-from-ucla.

41. *1971: Timeline of Computer History*, COMPUT. HIST. MUSEUM, https://www.computerhistory.org/timeline/1971/.

42. Charles Russo, *'It Changed the World': 50 Years on, the Story of Pong's Bay Area Origins*, SF GATE (Mar. 10, 2023), https://www.sfgate.com/local/article/bay-area-roots-pong-atari-17824939.php.

43. Michelle Delgado, *From 'the Brick' to the iPhone, the Cellphone Celebrates 50 Years*, SMITHSONIAN MAG. (Apr. 3, 2023), https://www.smithsonianmag.com/innovation/from-the-brick-to-the-iphone-the-cellphone-celebrates-50-years-180981910/.

44. Griswold v. Connecticut, 381 U.S. 479 (1965).

45. Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967).

46. Stanley v. Georgia, 394 U.S. 557 (1969).

47. *Id.* at 565 (1969).

While there had been some strong privacy decisions, many activists understood that these judicial decisions were not going to be adequate and that many more protections needed to be in place. For example, following the privacy decisions by the U.S. Supreme Court in *Berger* and *Katz* in 1967, Congress passed the federal omnibus crime bill of 1968 and legally authorized wiretapping by federal law enforcement. The ACLU opposed the use of wiretapping or other electronic eavesdropping devices;[48] and following the unfortunate passage of the federal law, California ACLU staff and activists actively fought California legislative efforts to extend wiretapping powers to local and state law enforcement.[49]

B. CALIFORNIA CONSTITUTIONAL RIGHT TO PRIVACY WAS DEVELOPED AND PASSED IN A PERIOD OF GROWING ATTENTION TO TECHNOLOGY'S IMPACT ON RIGHTS AND SOCIETY

During the late 1960s and early 1970s, activists, lawyers, academics, and artists started to deliberately consider technology's impacts and intersections with social justice movements.

Black activists were engaging in critical ways with new technology and imagining a future where it would support power, equity, and justice rather than perpetuate the status quo.[50] By 1972, the Black Panther Party's Ten Point Plan included an explicit provision in Point 10 about "people's community control of modern technology" in addition to "land, bread, housing, education, clothing, justice, peace."[51] In the Bronx, New York, Black musicians like

48. The ACLU has opposed wiretapping as a matter of policy since the 1960s, and this national board policy position remains in force today. *See* ACLU Policy 254 (unpublished board policy) (on file with author).

49. Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act), 18 U.S.C. §§ 2510-22; ACLU OF N. CAL. NEWS VOL. 37, NO. 3, (Apr. 1972), at 4, https://digitallibrary.californiahistoricalsociety.org/object/16045); AM. C.L. UNION NEWS VOL. 33, NO. 8, at 1 (Aug. 1968), https://digitallibrary.californiahistoricalsociety.org/object/15658.

50. C. B. Ogbunu, *How Afrofuturism Can Help the World Mend*, WIRED (July 15, 2020), https://www.wired.com/story/how-afrofuturism-can-help-the-world-mend/.

51. 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 (Feb. 7, 2024), https://www.ucpress.edu/blog/25139/the-black-panther-partys-ten-point-program/; Andrew Beale, Cassady Rosenblum, Rachel Loyd, Tian Chenwei, Khaled Sayed & Ryan Lindsay, *The Black Panther Party's Ten-Point Program, 50 Years Later*, OAKLAND N. (Nov. 4, 2016), https://oaklandnorth.net/2016/11/04/the-black-panther-partys-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.

Grandmaster Flash were utilizing technology to create a new kind of revolutionary music—using electronics training to invent the new musical sounds, tools, and techniques that became hip-hop.[52] Hip hop is interwoven as "an integral part of social and racial justice movements."[53] The music "emanating from the DJ's equipment might tell partiers to 'move your feet,' and in the very next set, tell them to 'fight the power.'"[54]

Technology and privacy were also intersecting with race and class at this time in complex ways that spurred attention to these issues from very different sectors of society. As Richard Ruggles described in a 1968 article for a symposium on computers, data banks, and individual privacy, the "present concern with the right to privacy has two quite different aspects."[55] Both the fight for civil rights and the libertarian concerns of the wealthy operated together to bring attention to privacy issues. 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."[56] Second, the rich "resent[ed]" reporting information to the government about their financial dealings, safety standards, fair employment practices and more.[57] They felt that it was "an invasion of privacy" to not be "free" to run affairs as they saw fit without government interference.[58] Further evidence of these class dynamics shows up in the legislative history of the California constitutional right to privacy. The City Administrator for Carmel-by-the-Sea, a wealthy Northern California beachfront community, submitted a letter urging its State Senator to support the Privacy Amendment's passage through the legislature.[59]

---

52. Monica M. Smith, *Revolutionary Invention: Hip-Hop and the PC*, SMITHSONIAN: LEMELSON CTR. (Sept. 4, 2012), https://invention.si.edu/revolutionary-invention-hip-hop-and-pc; *Grandmaster Flash*, WIKIPEDIA (July 21, 2024) https://en.wikipedia.org/wiki/Grandmaster_Flash (electronics training); Aaron Morrison, *Hip-hop and Justice: Culture Carries the Spirit of Protest, 50 Years and Counting*, AP NEWS (Aug. 10, 2023), https://apnews.com/article/hip-hop-social-justice-protest-50th-anniversary-5351511d2cd79ffe0b10d70db7772357.

53. Aaron Morrison, *Hip-hop and Justice: Culture Carries the Spirit of Protest, 50 Years and Counting*, AP NEWS (Aug. 10, 2023), https://apnews.com/article/hip-hop-social-justice-protest-50th-anniversary-5351511d2cd79ffe0b10d70db7772357.

54. *Id.*

55. Richard Ruggles, *On the Needs and Values of Data Banks*, 53 MINN. L. REV. 211, 212 (1968).

56. *Id.* at 213.

57. *Id.*

58. *Id.*

59. *Support Letter from Carmel-by-the-Sea City Administrator Hugh Bayless 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.

Carmel's leaders were likely following privacy issues closely: the city had recently lost a constitutional challenge at the California Supreme Court to a 1969 financial disclosure law that required every public officer and candidate for state or local public office in California to file a statement describing the nature and extent of their investments.[60] From Black Panther Party members in Oakland to affluent Carmel residents, Californians at different ends of the economic spectrum were concerned about privacy issues at this time.

In the late 1960s and early 1970s, organizations were also starting to recognize the growing intersection of technology and rights issues. Grassroots organizations like Computer People for Peace and larger organizations like the American Civil Liberties Union (ACLU) spoke out and discussed the threats of government surveillance and corporate information collection on personal lives, democracy, and society as a whole.[61]

Computer People for Peace, founded in New York City, was an organization of individuals who worked in the early years of the computer industry.[62] It started in 1968 with opposition to the Vietnam War and then became engaged in more intersectional social justice movements. It worked to highlight gender inequality and discrimination in the emerging technology industry, to free computer programmer and Black Panther activist Clark Squire (Sundiata Acoli),[63] and bring attention to IBM's role in providing computer equipment to support the apartheid regime in South Africa.[64]

60. City of Carmel-By-The-Sea v. Young, 466 P.2d 225 (Cal. 1970).

61. *See Public Service Announcements by the New Mexico Civil Liberties Union (Godfrey Reggio)*, YOUTUBE (1974), https://www.youtube.com/watch?v=yah54al6Cks (last visited Sept. 21, 2023).

62. Shwetha Jayaraj, *A Brief History from Hack Manhattan — an Ode to the 1970's Computer People for Peace*, MEDIUM (Dec. 31, 2022), https://medium.com/@shwethajayaraj/a-brief-history-from-hack-manhattan-an-ode-to-the-1970s-computer-people-for-peace-fe04623d5d21.

63. Sundiata Acoli was imprisoned from 1973–2022, when he was implicated in the death of a state trooper during a traffic stop for a broken taillight. When he was finally released on bail at the age of 85, he was the oldest former member of the Black Panthers still incarcerated for acts of violence during the 1970s Black Liberation struggle. He was denied bail for 29 years despite having an "exemplary" prison record. In 2022, the New Jersey Supreme Court ruled that he was no longer a risk to public safety. *See* Ed Pilkington, *Former Black Panther Sundiata Acoli to be Released From Prison After 49 Years*, GUARDIAN (May 10, 2022), https://www.theguardian.com/world/2022/may/10/sundiata-acoli-black-panthers-released-prison.

64. Joan Greenbaum, *Questioning Tech Work*, AINOW INST. (Jan 31, 2020), https://ainowinstitute.org/publication/questioning-tech-work-2.

Privacy was an important Computer People for Peace issue.[65] In 1971, the organization published *Data Banks, Privacy and Repression*, a booklet discussing the need to take action to limit data collection, to prohibit the sale or interchange of data between companies and governments, and to advocate that workers in the technology industry had an obligation to inform and protect the public about the harmful effect of misuse of data. Further, in 1972, the organization drafted an "Electronic Bill of Rights." Its principles included encouraging data encryption and secure communications free from government and corporate monitoring and supporting the development of electronic mail and databases with robust privacy and security features including data retention limits. It also advocated for ensuring that rights were secured in the emerging global information environment.[66]

The ACLU actively started to speak out about privacy in the digital age in the late 1960s and early 1970s—one of the few (if only) public interest law organizations working on these issues at the time.[67] As early as the spring of 1967, the ACLU was working on technology and privacy issues at both the state and federal level. In March 1967, Lawrence Speiser, Director of the ACLU Washington Office, testified to a Subcommittee of the United States Senate Judiciary Committee about "grave concern[s]" with a proposed National Data Center, which would "create the machinery for the maintenance of personal dossiers."[68] Later that spring, in May 1967, the ACLU of Northern California and San Francisco State College hosted a full day privacy conference. The day was comprised of thirteen privacy panels, a keynote speech by Professor Alan Westin on "Privacy in a Free Society," and a banquet speech by U.S. Supreme Court Justice William O. Douglas on "Computerized Man."[69] The conversations of the day underscored the importance of taking

65. *Id.*; Joan Greenbaum is Professor Emerita at City University of New York (CUNY) where she is on the faculty of Environmental Psychology (the study of place) and the program in Interactive Technology and Pedagogy.

66. *Electronic Bill of Rights*, COMPUT. PEOPLE FOR PEACE, http://www.flyingsnail.com/missingbbs/ct23.html.

67. 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) (on file with author).

68. *Lawrence Speiser's Testimony: The Proposed Federal Data Center*, ACLU OF N. CAL. NEWS VOL. 32, NO. 4, at 3 (Apr. 1967), https://digitallibrary.californiahistoricalsociety.org/object/15631?islandora_paged_content_page=3.

69. ACLU OF N. CAL. NEWS VOL. 32, NO. 5, (May 1967), https://digitallibrary.californiahistoricalsociety.org/object/15606?solr_nav%5Bid%5D=6f116fdfadb5309128bd&solr_nav%5Bpage%5D=0&solr_nav

prompt and robust action to address the advances of technology and its impact on rights and democratic society.[70]

Several years earlier, Martin Luther King, Jr. had critiqued the assumption that modernity in itself would improve people's lives. In his 1964 Nobel Prize lecture, he highlighted the "new and astonishing peaks of scientific success" and warned that "[s]o much of modern life can be summarized in that arresting dictum of the poet Thoreau: 'Improved means to an unimproved end.'"[71] King also wrote eloquently in his 1963 *Letter from a Birmingham Jail* about the foundational role of solidarity across people and movements to push for change—"Injustice anywhere is a threat to justice everywhere. We are caught in an inescapable network of mutuality, tied in a single garment of destiny. Whatever affects one directly, affects all indirectly."[72]

During the years immediately surrounding the passage of the California constitutional right to privacy, activists from organizations as diverse as the Black Panther Party and Computer People for Peace were engaged in intersectional movement work and solidarity across issues and understood how advances in technology could exacerbate government and capitalist threats to social change. The intersectional liberation movements during this important time in history understood the power that technology could wield to support or undermine their efforts and democracy as a whole. This awareness undergirded the development and passage of the California constitutional right to privacy in 1972.

C. CALIFORNIA CONSTITUTIONAL PRIVACY WAS A HIGH IMPACT STRATEGY WITHIN A BROADER INTEGRATED ADVOCACY VISION

The California constitutional right to privacy was drafted as a high impact strategy within a broader integrated advocacy vision. In the spring of 1972,

---

%5Boffset%5D=4; ACLU OF N. CAL. NEWS VOL. 32, NO. 3, (Mar. 1967), https://digitallibrary.californiahistoricalsociety.org/object/15636?solr_nav%5Bid%5D=394161b2536c2b387f02&solr_nav%5Bpage%5D=0&solr_nav%5Boffset%5D=3; ACLU OF N. CAL. NEWS VOL. 32, NO. 4, at 3 (Apr. 1967), https://digitallibrary.californiahistoricalsociety.org/object/15631?islandora_paged_content_page=3.

70. ACLU OF N. CAL. NEWS VOL. 32, NO. 4, at 3 (Apr. 1967), https://digitallibrary.californiahistoricalsociety.org/object/15631?islandora_paged_content_page=3.

71. Martin Luther King Jr., *Martin Luther King, Nobel Peace Prize Lecture, December 11, 1964 [excerpts]*, IAJU GLOB. CITIZEN CURRICULUM PROJECT (Dec. 11, 1964), https://globalcitizenship.georgetown.edu/essays/martin-luther-king-nobel-peace-prize-lecture-december-11-1964-excerpts.

72. Martin Luther King Jr., *Letter from a Birmingham Jail [King, Jr.]*, AFR. STUD. CTR. - UNIV. OF PA. (Apr. 16, 1963), https://www.africa.upenn.edu/Articles_Gen/Letter_Birmingham.html.

Assemblymember Kenneth Cory[73] introduced Constitutional Amendment 51 (ACA 51) (the "Privacy Amendment") in the California legislature. It was an important component of an integrated legal advocacy strategy to support social movements and expand rights and protections of Californians in the modern technological world.[74] It bolstered an emerging framework for social change with just a few words, by adding "and privacy" to the inalienable rights in Article I, Section 1 of the California Constitution and changing the word, "men," to "people."

Assemblymember Cory explained what animated the introduction of the constitutional amendment in his letter to the legislative file. He presciently discussed the rising surveillance ecosystem and the threats of surveillance capitalism, writing that "[i]n the face of a cybernetics revolution and the increasingly pervasive amount of information being compiled, it would be highly desirable that our constitution state in clear terms that each person has a fundamental right to privacy." He proposed an amendment to create a positive, inalienable right to privacy and "put the State and private firms on notice that the people have this fundamental right and it can only be abridged when the public concern is an overriding concern."[75]

Assemblymember Cory was personally motivated to pass ACA 51 because he had personally felt the sting of spying. In 1967, Cory was the first Democrat ever to be elected to the Assembly from famously conservative, Orange County. According to Cory's daughter, local law enforcement "wanted Cory out" and tried in every way to "sink him."[76] She said their failure led him to

---

73. Kenneth Cory was a Democratic Assemblymember representing Orange County from 1967–1974 and served as State Controller from 1976–1986. His obituary notes that he was a protégé of longtime Assembly Speaker Jesse M. Unruh and was popular with both Democrat and Republican colleagues. *Ken Cory; State Controller, Assemblyman*, L.A. TIMES (Nov. 14, 1998), https://www.latimes.com/archives/la-xpm-1998-nov-14-mn-42652-story.html.

74. The legislative archives reveal that a similar assembly constitutional amendment, ACA 69, was attempted in the previous legislative year, 1971. *See* S. COMM. ON JUDICIARY, BACKGROUND INFO. – ACA 51,
(last visited July 22, 2024). But ACA 69 did not progress past the Assembly Judiciary Committee. *See* STAFF OF ASSEMB. COMM. ON CONST. AMEND., ANALYSIS, ACA 51 (CORY) AS INTRODUCED MARCH 13, 1972, Assemb. (Cal. 1972), https://www.aclunc.org/sites/default/files/Staff%20Analysis%20ACA%2051%20%28Cory%29%20as%20introduced%20March%2013%2C%201972%20%28April%2024%2C%201972%29.pdf.

75. Letter Response to Chairman Ignazio Vella from Hon. Kenneth Cory (1972), at 1–2, https://www.aclunc.org/sites/default/files/Letter%20Response%20to%20Chairman%20Ignazio%20Vella%20from%20Hon.%20Kenneth%20Cory.pdf.

76. Dorothy Ehrlich, former Deputy Executive Director, ACLU, Panel at the Berkeley Technology Law Journal Symposium: California Constitutional Privacy at 50: Power of State Law and Promoting Racial Justice in the Digital Age (Oct. 27, 2023), https://bk.webcredenza.com/watch?id=85341 at (12:01).

brag that he must be the "cleanest politician around" because they never found anything they could use against him.[77] His daughter also shared that Assemblymember Cory was personally inspired by a deep commitment to reproductive rights and personal autonomy, and he saw ACA 51 as a quiet, yet effective vehicle to firmly establish these rights.[78]

Legislative testimony prepared in support of ACA 51 by Mary Dunlap, a 1971 Berkeley Law graduate and co-founder of the San Francisco-based legal organization Equal Rights Advocates,[79] highlighted the importance of the constitutional right to privacy for gender justice. She discussed how crucial it was to change the term, "men" to "persons," and ensure that fundamental rights in law and practice are extended to all people.[80] She noted that "[t]he principles herein described carry such importance . . . we hope this committee will not treat them lightly."[81] While the constitutional amendment's changes to the text of Article I, Section 1 was "a miniscule change," she emphasized that it was "a crucial one."[82] Although the U.S. Supreme Court had, at the time, held that people have a right to privacy, Dunlap pointed out that "the people charged with carrying out the law are not necessarily familiar with the courts [sic] decisions. It is important then that the right to pursue and obtain privacy be understood by the people."[83]

The staff report of the Assembly Constitutional Committee on ACA 51 further examined the purpose, reach, and goals of the constitutional amendment. The report explained that "[w]ith the technological revolution," the Fourth Amendment and other federal constitutional protections "do not offer sufficient protection against state surveillance, record collection, and government snooping into our personal lives. We must, therefore, develop new safeguards to meet the new dangers."[84] The California constitutional right would create a distinct, positive, and expansive right to both pursue and obtain

77. *Id.* at (12:07).

78. *Id.* at (11:33).

79. Henry K. Lee, *Mary Dunlap -- S.F. Police Watchdog, Rights Advocate*, SF GATE (Jan. 22, 2003), https://www.sfgate.com/bayarea/article/Mary-Dunlap-S-F-police-watchdog-rights-2638828.php.

80. *Hearing on ACA 51 before the Assembly Constitutional Amendments Committee*, (Cal. 1972) (statement of Cheriel Moensh Jensen), https://www.aclunc.org/sites/default/files/Testimony%20before%20Assembly%20Constitutional%20Amendments%20Committee%20%28April%2024%2C%201972%29.pdf.

81. *Id.* at 8.

82. *Id.* at 4.

83. *Id.* at 7.

84. STAFF OF ASSEMBLY CONST. COMM., REP. ON ACA 51, at 5 (Cal. 1972). https://www.aclunc.org/sites/default/files/Staff%20report%20of%20Assembly%20Constitutional%20Committee%20on%20ACA%2051%20%28before%20April%2024%29.pdf.

privacy. It would chart a new path that did not rely on the U.S. Supreme Court's search and seizure jurisprudence of reasonable expectations of privacy, which so far defined the right solely by prohibiting certain wrongs like unlawful search and seizure and telephone tapping and was a formulation of privacy that was not clear "who is protected and from what."[85]

1. *California Constitutional Privacy Was Passed With Organized Political Effort and Clear Plan to Give Power to the People Over Privacy in the Digital Age*

The legislative archives also reveal both the diversity of the organized political effort to support the Privacy Amendment as well as the significant opposition that it had to combat more than fifty years ago from powerful forces like government agencies and corporate lobbying interests. Many of the arguments against the constitutional right are the same types of arguments that privacy efforts still regularly face today. Legislative committee staff analysis, memos from the legislative counsel, and support letters in the summer of 1972 reveal that Assemblymember Cory, the Privacy Amendment's author, was successfully battling opposition arguments on many fronts. Law enforcement was floating arguments that the effort would undermine policing methods like wiretapping.[86] The Department of Motor Vehicles questioned whether it would affect the "public records" status of automobile registration information.[87] There were also "pressures from those businesses that can profit from the various invasions of privacy."[88]

---

85. STAFF OF ASSEMB. COMM. ON CONST. AMEND., ANALYSIS, ACA 51 (CORY) AS INTRODUCED MARCH 13, 1972, at 1 (Cal. 1972), https://www.aclunc.org/sites/default/files/Staff%20Analysis%20ACA%2051%20%28Cory%29%2C%20as%20introduced%20March%2013%2C%201972.pdf.

86. STAFF OF S. JUDICIARY COMM., ANALYSIS OF ACA 51 (Cal. 1972), https://www.aclunc.org/sites/default/files/Senate%20Committee%20on%20Judiciary%20Backround%20Information.pdf.

87. Legislative Counsel Memorandum from George H. Murphy and Marguerite Roth to Hon. Kenneth Cory, at 1 (June 30, 1972), https://www.aclunc.org/sites/default/files/Letter%20from%20George%20H.%20Murphy%20and%20Marguerite%20Roth%20to%20Hon.%20Kenneth%20Cory%20%28June%2030%2C%201972%29.pdf.

88. Support letter from Carmel-by-the-Sea City Administrator Hugh Bayless to Hon. Donald L. Grunsky, at 1 (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%28June%2012%2C%201972%29.pdf. The City Administrator of City of Carmel-by-the-Sea may have had a particular interest and engagement in privacy issues at that time due to the city's recent unsuccessful attempt to invalidate a state law requiring financial disclosures of local officials. City of Carmel-By-The-Sea v. Young, 466 P.2d 225 (Cal. 1970).

Despite these forces in opposition, Assemblymember Cory used his political skill[89] to marshal the support needed for this effort and succeeded in obtaining the required two-thirds majority vote for ACA 51 in both houses of the California legislature.[90] The Privacy Amendment moved to the next step in the constitutional amendment process[91] and was put on the November 1972 ballot as Proposition 11.[92]

The ballot argument in favor of the Privacy Initiative was officially authored by Assemblymember Cory and State Senate Majority Leader George Moscone.[93] With urgency and precision, it explains its objectives, purpose and scope:

> The proliferation of government snooping and data collecting is threatening to destroy our traditional freedoms. Government agencies seem to be competing to compile the most extensive sets of dossiers of American citizens. Computerization of records makes it possible to create 'cradle-to-grave' profiles of every American.
>
> At present there are no effective restraints on the information activities of government and business. This amendment creates a legal and enforceable right of privacy for every Californian. (emphasis in original).

The argument in favor continues:

> The right of privacy is the right to be left alone. It is a fundamental and compelling interest. It protects our homes, our families, our thoughts, our emotions, our expressions, our personalities, our

89. Kenneth Cory was, as they say in the vernacular, a legislator with "political juice." He was a protégé of longtime Assembly Speaker Jesse M. Unruh and was popular with both Democrat and Republican colleagues. *Ken Cory; State Controller, Assemblyman*, L.A. TIMES (Nov. 14, 1998), https://www.latimes.com/archives/la-xpm-1998-nov-14-mn-42652-story.html.

90. *See* Assemb. Const. Amend. No. 51 (Feb. 16, 1972), https://www.aclunc.org/sites/default/files/Assembly%20Consitutional%20Amendment%20No.%2051%20%28Feb.%2016%2C%201972%29.pdf*; see also Constitutional Amendments*, CAL. DEP'T OF GEN. SERVS. (Feb. 1998), https://www.dgs.ca.gov/en/Resources/SAM/TOC/6000/6920.

91. California ballot measures can be placed on the ballot either by 2/3 legislative passage or by public signature process. *See Ballot Measures*, CAL. SEC'Y OF STATE, https://www.sos.ca.gov/elections/ballot-measures (last visited May 3, 2024).

92. *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), https://repository.uclawsf.edu/ca_ballot_props/762.

93. Oral history from Dorothy Ehrlich is that Anthony Amsterdam, an expert on Fourth Amendment law who was a Professor at Stanford Law School during this time, helped to draft the ballot argument in support. *See Anthony G. Amsterdam*, WIKIPEDIA (2024), https://en.wikipedia.org/wiki/Anthony_G._Amsterdam (last visited May 3, 2024); Dorothy Ehrlich, former Deputy Executive Director, ACLU, Panel at the Berkeley Technology Law Journal Symposium: California Constitutional Privacy at 50: Power of State Law and Promoting Racial Justice in the Digital Age (Oct. 27, 2023), https://bk.webcredenza.com/watch?id=85341.

> freedom of communion, and our freedom to associate with the people we choose. It prevents 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.
>
> Fundamental to our privacy is the ability to control circulation of personal information. (emphasis in original), This is essential to social relationships and personal freedom. The proliferation of government and business records over which we have no control limits our ability to control our personal lives.

The argument continues: "The right of privacy is an important American heritage and essential to the fundamental rights guaranteed by the First, Third, Fourth, Fifth and Ninth Amendments to the U.S. Constitution. This right should be abridged only when there is compelling public need."

The argument concludes by stating that:

> Proposition 11 also guarantees that the right of privacy and our other constitutional freedoms extend to all persons by amending Article I and substituting the term 'people' for 'men.' There should be no ambiguity about whether our constitutional freedoms are for every man, woman and child in this state." (emphasis in original)[94]

The opposition ballot argument was drafted by Republican State Senator James E. Whetmore, who argued the Privacy Amendment was "unnecessary" because privacy was already protected by the courts, and that the addition of the two words, "and privacy," would make the constitution more wordy.[95] Whetmore's primary argument in opposition, though, was a political dog whistle that Proposition 11 would facilitate welfare fraud, giving people a free pass to cheat the system if their privacy was protected.[96] Whetmore put forth an unsupported legal argument that the amendment would prohibit any information collection by government and thus "emasculate all government

94. *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), https://repository.uclawsf.edu/ca_ballot_props/762.

95. James Whetmore, *Argument Against Proposition 11*, ACLU OF N. CAL., https://www.aclunc.org/sites/default/files/Argument%20Against%20Proposition%2011.pdf.

96. Dorothy Ehrlich, former Deputy Executive Director, ACLU, Panel at the Berkeley Technology Law Journal Symposium: California Constitutional Privacy at 50: Power of State Law and Promoting Racial Justice in the Digital Age (Oct. 27, 2023), https://bk.webcredenza.com/watch?id=85341.

programs based on recipient need" and "bring chaos to all government benefit programs."[97]

In the ballot support rebuttal, Cory made short work of these arguments, writing "[t]he right to privacy is much more than 'unnecessary wordage.'"[98] Nor will the right to privacy "destroy welfare" or "undermine any important government programs. It is limited by 'compelling public necessity' and the public's need to know."[99] Cory also wrote a separate rebuttal to the claim that Proposition 11 would affect benefits programs in California.[100] He explained that "this is simply untrue," that no constitutional right is absolute, and that the government could continue to require people to disclose information when there was a compelling state interest. But the "public should be able to expect that in carrying out necessary government projects, care is taken to infringe as little as possible on individual rights."[101]

The ACLU of Northern California supported the constitutional right to privacy, both through the legislative process and as a ballot measure. In a September 1972 article in *ACLU News*, which still rings true today, the organization explained how the growth of technology reduced the friction that had been operationally protecting privacy, emphasized the importance of enacting the constitutional right with a scope covering both government and companies, and urged its adoption.[102]

But this support by the ACLU was relatively quiet because the passage of Proposition 11 was largely a "stealth campaign."[103] The November 1972 ballot was chock-full, with a daunting list of twenty-two ballot measures. Seven of these propositions were especially consequential, relating to everything from the death penalty and felony disenfranchisement, race-based bussing, whether to legalize marijuana, ban "obscene" material, allow farmworkers to continue

97. James Whetmore, *Argument Against Proposition 11*, ACLU OF N. CAL., https://www.aclunc.org/sites/default/files/Argument%20Against%20Proposition%2011.pdf.

98. *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), https://repository.uclawsf.edu/ca_ballot_props/762.

99. *Id.*

100. Kenneth Cory, *Rebuttal to the Claim That Proposition 11 will Destroy Welfare in California*, ACLU OF N. CAL., https://www.aclunc.org/sites/default/files/Rebuttal%20to%20the%20Claim%20That%20Proposition%2011%20will%20Destroy%20Welfare%20in%20CaIifornia.pdf.

101. *Id.*

102. ACLU OF N. CAL. NEWS VOL. 37, NO. 7, https://digitallibrary.californiahistoricalsociety.org/object/16083.

103. Dorothy Ehrlich, former Deputy Executive Director, ACLU, Panel at the Berkeley Technology Law Journal Symposium: California Constitutional Privacy at 50: Power of State Law and Promoting Racial Justice in the Digital Age (Oct. 27, 2023), https://bk.webcredenza.com/watch?id=85341.

to strike, and protect the beaches.[104] Cory's political strategy for Proposition 11's ballot passage appeared to be for it to sail through amidst the sea of other ballot measures.[105] There were some newspaper editorials on the measure, with some outlets writing in favor of its passage like the *Modesto Bee*:

> [Proposition 11] would prevent government and business interests from 'squirreling' unnecessary information about citizens . . . the entire process of dossier building . . . integrated information systems and building up new dossiers from previously unrelated data about individuals creates a 'record prison' . . . . A Yes vote on Proposition 11 would create a legal and enforceable right of privacy for every Californians. Voters should approve the measure.[106]

Other outlets wrote in opposition to its passage, including the *Hi-Desert Star*, which highlighted its focus on preventing "suspected welfare fraud" and that "the principal of privacy is well established in the law," and that "no further action is needed by the state on this particular matter."[107]

The *Anaheim Bulletin* appeared to support much of the purpose of Proposition 11, which was sponsored by its own Orange County Assemblymember, but the newspaper still recommended a no vote. It wrote:

> The 'right of privacy" is, of course, one of the key issues of modern times. The Anaheim Bulletin is especially susceptible to plans which would limit political snooping into the private lives and transactions of individuals . . . . Proposition 11 swings the ax too far . . . . Cory's measure . . . is not the right procedure. We urge a 'No' vote on Proposition 11.[108]

While newspaper editorials both supported and opposed Proposition 11, the *Los Angeles Times* described it as largely attracting "no attention or controversy . . . innocuous on the face of it. It is something like coming out in favor of motherhood."[109] The article noted some "uneasy opposition, unorganized and not very vocal" and that proponents contended the Privacy Amendment was necessary because "modern technology is capable of monitoring, centralizing and computerizing information so as to eliminate any possibility of individual privacy."[110] Dorothy Ehrlich, who worked with the

104. *Id.*
105. *Id.*
106. *Proposition 11: Right to Privacy*, MODESTO BEE, Oct. 20, 1972.
107. *Proposition 11: Rates a NO Vote*, HI-DESERT STAR (YUCCA VALLEY), Oct 19, 1972.
108. *Proposition 11*, ANAHEIM BULL., Nov 4, 1972.
109. Gene Blake, *Prop. 11 Adds Privacy to Peoples' Rights in California Constitution*, L.A. TIMES, Oct. 18, 1972, at 43, https://www.newspapers.com/image/385981148.
110. *Id.*

ACLU in California in the time leading up to November 1972 election, recounted more than fifty years later that it was not clear whether this unobtrusive Privacy Amendment campaign was entirely a result of political strategy or lack of campaign resources.[111] But Ehrlich knows Cory "definitely asked controversial groups to step back," pro-choice organizations were hidden from view, and the ACLU was directly asked to publicly stay out of the Proposition 11 campaign, and they did.[112]

Proposition 11 was passed by the California voters in 1972 by a substantial majority, 62.9% of the vote.[113] With its passage, the California Constitution became the first constitution in the nation—either federal or state—to include an explicit right to privacy. The constitutional amendment was drafted and passed to set a clear legal trajectory for the courts: that the right to pursue and obtain privacy was an inalienable and legally enforceable right, that it applied to both government and private parties, and that it should only be abridged when public need is an overriding concern. It enacted a modern right to privacy that was intended to address and robustly limit how technological advances and the surveillance ecosystem of both business and government actions could invade our private lives and undermine our fundamental rights.[114] It also unequivocally ensured that privacy—and all other inalienable rights in California—applied to all people. As the Staff Report of the Assembly Committee on ACA 51 discussed, "[w]ith the right of privacy explicitly written into the Constitution, it will itself become the basis for an expansion of constitutional protections."[115]

But the archives also illuminate that its passage was strategically intended to have a much broader integrated advocacy effect—to educate and mobilize people to be able to fight against privacy invasions and to spur policymakers to hear the voice of the public and take action to further advance privacy in

111. Dorothy Ehrlich, former Deputy Executive Director, ACLU, Panel at the Berkeley Technology Law Journal Symposium: California Constitutional Privacy at 50: Power of State Law and Promoting Racial Justice in the Digital Age (Oct. 27, 2023), https://bk.webcredenza.com/watch?id=85341.

112. *Id.* at (10:30).

113. *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP Repository (1972), https://repository.uclawsf.edu/ca_ballot_props/762.

114. "[T]he moving force behind the new constitutional provision was a more focused privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society. The new provision's primary purpose is to afford individuals some measure of protection against this most modern threat to personal privacy." White v. Davis, 533 P.2d 222, 233 (Cal. 1975).

115. STAFF OF ASSEMB. CONST. COMM., REP. ON ACA 51, at 5 (Cal. 1972). https://www.aclunc.org/sites/default/files/Staff%20report%20of%20Assembly%20Constitutional%20Committee%20on%20ACA%2051%20%28before%20April%2024%29.pdf.

the digital age. Assemblymember Cory talked about this strategic intent and that "[t]he concern that our privacy is increasingly becoming a mere myth and that individuals are powerless to control it led to the introduction of ACA 51."[116] Further, as the Staff Report highlighted in more detail, "[t]he major contribution of this amendment is to make the public aware that its freedoms are being slowly eroded, that this trend must be reversed. Passage of Proposition 11 will serve notice on the Legislature and the Courts that the public will not permit the continual abrogation of their rights. The right to privacy must be clearly spelled out and must be firmly adhered to."[117]

2. *Passage of California Constitutional Privacy is An Early Example of Integrated Advocacy in Action*

The passage of the constitutional right to privacy is an early example in the technology and social justice field of integrated advocacy in action.[118] The development and passage of the 1972 California Privacy Amendment complemented and buttressed existing strategies to protect privacy in the digital age and helped create a virtuous cycle that powered further integrated advocacy strategies and supported needed change.

With integrated advocacy, organizations utilize a layered approach to powering social change. It is an expansive approach that leverages diverse strategies, both within and outside of formal lawmaking arenas, to build momentum and better support long-term social change.[119] Using an integrated advocacy approach means considering all of the potential avenues to support change, including but not limited to academic and policy research; investigations; litigation and legal advocacy; local, state, federal and international legislative and agency work; electoral and political advocacy; in

116. Letter from Kenneth Cory to the Legislative File, (1972), https://www.aclunc.org/sites/default/files/Letter%20Response%20to%20Chairman%20Ignazio%20Vella%20from%20Hon.%20Kenneth%20Cory.pdf.

117. STAFF OF ASSEMB. CONST. COMM., REP. ON ACA 51, at 5 (Cal. 1972). https://www.aclunc.org/sites/default/files/Staff%20report%20of%20Assembly%20Constitutional%20Committee%20on%20ACA%2051%20%28before%20April%2024%29.pdf.

118. Dorothy Ehrlich, the longtime Executive Director the ACLU of Northern California and Deputy Director of the National ACLU, helped me develop and implement an integrated advocacy approach for the Technology and Civil Liberties Program from its inception in 2004. *See Technology & Civil Liberties*, ACLU OF N. CAL., https://www.aclunc.org/issue/technology-civil-liberties; *Fighting High-Tech Government Surveillance*, ACLU OF N. CAL., https://www.aclunc.org/fighting-high-tech-government-surveillance.

119. *See* LUCY BERNHOLZ, NICOLE OZER, KIP WAINSCOTT, & WREN ELHAI, STANFORD DIGITAL CIVIL SOCIETY LAB, INTEGRATED ADVOCACY: PATHS FORWARD FOR DIGITAL CIVIL SOCIETY (2020), https://pacscenter.stanford.edu/wp-content/uploads/2020/01/Integrated-Advocacy-Report__Digital.pdf; Scott L. Cummings, *Movement Lawyering*, 2017 U. ILL. L. REV. 1645 (2017).

person and online organizing; corporate advocacy; public education; and strategic communications. Integrated advocacy strategies are then used in combination, concurrently, or sequentially, to maximize overall impact.

Integrated advocacy campaigns can differ in duration—they can be developed and utilized for a period of weeks for a fast-moving, reactive issue, or planned and executed over months, years, or even decades.[120] They can be built for a single issue or for multiple, interconnected issues. Using an integrated advocacy approach does not mean that all strategies are always used or used by the same organization. Depending on an organization's focus, expertise, and available resources for particular change strategies, an integrated advocacy approach can be used inside a single organization or it can be shared between partner organizations. For example, with one organization focusing on litigation, another partner focusing on legislative work, a third focusing on organizing, but all sharing an overall integrated advocacy vision through a coordinated campaign. The "crucial point" and what makes it integrated advocacy is that the tactics are "deliberately coordinated" by lawyers and other stakeholders and "executed according to an overarching strategy designed to maximize their combined power to advance the movement-defined goal."[121] Within these integrated advocacy campaigns, lawyers can themselves directly implement a diverse combination of tactics or may be coordinating different tactics implemented by others.[122]

The increased use of an integrated advocacy model and this layered approach is rooted in academic literature and empirical research on how to build and support social movements and the role of lawyers in most effectively supporting social change. As Austin Sarat and Stuart Scheingold explored, lawyers can contribute most compellingly to social movements "often not as a direct result of the outcomes of litigation," but indirectly by "lawyering outside the lines" and deploying the law 'strategically' in many realms.[123] This work of strategic lawyering can include litigation in the courts, but also work in legislatures, public and private institutions, and the court of public opinion to politicize grievances, mobilize activists and build, maintain, and drive social movements.

Deborah Rhode and Scott Cummings have also written extensively on public interest lawyering. Rhode and Cummings' 2009 work, *Public Interest Litigation: Insights from Theory and Practice*, highlighted that a key lesson from law

120. *Id.*

121. Cummings, *supra* note 119 at 1704.

122. *Id.*

123. CAUSE LAWYERS AND SOCIAL MOVEMENTS 9–11 (Austin Sarat & Stuart A. Scheingold eds., 1st ed. 2006).

and social change research is the importance of situating litigation within broader political campaigns—of using it as means to an end, rather than an end in itself."[124] There has been a continued growth of lawyering for social justice that has structurally moved beyond just using multiple legal approaches to proactively and effectively use integrated advocacy.[125] Rather than seen as lawyering outside the lines, as Sarat and Scheingold described it in 2006, integrated advocacy is recognized by modern movement lawyering as necessary to effectively support social change. That effective public interest lawyering is more than technical legal skill, especially litigation. It encompasses a broader set of skills in the "art of persuasion across strategies"—telling compelling stories to those with decision-making power and the wider public to exert pressure and build support for political and cultural change.[126] Integrated advocacy is used to create what I characterize as virtuous cycles.[127] Cummings describes it as "embedding change at one level that creates positive feedback loops in others" and produces a "widening circle of democratic transformation."[128]

In the area of technology, integrated advocacy and layered lawyering is particularly critical since technical advances can quickly make existing law obsolete or make a legal issue outdated before a court case reaches its conclusion. For example, the U.S. Supreme Court was still deciding privacy cases about electronic beepers in the 1980s.[129] The Court did not decide its first case about cell phone privacy until 2014 in *Riley v. California*. By then, as Chief Justice John Roberts noted, cell phones were "now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[130]

The development of a more cohesive integrated advocacy model for legal change began in earnest in the late 1990s and early 2000s as a response to more diverse perspectives and constituencies, a growing conservatism in the courts and the public, and the existence of more organizations with more resources

124. *Id.* at 615–16.

125. Cummings, *supra* note 119.

126. *Id.* at 1703.

127. Nicole Ozer, *Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. L. & SOC. CHANGE 215, 220, 255 (2012).

128. Cummings, *supra* note 119 at 1715.

129. United States v. Karo, 468 U.S. 705 (1984).

130. Riley v. California, 573 U.S. 373, 385 (2014), (warrantless search and seizure of a cell phone's digital contents during an arrest unconstitutional); *see also* Brief of ACLU, ACLU of NorCal, ACLU of SoCal, and ACLU of San Diego and Imperial Counties as Amici Curiae in Support of Petitioner, Riley v. California, 573 U.S. 373 (2014) (no. 13-132), https://www.aclu.org/cases/riley-v-california?document=riley-v-california-aclu-amicus-brief.

that could support multiple strategies.[131] But as Cummings notes, the features of integrated advocacy are not "entirely discontinuous with past movement lawyering practice . . . progressive lawyers have long used coordinated legal and political tactics to challenge power and solve social problems."[132] The use of this layered lawyering and integrated advocacy approach was already readily apparent in the late 1960s and early 1970s in the ACLU and ACLU of Northern California's work on privacy and technology.

3. California Constitutional Privacy Was Passed as Part of Integrated Advocacy Work on Technology, Rights, and Democracy

The development and passage of the California constitutional right to privacy was not isolated work. It was part of an integrated advocacy approach that the ACLU was already using both on the federal level and in California in the late 1960s and early 1970s to work on issues at the intersection of technology, rights, and democracy.

By the 1960s, the ACLU was actively engaged in legal work related to privacy, much of it at the intersection of gender, sexuality, and reproductive justice and policing and criminal justice. The ACLU filed an amicus brief and argued in front of the U.S. Supreme Court in *Mapp v. Ohio*, the 1961 case holding that the Fourth Amendment's protections against illegal search and seizure applied to proceedings in state courts as well as proceedings in federal courts.[133] The ACLU also filed an amicus brief in the Court's privacy decision in *Griswold v. Connecticut* in 1965, striking down that state's anti-contraceptive statute.[134] ACLU cooperating attorneys litigated the seminal Fourth Amendment "stop and frisk" policing case, *Terry v. Ohio*, decided by the U.S. Supreme Court in 1968.[135] In 1972, in an extension of the Court's evolving privacy doctrine, the ACLU reversed the conviction of a reproductive rights activist who had given a contraceptive device to an unmarried Massachusetts woman in *Eisenstadt v. Baird*.[136]

Archive documents show that those working on the California constitutional right to privacy were well aware of the development of privacy

131. Deborah L. Rhode, *Public Interest Law: The Movement at Midlife*, 60 STAN. L. REV. 2027, 2049 (2008), https://www.jstor.org/stable/40040430.

132. Cummings, *supra* note 119 at 1696.

133. Mapp v. Ohio, 367 U.S. 643 (1961).

134. Griswold v. Connecticut, 381 U.S. 479 (1965); *see also Timeline of Important Reproductive Freedom Cases Decided by the Supreme Court*, ACLU (2003), https://www.aclu.org/documents/timeline-important-reproductive-freedom-cases-decided-supreme-court.

135. Terry v. Ohio, 392 U.S. 1 (1968).

136. Eisenstadt v. Baird, 405 U.S. 438 (1972); *see also The Success of the American Civil Liberties Union*, ACLU, https://www.aclu.org/successes-american-civil-liberties-union.

jurisprudence in the U.S. Supreme Court and felt that while those cases were helpful, they were not sufficient. As Assemblymember Cory articulated,

> When our constitution was adopted the First, Third, Fourth, Fifth, and Ninth Amendments offered sufficient protection of individual privacy. In the era of the computerized data banks, increased government surveillance and the pervasiveness of government in everyone's lives, a clearer statement of our rights is needed. ACA 51 is an attempt to shore up our constitutional rights and perserve [sic] our heritage of freedom and individual privacy.[137]

The Privacy Amendment was a deliberate effort to buttress the privacy rights already protected by the Fourth Amendment and the corollary state constitutional right against unreasonable search and seizure and make a new explicit constitutional right to privacy in California to guarantee broader and stronger protections against modern threats to privacy.[138] The Privacy Amendment would protect against privacy invasions by both government and private parties and also not perpetuate the "reasonable expectation of privacy" test that put the burden on people to justify that their rights needed to be protected. Rather, the new constitutional right would affirmatively protect people's privacy by default and require the government or business to show a compelling interest to overcome this fundamental right. This right would be a distinct and critical legal lever to protect privacy as technology was advancing and address how government and private parties could increasingly collect and use information for surveillance and threaten rights, safety, and democracy.

As early as 1967, the ACLU and the ACLU of Northern California developed integrated advocacy work in Congress, the California legislature, state and federal courts, as well as strategic communications and public education. ACLU archives reveal that a 1967 federal proposal to create a "national data center" or "databank" sparked some of the first considerable debate on technology and privacy issues. As discussed earlier, Art Speiser of the ACLU's Washington office testified in opposition. He highlighted both big picture concerns about the system as a whole and the threats of biased and error-prone information. These risks still stand the test of time more than fifty-five years later, sparking current conversations about data brokers and the

137. Letter from Kenneth Cory to the Legislative File, (1972), https://www.aclunc.org/sites/default/files/Letter%20Response%20to%20Chairman%20Ignazio%20Vella%20from%20Hon.%20Kenneth%20Cory.pdf.

138. The California Constitution has included a state corollary to the Fourth Amendment protections against unreasonable search and seizure since the first state constitution in 1849. CAL. CONST. of 1849 art. I. § 19. The constitutional protection against unreasonable search and seizure is the modern-day Article I, Section 13 of the California Constitution. CAL. CONST. art. I, § 13.

potential impact of new artificial intelligence systems on access and opportunity.[139] Speiser observed:

> [T]here is a considerable interchanging of data among government and private sources. Once an unreliable bit of information makes its way into a file it forms an indelible mark on a person's record. The individual who is denied the chance of employment or some other opportunity on the basis of such information is given no chance to rebut or disprove it. Dossiers are compiled, the accuracy of which increasingly becomes questionable.[140]

The ACLU of Northern California was also working on issues of technology and privacy in the California legislature, prioritizing efforts to halt police-sponsored legislation to extend wiretapping and other electronic eavesdropping authority to state officials. The organization successfully stopped two bills that would have authorized these police surveillance powers in 1968[141] and continued to fight wiretapping expansion—law enforcement's "number one legislative priority."[142] In 1971, the ACLU, with additional support from the Public Defender's Association and the State Bar, again stopped multiple bills to authorize wiretapping and electronic eavesdropping.[143]

In 1971, the ACLU was also actively engaged in a series of Congressional hearings on "Federal Data Banks, Computers, and the Bill of Rights" in the Subcommittee on Constitutional Rights of the Senate Judiciary Committee. Senator Sam Ervin, who chaired this series of eleven hearings from February 23 to March 17, 1971, explained that they were "called because it is clear from the complaints being received by Congress that Americans in every walk of life are concerned about the growth of government and private records on individuals."[144] In his testimony on behalf of the ACLU for these hearings, New York Civil Liberties Union staff counsel Burt Neuborne[145] presciently

139. *Lawrence Speiser's Testimony: The Proposed Federal Data Center*, ACLU OF N. CAL. NEWS VOL. 32, NO. 4, at 3 (Apr. 1967), https://digitallibrary.californiahistoricalsociety.org/object/15631?islandora_paged_content_page=3.

140. *Id.*

141. ACLU OF N. CAL. NEWS VOL. 33, NO. 8 (Aug. 1968), https://digitallibrary.californiahistoricalsociety.org/object/15658.

142. ACLU OF N. CAL. NEWS VOL. 37, NO. 3 (Apr. 1972).

143. *Id.*

144. *Federal Data Banks, Computers, and the Bill of Rights: Hearings Before the Subcommittee on Constitutional Rights of the Committee of the Judiciary*, 92nd Cong. at 1 (1971), https://babel.hathitrust.org/cgi/pt?id=uc1.c051765460&view=1up&seq=19&q1=aclu.

145. Burt Neuborne is the Norman Dorsen Professor of Civil Liberties at NYU Law School. He started his ACLU career in 1967 as a staff counsel at the New York Civil Liberties

connected the societal impact dots between emerging technology power on people and democracy. He explained:

> [a]s with almost every field of technological advance, we are faced in the area of surveillance with the dilemma of controlling the technological Frankensteins we have created. In the industrial area, production technology threatens the physical ecology of our continent; in the political area, surveillance technology threatens the psychological ecology of the democratic spirit. If we are to survive . . . we must insure [sic.] that the delicate sense of freedom which is depending upon a commitment to individual privacy is not destroyed in the often spurious name of 'efficiency.'[146]

In that same testimony, the ACLU also submitted materials from its 1971 Biennial Conference. At the conference, the organization adopted a resolution to study the civil liberties impact of all local, state and federal laws related to data collection, storage and dissemination. It also proposed the creation of a national committee to grapple directly with the issues of data privacy and develop a public education program for these issues.[147]

Once created, the National Privacy Committee of the ACLU worked with ACLU leadership and staff to plan and implement integrated advocacy approaches to build momentum on technology and privacy issues. ACLU archives include correspondence about both the planning and implementation of strategies combining academic writing, testimony on state and federal legislative and agency work, coalition development, and strategic communications including opinion pieces and other public education materials by prominent legal scholars.[148]

By 1971, the ACLU was engaged in both proactive state and federal court litigation and legislative work on technology and privacy. The ACLU of Northern California filed the "first computer privacy suit" in San Francisco Superior Court in December 1971.[149] The case was filed on behalf of California social workers who had been suspended from work without pay for upholding

---

Union (NYCLU)—and then served from 1981–1986 as ACLU National Legal Director. In 1995, he co-founded the Brennan Center for Justice at NYU and served as its founding legal director until 2007. *Burt Neuborne Bio*, ACLU, https://www.aclu.org/bio/burt-neuborne.

146. *Federal Data Banks, Computers, and the Bill of Rights: Hearings Before the Subcommittee on Constitutional Rights of the Committee of the Judiciary*, 92nd Cong. at 64 (1971), https://babel.hathitrust.org/cgi/pt?id=uc1.c051765460&view=1up&seq=82&q1=aclu.

147. *Id.*

148. Variety of memoranda, letters, and other 1970 and 1971 documents discussing strategic plans to address privacy and computerization issues. American Civil Liberties Union Records MC#001 Box 1097 Folder 14 Surveillance Date(s) 1971.

149. ACLU OF N. CAL. NEWS VOL. 36, NO. 11, at 4 (Dec. 1971), https://digitallibrary.californiahistoricalsociety.org/object/15869.

their professional ethics and refusing to participate in a new "computer surveillance system."[150] The new system required them to collect personal information from clients about "alcoholism, sex offense, or mental illness" for inclusion in computer storage without assurance that there would be limitations on access to this information by outside interests.[151] In 1972, the ACLU of Northern California and the ACLU also filed a lawsuit against the "so-called Bank Secrecy Act" passed by Congress in 1970, which required banks to report information about financial transactions directly to the government without consultation with the customer.[152] The ACLU also applauded the introduction of the Financial Records Privacy Act, a federal bill for banking privacy that would establish default privacy protections for banking records by requiring an individual's consent, a subpoena, or a probable cause order for the government to obtain information outside regular auditing procedures. It also prohibited any information obtained to be used or retained for a purpose other than for which it was originally sought.[153]

The ACLU of Northern California also worked extensively on government surveillance and privacy issues. When a Sacramento Superior Court judge ruled in favor of the release of state documents about covert surveillance by Law Enforcement Intelligence Units, formerly known as "red squads," he noted the organization's deep engagement in the privacy field. "This court is unaware of any organization or individual more actively concerned with an[d] engaged in defending and protecting constitutional rights and resisting unlawful invasions of privacy by over-zealous spying, surveillance, and covert activities than the plaintiff [ACLU of Northern California]."[154]

By the mid-1970s, the ACLU's work on information privacy also included thought-provoking television public service announcements.[155] The PSAs developed by experimental filmmaker Godfrey Reggio for the New Mexico Civil Liberties Union pushed people to consider the impact of surveillance dossiers on democracy, how surveillance undermined the privacy of the home

150. *Id.*

151. *Id.*

152. ACLU OF N. CAL. NEWS VOL. 37, NO. 5, (June 1972), https://digitallibrary.californiahistoricalsociety.org/object/16066?solr_nav%5Bid%5D=463aa21840a90a89b7ca&solr_nav%5Bpage%5D=0&solr_nav%5Boffset%5D=4.d.

153. ACLU OF N. CAL. NEWS VOL. 44, NO. 1, at 2 (Feb. 1979), https://digitallibrary.californiahistoricalsociety.org/object/16058.

154. ACLU OF N. CAL. NEWS VOL. 37, NO. 6, at 2 (Aug. 1972), https://digitallibrary.californiahistoricalsociety.org/object/16448?islandora_paged_content_page=2.

155. *See Public Service Announcements by the New Mexico Civil Liberties Union (Godfrey Reggio)*, YOUTUBE (1974), https://www.youtube.com/watch?v=yah54al6Cks (last visited Sept. 21, 2023).

and family and childhood safety, and asked people to consider if they were unthinkingly adopting technology like rats in a maze eating cheese.

A longer PSA that described the purpose of the short films explained:

> Our ads from the last few weeks, different from what you usually see, have tried to raise questions that we feel are extremely important. As the first generation of the technological society, that we have been acted on by forces of such power that few of any of us can understand.
>
> Extensive information gathering on every American . . . electronic surveillance.
>
> The era of the computer, invasion of privacy.
>
> Growing government and corporate power over our lives, a people plagued by dehumanization, loneliness and violence.
>
> Dramatic? Perhaps.
>
> But we are losing control of our technology and our lives. Not so long ago, people in a similar situation did not awaken to the forces around them. Are we so unwise as to do the same?

The scope and language of the California constitutional right to privacy both echoed and reinforced all this nascent integrated advocacy work happening across the country. When the constitutional right to privacy passed, it also further propelled important work forward in the courts, legislatures, and other arenas.

III. THE IMPACT OF THE CALIFORNIA CONSTITUTIONAL RIGHT TO PRIVACY

A. CALIFORNIA CONSTITUTIONAL RIGHT TO PRIVACY SUPPORTED WIDE-RANGING CHANGE

The passage of the California constitutional right to privacy, with its foundation in the intersectional movement work happening at the time, and its deep understanding of the connection between consumer privacy, government surveillance, autonomy, freedom, and democracy, has both protected and advanced rights across legal and policy arenas.

1. California Constitutional Right Supported Privacy Change in the Courts

The California constitutional right to privacy immediately changed the trajectory of legal decisions in California courts, putting California jurisprudence at the vanguard of protecting both informational privacy and autonomy privacy. In *White v. Davis*, the first California Supreme Court case to

interpret the Privacy Amendment, the Court held 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."[156] The California Supreme Court further highlighted that this surveillance operation in many ways "epitomizes" what the new constitutional amendment condemns,[157] since the "moving force behind the new constitutional provision was a more focused privacy concern, relating to the accelerating encroachment on personal freedom and security caused by increased surveillance and data collection activity in contemporary society."[158]

In this case of first impression, the Court engaged in important interpretation of the language of the ballot measure, including the compelling interest language and how it should be used by the courts in adjudicating privacy claims. The Court discussed that the party engaged in the privacy-invading conduct must establish a compelling interest to justify the intrusion—three separate times in the opinion. First, it discussed the need for compelling interest in relation to the government surveillance in the instant case. The Court explained that the Privacy Amendment "require[s] that the government establish a compelling justification for such conduct."[159] Second, the Court explained that at trial, "defendant will be free . . . to designate the compelling governmental interests upon which they rely for their intrusive conduct."[160]

The third time the Court discussed the required demonstration of "compelling interest" was in its discussion of the broad scope of the California constitutional right to privacy and how it related to privacy incursions by both government and business interests. This section of the *White v. Davis* decision quoted heavily from the ballot brochure statement, which the California Supreme Court found to be the Privacy Amendment's legislative history and used to construe the state's constitutional right to privacy.[161] The court highlighted that the ballot argument stated "[t]his right should be abridged only when there is a compelling public need."[162] The court also took care to highlight that "several important points emerge from this election brochure 'argument.'"[163] It then identified the "principal mischiefs" at which the

156. White v. Davis, 533 P.2d 222, 224 (Cal. 1975).
157. *Id.* at 234.
158. *Id.* at 233.
159. *Id.* at 225.
160. *Id.* at 234.
161. *See id.* at n. 11.
162. *Id.* at 234.
163. *Id.*

amendment is directed, including privacy incursions by both the government and business interests:

> (1) '[G]overnment snooping' and the secret gathering of personal information; (2) the overbroad collection and retention of unnecessary personal information by government and business interests; (3) the improper use of information properly obtained for a specific purpose, for example, the use of it for another purpose or the disclosure of it to some third party; and (4) the lack of a reasonable check on the accuracy of existing records.[164]

After the court delineated these "principal mischiefs" related to privacy incursions by either government or business, it held that the ballot statement also made clear "that the amendment does not purport to prohibit all incursion into individual privacy" "but . . . that any such intervention must be justified by a compelling interest."[165]

The decision in *White v. Davis* provided important clarity for the reach of the California constitutional right to privacy and moved it from paper to practice. It reinforced an expansive standing right for Californians to be heard in court on privacy claims, finding that the Privacy Amendment is intended to be self-executing—"that the constitutional provision, in itself, 'creates a legal and enforceable right of privacy for every Californian.'"[166] The Court also made it clear that the compelling interest language in the Privacy Amendment requires that the government or business interest bears the responsibility of demonstrating or establishing that a compelling interest justifies the privacy incursion. At the pleading stage in *White v. Davis*, no such compelling interest justification was present, so the Court reversed the judgement on the demurrer and remanded for trial on the merits.

Several other cases in the late 1970s and early 1980s further fleshed out the contours of the constitutional right to privacy and the compelling interest standard. For example, in *Long Beach City Employees Assn. v. City of Long Beach*, the Court analyzed whether a statutory scheme to require polygraph examinations of city employees violated the state's constitutional right to privacy.[167] The Court looked to the scope of the privacy right, highlighted the ballot measure language, and noted that "if there is a quintessential zone of human privacy it is the mind."[168] The Court found that polygraph examinations "inherently intrude upon the constitutionally protected zone of

164. *Id.*
165. *Id.*
166. *Id.*
167. Long Beach City Emps. Assn. v. City of Long Beach, 719 P.2d 660, 666 (Cal. 1986).
168. *Id.* at 663.

individual privacy," and no compelling interest offered by the City of Long Beach justified the city's conduct.[169] In *City of Santa Barbara v. Adamson*, the Court reinforced that people have a right to privacy in their family and also their home and the government must demonstrate a compelling interest to justify the invasion.[170] In *Loder v. Municipal Court*, the Court used the compelling interest test in determining limited retention and dissemination of arrest records.[171] In the same year, the Court also found a prima facie violation of the state constitutional right of privacy when information was used for another purpose in *Porten v. University of San Francisco*.[172] Further, in *Britt v. Superior Court*, the Court found that a discovery order compelling disclosure of plaintiffs' activities in local political associations, including affiliations with organizations that had protested defendant's operations, was an unconstitutional infringement of plaintiffs' privacy rights protected by Article I, Section 1, and rights to free expression.[173]

2. *California Constitutional Privacy Supported Privacy Change in the Legislature*

The passage of the California constitutional right to privacy also spurred political action to pass dozens of cutting-edge state privacy laws in both the government surveillance and consumer privacy contexts. Several of the laws helped operationalize the inalienable right to privacy by prohibiting privacy intrusions, rather than requiring Californians to go to court for redress after they have already suffered invasions of their privacy.[174] It set California on a trajectory of passing many of the strongest privacy laws in the nation.

---

169. *Id.* at 666.

170. City of Santa Barbara v. Adamson, 610 P.2d 436, 440 (Cal. 1980).

171. Loder v. Mun. Court, 553 P.2d 624, 628 (Cal. 1976).

172. Porten v. Univ. of S.F., 134 Cal. Rptr. 839 (1976).

173. The California Supreme Court also made important decisions on autonomy privacy. *See* Comm. to Defend Reproductive Rights v. Myers, 625 P.2d 779, 791–97 (Cal. 1981) (invalidating state law that refused to pay medical expenses of poor women who chose to have an abortion; compelling state interest required to overcome indigent woman's privacy interest in reproductive rights; "By virtue of the explicit protection afforded an individual's inalienable right of privacy by Article I, Section 1 of the California Constitution . . . the decision whether to bear a child or to have an abortion is so private and so intimate that each woman in this state -- rich or poor -- is guaranteed the constitutional right to make that decision as an individual, uncoerced by governmental intrusion.").

174. California is also a national leader in statutory laws to protect autonomy privacy and reproductive rights specifically. *Your Legal Right to an Abortion*, CA.GOV, https://abortion.ca.gov/your-rights/your-legal-right-to-an-abortion/ (last visited May 6, 2024); *Your Privacy*, CA.GOV, https://abortion.ca.gov/your-rights/your-privacy/; *Know Your Rights: Abortion Access California*, ACLU OF N. CAL. (Mar. 2023), https://www.aclunc.org/our-work/

This legacy includes laws like the California Information Practices Act of 1977 (IPA), designed to help "implement the privacy amendment" by placing strict limits on the maintenance and dissemination of personal information by state agencies.[175] The law reiterated that the right to privacy is "a personal and fundamental right" and "that all individuals have a right of privacy in information pertaining to them." In the IPA's declaration of purpose, the Legislature stated that the right to privacy was being threatened by "the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies." Further, the "increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."[176]

The legacy of the California constitutional right to privacy also includes landmark laws related to surveillance. The California Reader Privacy Act, enacted in 2011, robustly protects the privacy of reading records in the digital age.[177] Its legislative history explained that it "updates reader privacy laws by mirroring the strong privacy and free speech standards in California law—ensuring that government and third parties cannot compel disclosure of private reading records without proper justification." The law requires both government and third parties to demonstrate to a court a compelling interest and that they are using the least intrusive means.[178]

The California Electronic Communications Privacy Act (CalECPA), enacted in 2015, and hailed as the "nation's best privacy law,"[179] updated California statutory surveillance privacy law for the modern digital age by requiring a warrant for any government demand for electronic communications information (everything from emails and text messages to online documents and metadata) and search electronic devices. The legislative history for CalECPA made clear that it was a statutory update to support the

know-your-rights/know-your-rights-abortion-access-california#item-2961; Press Release, Office of Governor Gavin Newsom, California Expands Access and Protections for Reproductive Health Care (Sept. 27, 2023), https://www.gov.ca.gov/2023/09/27/california-expands-access-and-protections-for-reproductive-health-care/.

175. CAL. CIV. CODE §1798.

176. CAL. CIV. CODE § 1798.1(a)-(b), subdiv. (a) and (b).

177. CAL. CIV. CODE § 1798.90; *Reader Privacy Act Signed into Law*, ACLU OF N. CAL. (Oct. 3, 2011), https://www.aclunc.org/blog/reader-privacy-act-signed-law.

178. *SB 602 (Yee) Reader Privacy Act of 2011: Updating California Book Privacy Law*, ACLU OF N. CAL. (2011), https://www.aclunc.org/sites/default/files/asset_upload_file991_9996.pdf.

179. Kim Zetter, *California Now Has the Nation's Best Privacy Law*, WIRED (Oct. 8, 2015), https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/.

constitutional privacy and free speech protections of Californians.[180] California State Senator Mark Leno distributed a fact sheet about the statute, explaining that "Californians are guaranteed robust constitutional rights to privacy and free speech . . . however, the emergence of new technology has left California's statutory protections behind . . . this bill will provide needed protection against warrantless government access."[181]

The constitutional right also undergirds numerous privacy laws that protect against the use of surveillance technology. These laws include landmark laws against Radio Frequency Identification technology,[182] face surveillance[183] and automated license plate readers.[184]

California has also been the national leader in enacting transparency laws related to consumer privacy. In 2003, California became the first state to require businesses and state agencies to alert Californians affected by a data breach.[185] In 2004, it became the first state to require websites to have a privacy policy.[186] California has also passed multiple laws that provide a statutory right for people to know about information collection and delete personal information that is collected about them. California's Shine the Light law, passed in 2003, gives Californians the right to know the "who, what, where, and when" of how a business handles personal information."[187] In 2018,

180. "Californians are guaranteed robust constitutional rights to privacy and free speech . . . however, the emergence of new technology has left California's statutory protections behind . . . this bill will provide needed protection against warrantless government access to mobile devices, email, text messages, digital documents, metadata, and location information." *Fact Sheet SB 178 (LENO and ANDERSON)*, OFFICE OF SENATOR MARK LENO (Sept. 2, 2015), https://www.aclunc.org/sites/default/files/SB%20178%20CalECPA%20Fact%20Sheet_1.pdf.

181. *Id.*

182. CAL. CIV. CODE § 1798.79; Nicole Ozer, *Rights "Chipped" Away: RFID and Identification Documents*, STAN. TECH. L. REV. 1 (2008).

183. *The Body Camera Accountability Act (AB 1215)*, ACLU, https://www.aclunc.org/our-work/legislation/body-camera-accountability-act-ab-1215.

184. CAL. CIV. CODE § 1798.90.5; *Lagleva v. Doyle (License Plate Surveillance)*, ACLU (June 2, 2022), https://www.aclunc.org/our-work/legal-docket/lagleva-v-doyle-license-plate-surveillance.

185. CAL. CIV. CODE §§ 1798.29, 1798.82, 1798.84.

186. CAL. BUS. & PROF. CODE, §§ 22575–22579.

187. SENATE JUDICIARY COMMITTEE, ANALYSIS OF SB 27 (S. Cal. 2003), http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_0001-0050/sb_27_cfa_20030507_132723_sen_comm.html; *see* 2003 CAL. STAT. 3891/. Unfortunately, it became more difficult for individuals to effectively using this landmark Shine the Light law over time as technology advanced and business practices changed dramatically and the law's definition of "direct marketing purposes" as solicitation by postal mail, telephone, or email was supplanted by companies increasingly collecting and then sharing and selling information

California also passed the California Consumer Privacy Act (CCPA), which enabled Californians to know more about how companies collect, use and share personal information and provides deletion rights and the ability to opt out of the sale of personal information.[188] Today, many of these laws provide the opportunity for tens of millions of people to understand more about how personal information is collected, used, shared and sold and take steps to try to better control their personal information.[189]

The constitutional right to privacy has also been an important lever for other integrated advocacy strategies, including successfully pushing California-based technology companies to adopt corporate policies that protect against

---

with online advertisers, third party applications, and data brokers. There were also additional procedural and legal obstacles to its efficient and effective use by Californians. *See* Nicole Ozer & Matt Cagle, *Losing the Spotlight: A Study of California's Shine the Light Law*, ACLU OF N. CAL. (2013), https://www.aclunc.org/sites/default/files/Losing%20the%20Spotlight%20-%20A%20Study%20of%20California%27s%20Shine%20the%20Light%20Law%20final.pdf. I developed an update to Shine the Light sponsored by the ACLU of California in 2013—California Right to Know Act (AB 1291-Lowenthal)—to provide Californians with transparency about how personal information is collected and shared in the entire data ecosystem—with online advertisers, data brokers, and third-party services. Unfortunately, it faced robust opposition and intense lobbying from the technology industry and was not able to make it through the legislative process. *Right to Know Act (AB 1291)*, ACLU, https://www.aclunc.org/our-work/legislation/right-know-act-ab-1291.

188. CAL. CIV. CODE §§ 1798.110, 1798.105, 1798.120; *id.* at § 1798.140(ah)(1); *California Consumer Privacy Act (CCPA)*, OFF. OF THE ATT'Y GEN., (2024), https://oag.ca.gov/privacy/ccpa. The CCPA used some of the foundational transparency concepts developed for the Right to Know Act, but the ACLU did not support CCPA and opposed Proposition 24 because of its loopholes and because it too heavily put the burden on people to protect themselves. Jacob Snow & Chris Conley, *Californians Should Vote No on Prop 24*, ACLU OF N. CAL. (Oct. 16, 2020), https://www.aclunc.org/blog/californians-should-vote-no-prop-24. I helped develop, and the ACLU in California supported, the 2019 Privacy for All (AB 1760 – Wicks). *ACLU Supports New California Bill to Ensure Privacy for All*, ACLU OF N. CAL. (Feb. 27, 2019), https://www.aclunc.org/news/aclu-supports-new-california-bill-ensure-privacy-all.

189. Some California privacy laws help not only Californians, but also people beyond its borders because their legal requirements are applicable to any business that collects information about individuals in California. Since it can be difficult for the business to ascertain Californian residents with certainty, there are compliance efficiency benefits to applying California law to all users. In this manner, many California privacy laws provide protections to people across the country. *See. e.g.*, Online Privacy Protection Act of 2003, CAL. BUS. & PROF. CODE, §§ 22575–22579 (requiring any operator of commercial web sites or online services that collect personal information on California consumers through a web site to conspicuously post a privacy policy on the site and to comply with its policy); *see also* Julie Brill, *Microsoft Will Honor California's New Privacy Rights Throughout the United States*, MICROSOFT: ISSUES (Nov. 11, 2019), https://blogs.microsoft.com/on-the-issues/2019/11/11/microsoft-california-privacy-rights/ ("Microsoft will honor California's new privacy rights throughout the United States").

surveillance of people in the state and around the world.[190] For example, following an investigation by the ACLU of Northern California on widespread social media surveillance by local police, including of racial justice activists,[191] an ACLU of Northern California-led coalition of civil rights organizations including MediaJustice and Color of Change, successfully advocated for Facebook, Instagram, and Twitter to strengthen their worldwide policies related to social media surveillance and stop sharing information.[192]

B. CALIFORNIA CONSTITUTIONAL PRIVACY AT FIFTY YEARS HAS NOT YET ACHIEVED ITS FULL PROMISE

Though there have been many successes in the past fifty years, the challenges to translate California's inalienable privacy rights into practice have been formidable. Police and other government agencies and private parties have consistently tried to violate rights and undermine the proper scope and reach of the California constitutional right to privacy. As Cummings and Rhode noted, "judicial decrees without a political base are vulnerable to chronic non-compliance, public backlash, statutory reversal, or judicial retrenchment."[193] Here, the California constitutional right to privacy was enacted by a substantial margin of voters, not by judicial decree. But the importance of the political base is still a critical element to the trajectory of the

190. Elizabeth Dwoskin, *Facebook Says Police Can't use its Data for 'Surveillance'*, WASH. POST: THE SWITCH (Mar. 13, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/13/facebook-says-police-cant-use-its-data-for-surveillance/; *ACLU Demands Twitter Take Immediate Action to Stop Developers from Facilitating Government Surveillance of Users*, ACLU OF N. CAL. (July 9, 2020), https://www.aclunc.org/news/aclu-demands-twitter-take-immediate-action-stop-developers-facilitating-government.

191. Nicole Ozer, *Police Use of Social Media Surveillance Software Is Escalating, and Activists Are in the Digital Crosshairs*, ACLU (Sept. 22, 2016), https://www.aclu.org/news/privacy-technology/police-use-social-media-surveillance-software; Sam Levin, *ACLU Finds Social Media Sites Gave Data to Company Tracking Black Protesters*, GUARDIAN (Oct. 11, 2016), https://www.theguardian.com/technology/2016/oct/11/aclu-geofeedia-facebook-twitter-instagram-black-lives-matter; Craig Timberg & Elizabeth Dwoskin, *Facebook, Twitter and Instagram Sent Feeds that Helped Police Track Minorities in Ferguson and Baltimore, Report Says*, WASH. POST: THE SWITCH (Oct. 11, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/10/11/facebook-twitter-and-instagram-sent-feeds-that-helped-police-track-minorities-in-ferguson-and-baltimore-aclu-says/.

192. *Facebook and Instagram Publicly Prohibit Surveillance of Users Following Coalition Demands*, ACLU OF N. CAL. (Mar. 10, 2017), https://www.aclunc.org/news/facebook-and-instagram-publicly-prohibit-surveillance-users-following-coalition-demands; BYRON TAU, MEANS OF CONTROL: HOW THE HIDDEN ALLIANCE OF TECH AND GOVERNMENT IS CREATING A NEW AMERICAN SURVEILLANCE STATE 106 (2024).

193. Scott L. Cummings & Deborah L. Rhode, *Public Interest Litigation: Insights From Theory and Practice,* 36 FORDHAM URB. L.J. 603, 647 (2009).

California constitutional right to privacy over the past decades and why it has not yet achieved its full promise.

As early as 1980, the *ACLU News* reported how the right was not being followed—"[t]he right to privacy has been explicitly guaranteed by the California Constitution since 1972, yet the translation of that principle into practice continues to challenge the ACLU. Abuses of this right by state and private agencies are still the norm."[194] Efforts to address the noncompliance and enforce the privacy right in the courts have been mixed. The California Supreme Court issued strong early rulings in the 1970s and early 1980s like *White v. Davis* and others discussed above. But the California Supreme Court showed an unfortunate tentativeness to fully enforce the reach of the constitutional right and erected regrettable roadblocks to actually enforcing the inalienable right to privacy in later cases, most notably *Hill v. National Collegiate Athletic Association.*[195]

1. Hill v. NCAA *and Its Profound Impact on Privacy Law in the Digital Age*

The *Hill v. NCAA* case, decided by the California Supreme Court in 1994, had a substantial impact on the trajectory of privacy law and the inability of people to fully utilize the California constitutional right to privacy to protect their rights in the modern digital age.

In 1987, the ACLU of Northern California brought the *Hill* case on behalf of student athletes at Stanford University who refused to consent to a new random and suspicionless drug testing program promulgated by the National Collegiate Athletic Association (NCAA).[196] *Hill v. NCAA* was a case of first impression for the California Supreme Court to rule on a constitutional privacy

194. *See* White v. Davis, 533 P.2d 222 (Cal. 1975), (police surveillance and data gathering activities of UCLA professor constitute a prima facie violation of the recently enacted state constitutional right of privacy); *see* ACLU OF N. CAL. NEWS VOL. 45, NO. 8, at 8 (1980), https://digitallibrary.californiahistoricalsociety.org/object/16534 ("The right to privacy has been explicitly guaranteed by the California Constitution since 1972, yet the translation of that principle into practice continues to challenge the ACLU. Abuses of this right by state and private agencies are still the norm.").

195. Hill v. Nat'l Collegiate Athletic Assn., 865 P.2d 633 (Cal. 1994); *see also* ACLU OF N. CAL. NEWS, VOL. 58, NO. 2, (Apr. 1994), https://digitallibrary.californiahistoricalsociety.org/object/17286; *see also* Rodolfo R. Aquino, *California's Constitutional Privacy Guarantee Needs a Reset*, SCOCABLOG (Apr. 9, 2021), https://scocablog.com/californias-constitutional-privacy-guarantee-needs-a-reset/.

196. *See* ACLU OF N. CAL. NEWS, VOL. 58, NO. 2, (Mar. 1994), https://digitallibrary.californiahistoricalsociety.org/object/17277?solr_nav%5Bid%5D=3195769d9b34197f364e&solr_nav%5Bpage%5D=0&solr_nav%5Boffset%5D=14.

case against a private party. It was the opportunity to move the equal reach of the constitutional right to government and private party action from paper to practice, and to exercise the principle that any privacy incursion must be justified by a compelling interest—as explicitly articulated in the ballot language and recounted lucidly in *White v. Davis*.

In 1994, the California Supreme Court issued its decision in *Hill*, and properly held that the privacy right applies to private parties. The Court noted that "[t]he repeated emphasis in the competing ballot arguments on private party relationships and transactions, as well as individual encounters with government, underscores the efforts of the Privacy Initiative's framers to create enforceable privacy rights against both government agencies and private entities."[197] The Court acknowledged its earlier holding about the scope of the Privacy Amendment in *White v. Davis*, "[a]s we have recognized: '[T]he overbroad collection and retention of unnecessary personal information by government and business interests' was one of the principal 'mischiefs' at which the Privacy Initiative was directed."[198] Further, it recognized that "the ballot arguments contain persuasive evidence of drafter and voter intent to recognize a right of action for invasion of privacy against private as well as government entities."[199] It concluded, "the Privacy Initiative in article I, section 1 of the California Constitution creates a right of action against private as well as government entities."[200]

But after hewing to drafter and voter intent with the scope of the privacy right, the Court then kneecapped the constitutional right to privacy in multiple ways. The Court subverted the burden by bolting on a new expectation that plaintiffs establish three threshold elements to allege a privacy invasion under Article I, Section 1: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant constituting a serious invasion of privacy. Pursuant to *Hill*, the three threshold elements are required to allege any constitutional privacy claim. These new elements to the claim adopted the "reasonable expectation of privacy" from Fourth Amendment jurisprudence and devised a "serious invasion" of privacy requirement, neither of which was consistent with the legislative history or ballot language of the constitutional right to privacy. Then after placing this high burden on the plaintiff, the Court also undermined the compelling interest standard and created a distinction between government and private party defendants. It allowed a defendant to prevail by arguing, as

197. Hill v. Nat'l Collegiate Athletic Assn., 865 P.2d 633, 642 (Cal. 1994).
198. *Id.* (citing White v. Davis, 533 P.2d 222, 234 (Cal. 1975)).
199. *Id.* at 19 (citing White v. Davis, 533 P.2d 222, 233–35, (Cal. 1975)).
200. *Id.* at 20.

an affirmative defense, that the invasion of privacy is justified because it "substantially furthers one or more countervailing interests."[201]

The Court also manufactured a legal distinction between information and autonomy privacy claims that is also not present in the legislative history or ballot language of the constitutional right to privacy.[202] The Court held that it was still necessary for a defendant to prove a compelling interest when the interest invaded is fundamental to personal autonomy. But otherwise, the privacy intrusion would only be subject to a more general balancing test of the privacy interests versus the defendant's interests.[203]

The Court then applied this new *Hill* test to the facts of the case and held that the NCAA's suspicionless drug testing of college athletes does not violate the privacy right because student athletes have a diminished expectation of privacy and the NCAA has a strong interest in safety and competition integrity.[204]

a) The *Hill* Decision Was a Departure from Legislative Language and Precedent

The *Hill* decision (1) developed new required elements for the privacy claim including a reasonable expectation of privacy under the circumstances and a serious invasion of privacy; (2) created an artificial legal distinction between informational privacy and autonomy privacy; and (3) undermined the compelling interest test. It was a departure from the text and legislative history of the constitutional right to privacy, as well as precedent.

As the ACLU of Northern California wrote in its 1991 briefing in the *Hill* case,

> In over 15 years of privacy litigation following White, this Court and the Courts of Appeal have uniformly demanded that a cognizable burden on privacy be justified as the least invasive means of achieving an objective. This familiar framework reflects the concept of privacy as a fundamental right, explicitly anchored in our state's highest law. When the voters added "privacy" to "life, "liberty" and "property" as the inalienable rights enumerated in the first section of the first article of the California Constitution, they expected that personal privacy would be sacrificed only when necessary to satisfy a paramount public need. The voters entrusted the courts with

201. *Id.* at 40.
202. *See* Section I for further discussion.
203. Hill., 865 P.2d at, 654–55.
204. *Id.* at 637.

> safeguarding their fundamental rights by applying traditional searching judicial scrutiny of privacy invasions.[205]

Requiring the "reasonable expectation of privacy" as element two of the *Hill* test is inconsistent with the language and legislative history of the California constitutional right to privacy. The legislative history and language of the Privacy Amendment noticeably does not include the reasonable expectation of privacy test of Fourth Amendment jurisprudence. This was intentional.[206] The legislative history of the right to privacy specifically discusses that in the era of computers, a "clearer statement of our rights is needed."[207] It was drafted to be a "new safeguard[] to meet the new dangers,"[208] rather than relying on search and seizure jurisprudence and the Fourth Amendment caselaw that so far had only articulated the right to be free from certain kinds of intrusion and was not clear "who is protected and from what."[209]

There is also no legislative or ballot language support for the Court's requirement that the plaintiff establish a "serious" invasion of privacy. Rather, the language of the ballot argument makes it clear that the right to privacy is expansive and the burden is on the government and private parties to justify an intrusion of the fundamental right. "The right to privacy . . . is a fundamental and compelling interest" and "this right should be abridged only when there is compelling public need."[210]

Justice Stanley Mosk and Justice Ronald George both issued separate opinions in *Hill*, detailing these types of concerns with the majority's decision. Justice Mosk issued a blistering dissent from the entirety of the decision.

---

205. Opposition Brief of Respondents in Hill v. NCAA, 865 P.2d 633 (Cal. 1994) (S018180), https://www.aclunc.org/sites/default/files/ACLU%20NorCal%20Brief%20in%20Hill.pdf.

206. As noted earlier, Professor Anthony Amsterdam, a national expert on Fourth Amendment law and a Stanford Law professor at the time, helped to draft the ballot argument in support. *Anthony G. Amsterdam*, WIKIPEDIA (2024), https://en.wikipedia.org/wiki/Anthony_G._Amsterdam. The ballot argument noticeably does not include any mention of the reasonable expectation of privacy and a foremost national expert on the Fourth Amendment would have well-understood the implications of this drafting decision.

207. Letter from Kenneth Cory to the Legislative File, (1972), https://www.aclunc.org/sites/default/files/Letter%20Response%20to%20Chairman%20Ignazio%20Vella%20from%20Hon.%20Kenneth%20Cory.pdf.

208. STAFF OF ASSEMB. CONST. COMM., REP. ON ACA 51, at 5 (Cal. 1972). https://www.aclunc.org/sites/default/files/Staff%20report%20of%20Assembly%20Constitutional%20Committee%20on%20ACA%2051%20%28before%20April%2024%29.pdf.

209. STAFF OF ASSEMB. COMM. ON CONST. AMEND., ANALYSIS, ACA 51 (CORY) AS INTRODUCED MARCH 13, 1972 (Cal. 1972).

210. *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props.

Justice George concurred with the majority's ultimate conclusion that the NCAA's drug testing program was constitutional, but he dissented from the decision to subvert the pleading burden and deviate from the compelling interest standard.[211]

Justice Mosk, who had been on the bench for the *White v. Davis* decision, 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."[212]

> I dissent. Article I, section 1 of the California Constitution declares a right of privacy. Its pronouncement is express. Nothing is left to implication. "All people" have an "inalienable right[]" to "pursu[e] and obtain[]" "privacy." Before proceeding a sentence further, we must make one point pellucidly clear. This is not a case about the "policy" this court may think it best to formulate and implement with regard to privacy. Rather, it is a case about the California Constitution and the role of the judiciary within the order it establishes. The majority all but abrogate the right of privacy . . . Regrettably, in this case the majority have not so conducted themselves with regard to the people's constitutional policy declaring a right of privacy.[213]

Justice Mosk's dissent further reinforced that the privacy provision's scope to government and private actions was clear: "the coverage of the right of privacy is unlimited. That is to say, it reaches both governmental and nongovernmental actors. Intrusion is what matters, not the identity of the intruder."[214] Further, he noted that the "compelling public need" standard is applicable to both governmental and nongovernmental actors.[215] Justice Mosk admonished that the majority took a position that is "not mere 'revisionism,' but creation ex nihilo" in asserting that the "compelling public need standard" does not apply to nongovernmental actors, and if it does apply to such actions, it only applies with regard to autonomy privacy.[216] He contended that the burden and the standard are not areas of confusion in either the ballot language or the caselaw precedent nor basic civil procedure.[217] Justice Mosk forcefully

211. Hill v. Nat'l Collegiate Athletic Assn., 865 P.2d 633, 672 (Cal. 1994) (George, J., concurring in part and dissenting in part).

212. *Id.* at 679–80 (Mosk, J., dissenting).

213. *Id.* (Mosk, J., dissenting).

214. *Id.* at 687 (Mosk, J., dissenting).

215. *Id.* (Mosk, J., dissenting).

216. *Id.* at 700 (Mosk, J., dissenting).

217. *Id.* at 688 (Mosk, J., dissenting).

portended in his dissent that "the majority's refusal to follow the law . . . all but renders the right of privacy nugatory."[218]

In Justice George's separate opinion in *Hill*, he also dissented from the majority in its decision to subvert the burden and deviate from the compelling interest standard. Justice George wrote that, the majority was "increasing the plaintiff's burden in establishing a prima facie violation of the state constitutional privacy"[219] and "fashion[ed] a novel general legal standard for the evaluation of privacy claims arising under the California Constitution"[220] that departed from twenty years of precedent.[221] He highlighted that the first element of the majority's "new cause of action" is unobjectionable because state constitutional privacy decisions have always required a plaintiff to demonstrate that the conduct has intruded upon a privacy interest. But "in elevating the considerations embodied in the second and third 'elements' of the new cause of action . . . the majority has . . . introduced an undesirable and unfortunate inflexibility into the constitutional analysis that, if faithfully applied, is likely to bar privacy claims that properly should be permitted to go forward."[222]

Justice George found it improper for the Court to deviate from the "familiar and well-established constitutional analysis," weighing a constitutionally protected interest against the 'compelling' nature of the defendant's justification for its actions (taking into account whether there are other, less intrusive means by which the defendant could achieve its objectives) [parentheses in original].[223] By failing to require the defendant to demonstrate the existence of a compelling interest, and suggesting that any competing or legitimate interest may justify an infringement, the majority decision "essentially ignores the constitutionally protected status that the Privacy Initiative clearly intended to afford the right of privacy."[224] He continued that "the Privacy Initiative clearly sought to provide individuals with assurance that privacy interests would be taken seriously and would be abridged only for a 'compelling' need."[225] Justice George concluded that he saw no reason to abandon an established analytical framework to replace it with "the entirely new legal structure fashioned by the majority, a structure that appears, at least on its face, to weaken the protection afforded the California constitutional

218. *Id.* at 702 (Mosk, J., dissenting).
219. *Id.* at 676 (George, J., concurring in part and dissenting in part).
220. *Id.* at 672 (George, J., concurring in part and dissenting in part).
221. *Id.* at 672, 674 (George, J., concurring in part and dissenting in part).
222. *Id.* at 675 (George, J., concurring in part and dissenting in part).
223. *Id.* at 672 (George, J., concurring in part and dissenting in part).
224. *Id.* at 676 (George, J., concurring in part and dissenting in part).
225. *Id.* at 676–70 (George, J., concurring in part and dissenting in part).

right of privacy in the past, by making it more difficult to prove a violation of this fundamental right."[226]

Hill was a significant departure from established precedent. Unfortunately, the predictions from Justice Mosk and Justice George about the decision's potential effect on Californians' ability to pursue and obtain their fundamental right to privacy, have also largely manifested.

C. CALIFORNIA'S SOCIAL AND POLITICAL LANDSCAPE IMPACTED REACH OF CALIFORNIA CONSTITUTIONAL RIGHT TO PRIVACY

It is hard to square the vast difference in jurisprudence between the decisions in *White v. Davis,* and the nearly twenty years of cases following, with the 1994 decision in *Hill v. NCAA*. But by the time the *Hill v. NCAA* case was decided, the California Supreme Court had gone through a period of significant change with retirements and other departures, including three Democratically appointed Supreme Court Justices, Chief Justice Rose Bird and Associate Justices Joseph R. Grodin and Cruz Reynoso, losing their 1986 retention elections for being perceived as "soft on crime" in the Reagan War on Drugs era.[227] 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.[228]

By 1994, not only was the California Supreme Court very different, but the social movement landscape in California was also different compared to the landscape in the 1970s. This was in part because the intersectional movement base that had powered social change in the 1960s and early 1970s had been attacked and badly undermined by efforts like the "War on Drugs."

1. War on Drugs Impacted Trajectory of Privacy Rights

President Richard Nixon launched his War on Drugs in 1971, and his efforts to undermine social justice movements had a considerable effect on the trajectory of privacy rights, both nationally and within California. It is widely understood by those who study this period, and now publicly acknowledged

226. *Id.* at 672 (George, J., concurring in part and dissenting in part).

227. Frank Clifford, *Voters Repudiate 3 of Court's Liberal Justices*, L.A. TIMES (Nov. 5, 1986), https://www.latimes.com/archives/la-xpm-1986-11-05-mn-15232-story.html; Committee on History of Law in California, *Oral History: Justice Joseph R. Grodin*, 16 HASTINGS CONST. L.Q. 7 (1988), 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 (2007).

228. Frank Clifford, *Voters Repudiate 3 of Court's Liberal Justices*, L.A. TIMES (Nov. 5, 1986), https://www.latimes.com/archives/la-xpm-1986-11-05-mn-15232-story.html.

by Nixon's advisor, that the War on Drugs was "really all about" an assault on Black and Brown people, activists, and social justice movements organizing for change.[229] As Nixon's domestic policy chief, John Ehrlichman, bluntly explained in a 1994 interview:

> The Nixon campaign in 1968, and the Nixon White House after that, had two enemies: the antiwar left and black people. You understand what I'm saying? We knew we couldn't make it illegal to be either against the war or black, but by getting the public to associate the hippies with marijuana and blacks with heroin, and then criminalizing both heavily, we could disrupt those communities. We could arrest their leaders, raid their homes, break up their meetings, and vilify them night after night on the evening news. Did we know we were lying about the drugs? Of course we did.[230]

As Jonathan Simon elucidated in his book, *Governing Through Crime*, "values like freedom and equality have been revised in ways that would have been shocking, if obviously unimaginable, in the late 1960s, and new forms of power institutionalized and embraced—all in the name of repressing seemingly endless waves of violent crime."[231] This new civil and political order is due to a modern era of "governing through crime," where the fear of crime is weaponized to rationalize laws and policies which that have resulted in mass incarceration of predominately Black, Brown, and poor Americans.[232]

Court cases and legislation combined in this era to eviscerate the federal Fourth Amendment right to privacy, further powering racially biased policing, massively disproportionate imprisonment, and disenfranchisement of Black and Brown community members. 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."[233] But in the decades after *Terry*, there was a deep erosion of privacy rights.[234] This "steady lowering of the

229. Dan Baum, *Legalize It All*, HARPER'S MAG. (Apr. 2014), https://harpers.org/archive/2016/04/legalize-it-all/.

230. *Id.*

231. JONATHAN SIMON, GOVERNING THROUGH CRIME: HOW THE WAR ON CRIME TRANSFORMED AMERICAN DEMOCRACY 3–4 (2007).

232. H.G. Fredrickson, *'Governing Through Crime': Politics and Administration in the Penal State*, GOVERNING (Mar. 16, 2010), https://www.governing.com/archive/governing-through-crime.html.

233. Donald F. Tibbs, *From Black Power to Hip Hop: Discussing Race, Policing, and the Fourth Amendment Through the 'War On' Paradigm*, J. OF GENDER, RACE & JUST. 15, 63 (2012).

234. *Id.* at 65 (citing Joseph Caracappa, *Terry v. Ohio and the Power of the Police to Accost Citizens Absent Probable Cause to Arrest: A Critical Look at the Pennsylvania Experience*, 16 DUQ. L. REV. 499 (1977)); *see also* Lawrence Rosenthal, *Pragmatism, Originalism, Race, and the Case Against Terry v.*

threshold of evidence required to satisfy *Terry*'s reasonable suspicion standard means that Fourth Amendment privacy rights have all but dissipated. And in many respects they have dragged the legal existence of young Black men deeper asunder."[235]

Federal and state legislation in the same War on Drugs era also made sure that people arrested for low-level and nonviolent drug offenses were put in prison and stayed there. Laws like the 1984 Comprehensive Crime Control and Safe Streets Act eliminated parole in the federal system[236] and the 1986 Anti-Drug Abuse Act established mandatory minimum sentencing schemes, including the infamous 100-to-1 ratio between crack and powder cocaine sentences.[237] The 1994 Violent Crime Control and Safe Streets Act[238] gutted habeas corpus, eviscerated the exclusionary rule, implemented the federal three strikes law, and authorized trying 13-year-olds as adults"[239] By 1994, California had passed its own three strikes sentencing law, the harshest of its kind in the nation. It required a prison term of twenty-five years to life for anyone convicted of a third felony after two previous serious or violent felony convictions. This draconian law resulted in situations where people were sentenced to decades in prison for stealing $153 of children's videotape or $1,200 worth of golf clubs.[240]

These new laws drove an exponential increase in the rate of incarceration.[241] At the same time, the vast majority of these hundreds of thousands of Californians behind bars also lost their voting rights and ability to influence the political climate in California. A constitutional amendment passed in 1972, at the same time as the Privacy Amendment, codified felony

Ohio, 43 TEX. TECH L. REV. 299 (2010); Gregory Williams, *The Supreme Court and Broken Promises: The Gradual but Continual Erosion of Terry v. Ohio*, 34 HOW. L.J. 567 (1991).

235. Tibbs, *supra* note 233 at 65.

236. Comprehensive Crime Control Act of 1984, 98 Stat. 1976 (1984).

237. Anti-Drug Abuse Act of 1986, 100 Stat. 3207 (1986).

238. Violent Crime Control and Law Enforcement Act, 108 Stat. 1796 (1994).

239. Nkechi Taifa, *Race, Mass Incarceration, and the Disastrous War on Drugs*, BRENNAN CTR. FOR JUST. (May 10, 2021), https://www.brennancenter.org/our-work/analysis-opinion/race-mass-incarceration-and-disastrous-war-drugs.

240. Press Release, ACLU of S. Cal., After High Court Upholds Harsh "Three Strikes" Sentencing Law, ACLU of Southern CA Vows Reform Efforts (Mar. 5, 2003), https://www.aclu.org/press-releases/after-high-court-upholds-harsh-three-strikes-sentencing-law-aclu-southern-ca-vows.

241. *Incarceration Trends in California*, VERA INST. OF JUST., https://www.vera.org/downloads/pdfdownloads/state-incarceration-trends-california.pdf. Since 1970, the incarceration rate in America has expanded more than fourfold, the United States leads the world in locking people up, and California had more 200,000 people behind bars by 2015. Black people in California are incarcerated at eight times the rate of white people and the Black incarceration rate has increased by 260% since 1978.

disenfranchisement in the state.[242] Pursuant to Article II, Section 4 of the California constitution, any individual serving a felony sentence in federal prison or serving a felony prison sentence in state prison, or on parole from a felony sentence (until 2020 when Proposition 17 restored the right to vote for Californians on parole)[243] are ineligible to vote in California.[244]

The War on Drugs and its intent to attack Black and Brown communities and undermine activism movements is intertwined with the history of privacy rights in this state. It is a part of the story about why California's constitutional right to privacy has not been able to be utilized to its full potential to safeguard and promote rights and democracy. After an era of progressive movement activism in the 1960s and early 1970s, there was a successful conservative political backlash and retrenchment. More decisionmakers in the courts and legislature refused to continue to interpret California's constitutional right to privacy as it was intended—as a liberatory force to offset the oppressive power of government and business.

In discussing the role of the War on Drugs and its intersection with constitutional privacy rights in California, it should also not be lost that the 1994 *Hill* case, which subverted the burden and undermined a consistent compelling interest standard for privacy claims, was a case about drugs and drug testing. Justice Mosk concluded his dissent in *Hill* by connecting the dots on this issue.

> The NCAA is now free to use in California the weapons it had chosen for its "war on drugs." What better way to show that it is serious about its "war on drugs" than to subject student athletes "to this invasion of their privacy and affront to their dignity? To be sure, there is only a slight chance that it will prevent some serious . . . harm resulting from student athlete drug use, but it will show to the world that it is "clean," and-most important of all-will demonstrate its determination . . . to eliminate this scourge of our society! I think it obvious that this justification is unacceptable; that the impairment of individual liberties cannot be the means of making a point. . . ."[245]

242. *Voter Information Guide for 1972, General Election (1972)*, UC L. SF SCHOLARSHIP REPOSITORY (1972), https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1773&context=ca_ballot_props.

243. Sarah Hopkins, *Voters' Decisions on Propositions 17 and 20 Bring Hope to Criminal Justice Reform in California*, ACLU OF N. CAL. (Nov. 19, 2020), https://www.aclunc.org/blog/voters-decisions-propositions-17-and-20-bring-hope-criminal-justice-reform-california.

244. CAL. CONST. art. II § 4.

245. Hill v. Nat'l Collegiate Athletic Assn., 865 P.2d 633, 704 (Cal. 1994) (Mosk, J., dissenting).

The War on Drugs had a significant effect on the ability of intersectional social movements to support continued action on privacy and promote rights and safety in the digital age. While technology was advancing exponentially, privacy law on the federal level was either being rolled back or frozen in time, rather than strengthened. While there continued to be some advances in statutory privacy law in California, the *Hill* decision made it very difficult for privacy claims to move forward in the courts. All of this combined to undermine what privacy law, especially California constitutional privacy rights, should have been doing in the past decades to protect the fundamental rights of individuals and the fabric of democracy as technology advanced.

D. WHAT WAS PRESCIENT IN 1972 IS NOW REALITY

The concerns that animated the development and passage of the California constitutional right to privacy in 1972 have now become reality. There has been a dramatic rise in the reach of technology and most of us are living digital lives. Even the U.S. Supreme Court recognized in 2018 that, for most people, electronic devices are "indispensable to participation in modern society."[246] Approximately 95% of adults use the internet[247] and 97% own a mobile phone.[248] By 2021, nearly all young people (97% of three- to eighteen-year-olds) had home internet access[249] and by 2022, 95% of teens had access to a smartphone.[250] Particularly during, and then following the global coronavirus pandemic, electronic devices and services became essential to connect and communicate with others, and to access everything from healthcare and education to transportation.[251]

Smartphones are constantly collecting detailed location information about who people are and where they go.[252] There are devices and applications

246. *See* Carpenter v. United States, 585 U.S. 296, 298 (2018).

247. *Internet, Broadband Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/internet-broadband/.

248. *Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/.

249. *Children's Internet Access at Home*, NAT'L CTR. FOR EDUC. STAT. (Aug. 2023), https://nces.ed.gov/programs/coe/indicator/cch/home-internet-access.

250. Emily A. Vogels, Risa Gelles-Watnick & Navid Massarat, *Teens, Social Media and Technology*, PEW RSCH. CTR., (2022), https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/.

251. Colleen McClain, Emily A. Vogels, Andrew Perrin, Stella Sechopoulos & Lee Rainie, *How The Internet And Technology Shaped Americans' Personal Experiences Amid COVID-19*, PEW RSCH. CTR., 1–2, (2021), https://www.pewresearch.org/internet/2021/09/01/how-the-internet-and-technology-shaped-americans-personal-experiences-amid-covid-19/.

252. *Location Information: Do You Know Where Your Privacy Is?*, ACLU OF N. CAL., https://www.aclunc.org/sites/default/files/location_information_do_you_know_where_your

collecting and combining even more of people's personal information, from services that track everything from reproductive cycles[253] and prayer schedules[254] to apps that are marketed to provide support on mental health issues.[255] When people go to restaurants after the global pandemic, many are told to scan a digital quick response (QR) code rather than read a physical menu—and when a smartphone scans that code, the QR code company often collects vast information about people and their devices.[256] Most children in school also now must use school-issued computers, many with school-issued email addresses, and the majority of these devices are from a single company—Google, which as of 2022, had at least fifty million of their Chromebooks in K–12 schools across the United States.[257]

Every day, when millions of Californians search online, shop, or use a mobile device, each click creates a trail of personal information in the form of search and chat histories, location information, photos, friend lists, and more. These digital footprints track people's movements, habits, interests, associations, and much more. Companies collect and share these detailed digital footprints, dossiers about who people are, where they go, what they do,

_privacy_is.pdf; Jon Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, MARKUP (Sept. 30, 2021), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.

253. Kari Paul, *How Private is Your Period-Tracking App? Not Very, Study Reveals*, GUARDIAN (Aug. 17, 2022), https://www.theguardian.com/world/2022/aug/17/pregnancy-period-tracking-apps-privacy.

254. *Muslim Pro Users Delete the App En Masse After Military Sales Revealed*, ACLU OF N. CAL. (2020), https://www.itsgoodfor.biz/case-study/muslim-pro-users-delete-app-en-masse-after-military-sales-revealed.

255. Shreya Tewari, *How to Navigate Mental Health Apps That May Share Your Data*, ACLU (Sept. 28, 2022), https://www.aclu.org/news/privacy-technology/how-to-navigate-mental-health-apps-that-may-share-your-data.

256. Nicole Ozer & Jay Stanley, *Diners Beware: That Meal May Cost You Your Privacy and Security*, ACLU (July 27, 2021), https://www.aclu.org/news/privacy-technology/diners-beware-that-meal-may-cost-you-your-privacy-and-security.

257. Ara Wagoner, *Chromebooks in Schools Top 50 Million as Google Seeks to Improve Repairs*, ANDROID CENTRAL (Feb. 3, 2022), https://www.androidcentral.com/chromebooks-schools-top-50-million-google-seeks-improve-repairs. In February 2024, the Danish privacy regulator ruled that cities in Denmark need considerably more assurances about privacy to use Google service that may expose children's data. The agency found that Google uses student data from Chromebooks and Google Workplace for Education "for its own purposes," which isn't allowed under European privacy law. Wes Davis, *Google's Use of Student Data Could Effectively Ban Chromebooks From Denmark Schools*, VERGE (Feb. 7, 2024), https://www.theverge.com/2024/2/7/24065332/denmark-google-student-data-collection-privacy.

and who they know, with online advertisers, third party applications, data brokers, and even the government.[258]

The threat of computerized monitoring that Assemblymember Cory described, and that the California constitutional right to privacy was drafted and passed by the voters with the intent to prevent, has become the lived experience of Californians:

> [E]ach time we apply for a credit card or a life insurance policy, file a tax return, seek government benefits, interview for a job or apply for a passport, a dossier is opened on that person and an informational profile is sketched. Modern technology is capable of monitoring, centralizing, and evaluating this information and making real the fear of a . . . dossier on each of us.[259]

Cory articulated the need to shore up rights and preserve freedom and individual privacy.[260] But legal obstacles have limited how people are able to use the California constitutional right to actually obtain their fundamental right to privacy. These challenges have contributed to the reality that dramatic advances in technology and new business practices now facilitate a vast industry sector, whose core profit centers are based on the very privacy intrusions that the constitutional right to privacy promised to protect Californians against.

The surveillance business models of most of the major technology companies—from Google to Meta—are based on collecting, using, and sharing vast amounts of personal information in hard to understand and often unwanted ways. Some of the richest and most powerful companies in the world have made their money doing all the things that the Privacy Amendment was specifically drafted and passed to address and prevent—or what *White v. Davis* called the "principal mischiefs."[261] There is a startling disconnect between the constitutional rights that Californians are guaranteed and the current reality of rampant surveillance.

---

258. NICOLE OZER & MATT CAGLE, LOSING THE SPOTLIGHT: A STUDY OF CALIFORNIA'S SHINE THE LIGHT LAW (2013), https://www.aclunc.org/sites/default/files/Losing%20the%20Spotlight%20-%20A%20Study%20of%20California%27s%20Shine%20the%20Light%20Law%20final.pdf; *Demand Your dotRights*, ACLU OF N. CAL., https://www.aclunc.org/sites/default/files/demand_your_dotrights_an_online_privacy_fact_sheet_from_the_aclu.pdf.

259. Letter from Kenneth Cory to the Legislative File at 1, (1972), https://www.aclunc.org/sites/default/files/Letter%20Response%20to%20Chairman%20Ignazio%20Vella%20from%20Hon.%20Kenneth%20Cory.pdf.

260. *Id.* at 4.

261. Hill v. Nat'l Collegiate Athletic Assn., 865 P.2d 633, 642 (Cal. 1994) (internal citations omitted).

1. Behavioral Advertising as Privacy Invasion

Behavioral advertising is a prime example of a privacy mischief that runs directly counter to the California constitutional right to privacy, yet the industry has been able to flourish. Google pioneered this surveillance capitalism advertising business model in 2000, just a few years after the *Hill* decision. Sheryl Sandberg then brought this same information-extractive business model to Facebook when she joined the company as chief operating officer in 2008.[262] Other companies in Silicon Valley and beyond adopted a similar strategy[263] to: (1) grow the user base as quickly as possible, luring people with "free" products and services; (2) collect as much information as possible about people as they use that "free" service; (3) monetize that information by selling targeted advertisements; (4) profit, richly. Additionally, companies like Facebook created partnerships with applications hosted on their platform and with third party websites to further grow the reach and information collection of the company.[264] Once information is collected by companies, it also does not stay just in their hands. It is often provided to the government for surveillance, and some companies may sell information to data brokers, who sell access to many other people, including the government.

As Zuboff explains, from the dawn of the world wide web in the mid-1990s, an ideology of radical market freedom combined with diminishing democratic prerogatives and power allowed America's internet startups to utilize novel digital-age economics of surveillance capitalism, based on the "secret capture and datafication of human experience."[265] "Surveillance

262. Shoshana Zuboff, *Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization*, 3 ORG. THEORY 1, 12 (2022).

263. *Id.*; Nathalie Maréchal, *Targeted Advertising Is Ruining the Internet and Breaking the World*, VICE (Nov. 16, 2018), https://www.vice.com/en/article/xwjden/targeted-advertising-is-ruining-the-internet-and-breaking-the-world.

264. Nicole Ozer & Chris Conley, *After the Facebook Privacy Debacle, It's Time for Clear Steps to Protect Users*, ACLU (Mar. 23, 2018), https://www.aclu.org/news/privacy-technology/after-facebook-privacy-debacle-its-time-clear-steps-protect; Lesley Fair, *FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making*, FTC: BUS. BLOG (July 24, 2019), https://www.ftc.gov/business-guidance/blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-and-history-making.

Third party plug ins like the Facebook "Like" button also collected information for Facebook. *Is Facebook's 'Like' Button Spying on You?*, WEEK (Jan. 8, 2015), https://theweek.com/articles/484539/facebooks-like-button-spying. The Meta pixel also sends information to the company. Skye Witley, *Meta Pixel's Video Tracking Spurs Wave of Data Privacy Suits (1)*, BLOOMBERG L. (Oct. 13, 2022), https://news.bloomberglaw.com/privacy-and-data-security/meta-pixels-video-tracking-spurs-wave-of-consumer-privacy-suits.

265. Shoshana Zuboff, *Democracy Can Still End Big Tech's Dominance Over Our Lives*, TIME MAG. (May 5, 2022), https://time.com/6173639/democracy-big-techs-dominance-shoshana-zuboff/.

capitalism now reorders every domain of economic activity, from education and healthcare to retail, finance, automobiles, agriculture, and everything in between. Every product called 'smart' and every service called 'personalized' is part of this regime."[266]

Similarly, sociologist Zeynep Tufekci has said, "we're building a dystopia just to make people click on ads."[267] There is no true public benefit to this beyond profit for the technology companies. While the technology industry consistently tries to claim that people derive a value from behavioral advertising and more targeted ads, this is "more frequently hypothesized than empirically demonstrated."[268] In fact, empirical studies show that online behavioral ads often push products that are worse and more expensive.[269] Companies sometimes also target advertisements in a discriminatory manner based on age, sex, race, or ethnicity, resulting in certain groups receiving information about opportunities that others do not.[270] Behavioral advertisements can also be used by outright scammers seeking out financially vulnerable consumers.[271] Even people who work in the industry have described it as "snake oil"—because few consumers find the ads to be relevant and the only parties that think it is worthwhile are the advertisers themselves or the technology companies that are selling it.[272] A 2019 Pew study found that

266. *Id.*

267. *Zeynep Tufekci: We're Building a Dystopia Just to Make People Click on Ads*, TED (Sept. 2017), https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads.

268. Eduardo S. Mustri, Idris Adjerid & Alessandro Acquisti, *Behavioral Advertising and Consumer Welfare,* SSRN ELEC. J. (Mar. 23, 2023), http://dx.doi.org/10.2139/ssrn.4398428.

269. *Id.* at 1 ("[A]ds targeted to a sample of online participants were more likely to be associated with lower quality vendors and higher product prices"); Julia Angwin, *Opinion, If It's Advertised to You Online, You Probably Shouldn't Buy It. Here's Why*, N.Y. TIMES (Apr. 6, 2023), https://www.nytimes.com/2023/04/06/opinion/online-advertising-privacy-data-surveillance-consumer-quality.html. Eduardo S. Mustri, Idris Adjerid & Alessandro Acquisti, *Behavioral Advertising and Consumer Welfare: An Empirical Investigation*, SSRN ELEC. J. (2023), http://dx.doi.org/10.2139/ssrn.4398428. Craig Silverman & Ryan Mac, *Facebook Gets Paid*, BUZZFEED NEWS (Dec. 10, 2020), https://perma.cc/WJN7-S2XQ.

270. Galen Sherwin & Esha Bhandari, *Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform*, ACLU (Mar. 19, 2019), https://www.aclu.org/news/womens-rights/facebook-settles-civil-rights-cases-making-sweeping.

271. John P. Strong, *Target Subprime Credit Using Facebook and Paid Search*, STRONG AUTO. (Apr. 14, 2019), https://perma.cc/XE96-ETXR; Andrew Chow, *Facebook Shopping Scams Have Skyrocketed During the Pandemic*, TIME MAG. (Dec. 18, 2020), https://perma.cc/UX28-AUUT; Bennett Cyphers & Adam Schwartz, *Ban Online Behavioral Advertising*, EFF (Mar. 21, 2022), https://www.eff.org/deeplinks/2022/03/ban-online-behavioral-advertising.

272. Augustine Fou, *Why Is Ad Tech Targeting So Bad?*, FORBES (May 5, 2021), https://www.forbes.com/sites/augustinefou/2021/05/05/why-is-ad-tech-targeting-so-bad/?sh=23f8321f7212.

only 7% of adults say that the targeted ads they see accurately reflect who they are very well.[273]

This reliance on surveillance business models also contributes to many of the characteristics that concern people about children's mental health and their internet activity. Without online behavioral advertising as a primary basis for profit, companies would be far less incentivized to lure as many young users, keep them on their websites as long as possible, and collect detailed information to build ads and other content that can make children vulnerable to their messaging.[274] Targeted advertising is also associated with harms to democracy itself, including discouraging people from freely expressing themselves and fully utilizing their constitutional rights,[275] weakening a diverse, free press,[276] and growing misinformation that has affected recent elections.[277] The Federal Trade Commission recommended that people opt out of targeted advertising to protect themselves.[278] But the current pervasiveness of online tracking and the operational challenges, including "dark patterns" utilized by companies to make opt-out choices more difficult for people,[279] makes it functionally impossible for most people to do so entirely.

People consistently do not like online behavioral advertising, despite how many times the technology industry tries to claim that they do. People find

273. Brooke Auxier, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, PEW RSCH. CTR., *Public Knowledge and Experiences with Data-driven Ads* (2019), https://www.pewresearch.org/internet/2019/11/15/public-knowledge-and-experiences-with-data-driven-ads/.

274. Corynne McSherry, Mario Trujillo, Cindy Cohn & Thorin Klosowski, *Privacy First: A Better Way to Address Online Harms*, EFF (Nov. 14, 2023), https://www.eff.org/wp/privacy-first-better-way-address-online-harms.

275. Without privacy protections, people may be unwilling to discuss "sensitive, personal, controversial, or stigmatized content." ACLU v. Gonzales, 478 F. Supp. 2d 775, 806 (E.D. Pa. 2007), aff'd sub nom. ACLU v. Mukasey, 534 F.3d 181 (3d. Cir. 2008).

276. Corynne McSherry, Mario Trujillo, Cindy Cohn & Thorin Klosowski, *Privacy First: A Better Way to Address Online Harms*, EFF (Nov. 14, 2023), https://www.eff.org/wp/privacy-first-better-way-address-online-harms.

277. *Election Misinformation*, BRENNAN CTR., https://www.brennancenter.org/election-misinformation (last visited May 8, 2024).

278. Emma Fletcher, *Social Media a Gold Mine for Scammers in 2021*, FED. TRADE COMM'N (Jan. 25, 2022), perma.cc/GHU2-2DRG ("Here are some ways to help you and your family stay safe on social media: . . . . Check if you can opt out of targeted advertising.").

279. Hana Habib & Lorrie Cranor, *It's Shockingly Difficult to Escape the Web's Most Pervasive Dark Patterns*, FAST CO. (Nov. 4, 2019), https://www.fastcompany.com/90425350/its-shockingly-difficult-to-escape-the-webs-most-pervasive-dark-patterns (citing research in *An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites*, USENIX ASS'N (2019), https://www.usenix.org/conference/soups2019/presentation/habib).

these targeted ads to be invasive and unnerving "stalker ads."[280] A 2012 Pew study found that over two-thirds of internet users disapprove of search engines and websites tracking their online behavior in order to aim targeted ads at them. These people say they disapprove of targeted advertising because they do not like having their online behavior tracked and analyzed.[281] In 2015, a Bain & Company survey of more than 900 consumers found that "they are often uncomfortable with how their data is used and shared. A full two-thirds feel that it should be illegal for companies to collect or use such data without getting prior consent."[282] A 2015 Annenberg study similarly debunked the claim of marketers that Americans accept widespread tracking of their backgrounds, behaviors, and lifestyles across devices as an tradeoff for benefits.[283] Rather, the study found that a large pool of Americans remain very concerned and object to these activities, but also feel resigned to the inevitability of surveillance and the power of marketers to harvest their information.[284] A 2023 follow-up Annenberg study found that 91% percent of people wanted to have control over what marketers can learn about them online.[285]

280. Brian X. Chen, *Are Targeted Ads Stalking You? Here's How to Make them Stop*, N.Y. TIMES (Aug. 15, 2018), https://www.nytimes.com/2018/08/15/technology/personaltech/stop-targeted-stalker-ads.html ("Even if you end up ordering the watch, the ads continue trailing you everywhere. They're stalker ads.").

281. Russel Heimlich, *Internet Users Don't like Targeted Ads*, PEW RSCH. CTR. (Mar. 13, 2012), https://www.pewresearch.org/short-reads/2012/03/13/internet-users-dont-like-targeted-ads/.

282. Press Release, Bain & Company, How Can Companies Acquire Customer Data While Building Customer Loyalty At The Same Time? Ask Permission (May 11, 2015), https://www.bain.com/about/media-center/press-releases/2015/Digital-privacy-survey-2015-press-release.

283. Joseph Turow, Michael Hennessy & Nora Draper, *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation*, SSRN ELEC. J. (June 26, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820060. For example, a 2014 Yahoo report, concluded that online Americans 'demonstrate a willingness to share information, as more consumers begin to recognize the value and self-benefit of allowing advertisers to use their data in the right way." *Id.* at 3 (citing *The Balancing Act: Getting Personalization Right,* YAHOO! ADVERT. (May 2014), https://yahooadvertising.tumblr.com/post/97766688710/the-balancing-act-getting-personalization-right/amp).

284. Joseph Turow, Michael Hennessy & Nora Draper, *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation*, SSRN ELEC. J. 5 (June 26, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820060.

285. Joseph Turow, Yphtach Lelkes, Nora Draper & Ari E. Waldman, *Americans Can't Consent to Companies' Use of Their Data*, U. PA. ANNENBERG SCH. FOR COMMC'NS 13 (2023), https://perma.cc/J3ZR-RBG6.

Another study published in 2023 also found that people characterize these behavioral ads as "creepy, privacy-invasive, and disruptive."[286] Further, that online behavioral advertising resulted in "psychological distress, loss of autonomy, behavior constriction, and algorithmic marginalization and traumatization."[287] One of the most common concerns that participants in the study voiced was a lack of consent or control over targeting. They felt a loss of autonomy and felt personally violated.[288] One participant shared how they had seen ads related to grocery purchases in a physical store, even though they never expressly consented to connecting these purchases with any shopping website or app. They felt "it should be against the law to . . . invade my privacy without express permission each time they want to do something like this."[289] Others felt like they had no control over the nature of the targeted advertising, even when the targeting was incorrect. As one participant described: "I feel like I'm being attacked by salesman at a used car dealership and I really have no control over it."[290] Other participants noted that even though they understood their information was being collected online, the use of their information still felt like a breach of consent; they found the pervasiveness and specificity of the ads overwhelming and invasive into their thoughts and feelings. "It's not even what I'm doing anymore, it's everything I am thinking."[291]

For community members from marginalized populations, the effect of information collection can often be much more pronounced and destructive, holding people back from life opportunities and with real financial impacts that prevent people from meeting basic needs.[292] Community members from Charlotte, Detroit, and Los Angeles who were interviewed for the Our Data Bodies research project discussed feeling "preyed upon, hounded, or harassed" by "predatory" data driven systems.[293] They described feeling "uneasy, frustrated, overwhelmed, frightened, and angered by their experiences with

286. The Slow Violence of Surveillance Capitalism How Online Behavioral Advertising Harms People; Yuxi Wu, Sydney Bice, W. Keith Edwards & Sauvik Das., FAccT '23: 2023 ACM Conference on Fairness, Accountability, and Transparency, Chicago, IL, USA, June 2023, https://dl.acm.org/doi/fullHtml/10.1145/3593013.3594119.

287. *Id.*

288. *Id.* at Section 4.3.

289. *Id.*

290. *Id.* at Section 4.3.1.

291. *Id.*

292. Tawana Petty, Mariella Saba, Tamika Lewis, Seeta Peña Gangadharan & Virginia Eubanks, *Reclaiming Our Data*, *OUR DATA BODIES* 24 (June 15, 2018), https://www.odbproject.org/wp-content/uploads/2016/12/ODB.InterimReport.FINAL_.7.16.2018.pdf.

293. *Id.*

data collection."[294] Niggie, a community member from Charlotte, shared how they felt targeted for increased information collection and how it affected them: "I think because my identities are so visible they make me stand out more. So a queer black person is definitely going to be hypervisible . . . to a surveillance system"[295] People also discussed how when they lack control over how their information is used, digital scrutiny feels "paralyzing and dangerous." Assata, another community member from Charlotte, shared that it is "stressful . . . like you're plagued . . . a red letter . . . like an outcast" and "it's something that can't escape, like it follows me."[296]

The concerns voiced by the participants in both research studies mirror the very types of privacy mischiefs and harms that the Privacy Amendment was intended to give people the power to address. The Privacy Amendment guaranteed the "right to be left alone." It was passed to protect "our homes, our families, our thoughts, our emotions, our expressions, our personalities, our freedom of communion, and our freedom to associate with the people we choose."[297] It was intended to give the people the power to stop privacy invasions and "control circulation of personal information," address "accuracy of government and business records," and the use of "information gathered for one purpose in order to serve other purposes."[298]

2. Data Brokers as Privacy Invasion

The data broker industry is another very significant part of the surveillance capitalism business ecosystem, with its profit powered by underlying privacy invasions. Data broker companies like Acxiom, Equifax, Experion, and Intelius rake in $200 billion dollars a year through buying, selling, and trading personal information obtained from both public records and private sources.[299] The data broker industry traffics in vast amounts of personal information—including information from mobile phones, financial institutions, social media sites, applications, and online and brick and mortar companies—and uses it to create detailed dossiers on almost every adult

294. *Id.*

295. *Id.*

296. *Id.*

297. *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY, at 3 (1972), https://repository.uclawsf.edu/ca_ballot_props/762 (last visited May 8, 2024).

298. *Id.*

299. Transparency Market Research, Data Brokers Market (2022), https://www.transparencymarketresearch.com/data-brokers-market.html. The data broker industry is estimated to reach more than $450 billion by 2031. Press Release, Transparency Market Research, Data Brokers Market Estimated to Reach US$ 462.4 billion by 2031, TMR Report (2022), https://www.globenewswire.com/news-release/2022/08/01/2489563/0/en/Data-Brokers-Market-Estimated-to-Reach-US-462-4-billion-by-2031-TMR-Report.html.

American.[300] As former Federal Trade Commission Chairman Jon Leibowitz described, way back in 2012, these companies "are the unseen cyberazzi who collect information on all of us."[301]

Data broker companies utilize large-scale data mining operations and organize information into types like mobile location information and social media identifiers as well as specific characteristics that facilitate targeting of particular individuals.[302] Data brokers profile and group people by characteristics such as: "frequent credit card user," "30, 60, 90-day mortgage lates," "sexual orientation," "clinical depression," "erectile dysfunction," "plus size clothing purchase," "dieting and weight loss," "expectant parents," "getting divorced," "age of children," "political affiliation," and the list goes on and on.[303] Information collected and organized by these data brokers may be sought out by online services, advertisers, and increasingly, the government.

The government's largely secret use of data brokers to sidestep Fourth Amendment protections and surveil Americans has been pushed into the light in recent years. In 2020, a *Vice* investigation revealed that the Defense Department purchased location information collected by data brokers from popular prayer apps to monitor Muslim communities.[304] In 2022, an ACLU investigation uncovered thousands of pages of previously unreleased records documenting how Customs and Border Protection, Immigration and Customs Enforcement, and other parts of the Department of Homeland Security bought access to (and used) huge volumes of people's cell phone location information that had been quietly extracted from their smartphone apps.[305]

The data brokers and how they collect, use, sell, and trade, information for profit and power surveillance is exactly the type of privacy harm of "cradle-to-

300. Nicole Ozer & Matt Cagle, *Losing the Spotlight: A Study of California's Shine the Light Law* ACLU OF N. CAL., at 5 (2013), https://www.aclunc.org/sites/default/files/Losing%20the%20Spotlight%20-%20A%20Study%20of%20California%27s%20Shine%20the%20Light%20Law%20final.pdf.

301. Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES, at BU1 (June 16, 2012), http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html.

302. *Testimony of Pam Dixon Executive Director, World Privacy Forum*, Senate Judiciary, at 4–10 (Nov. 3, 2015), https://www.judiciary.senate.gov/imo/media/doc/11-3-15%20Dixon%20Testimony.pdf (last visited Sept. 21, 2023).

303. *Id.*

304. Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE (Nov. 16, 2020), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x.

305. Shreya Tewari & Fikayo Walter-Johnson, *New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data*, ACLU (July 18, 2022), https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data.

grave" dossiers that the California constitutional right to privacy was passed to protect against.[306]

3. Government Surveillance as Privacy Invasion

The surveillance business model ecosystem is also a treasure trove for government surveillance and the very type of privacy invasion that the Supreme Court found in *White v. Davis* to epitomize what is condemned by the constitutional right to privacy. All the personal information collected and retained by companies has become a gold mine for government surveillance. Local, state, and federal law enforcement agencies have consistently taken advantage of woefully outdated electronic privacy laws to seek access to personal information collected about who people are, where they go, what they do, and who they know.[307]

A wide variety of advocacy from the ACLU and other organizations[308] spurred technology companies to start releasing transparency reports that detail just how often law enforcement takes advantage of outdated legal protections to surveil people. Google released the first corporate transparency report in 2010 and by the end of 2016, more than fifty companies published regular transparency reports.[309] These transparency reports brought to light the

306. *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY, at 26–27 (1972), https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props (last visited Sept. 21, 2023).

307. *See* Nicole Ozer, *Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. OF L. & SOC. CHANGE 215, 272–75 (2012), https://socialchangenyu.com/review/putting-online-privacy-above-the-fold-building-a-social-movement-and-creating-corporate-change/; *see also Demand Your dotRights*, ACLU OF N. CAL., https://www.aclunc.org/sites/default/files/demand_your_dotrights_an_online_privacy_fact_sheet_from_the_aclu.pdf.; ACLU of Northern California*, Demand Your dotRights!*, YOUTUBE (2009), https://www.youtube.com/watch?v=OtQ9EBV8tTo (last visited May 8, 2024).

308. I helped develop and worked on the 2013 shareholder proposal campaign to push AT&T and Verizon to publish its first transparency reports. *See* Nicole Ozer, *Victory! Verizon Agrees to Publish Transparency Report (Updated)*, ACLU (Dec. 20, 2013), https://www.aclu.org/news/national-security/victory-verizon-agrees-publish-transparency-report-updated; *see also* Chris Conley, *Google's New Transparency Tool: A Window Into Government Surveillance*, ACLU (Apr. 20, 2010), https://www.aclu.org/news/national-security/googles-new-transparency-tool-window-government-surveillance (advocating for Google to issue its first transparency report as part of the ACLU Demand your dotRights campaign); *see also* Chris Calabrese, *Hurray for Google Transparency, Now Where is Everyone Else?*, ACLU (Jan. 23, 2013), https://www.aclu.org/news/national-security/hurray-google-transparency-now-where-everyone-else.

309. Google published the first transparency report in 2010, followed by LinkedIn, Microsoft, and Twitter. Then Apple, Facebook, and Yahoo released transparency reports in June 2013 following the Snowden revelations, and Verizon and AT&T were pushed by ACLU

exponential increase in warrantless government access to mobile devices, email, text messages, electronic documents, metadata and location information. For example, corporate transparency reports revealed that by 2015, Google had a 250% jump in government demands in just the previous five years.[310] Current transparency reports continue to provide important information about growth and changes in government surveillance. In its 2020 transparency report, Google revealed that geofence warrants—a type of reverse warrant to try to identify people who are in a particular place at a particular time—now constituted more than a quarter of the company's warrant requests in the United States, and that the company had received more than 11,500 geofence demands in that single year alone.[311] Further, Google reported that law enforcement in California had submitted more of these dragnet surveillance demands than any other state.[312]

---

of Northern California work in partnership with shareholders to release their first transparency reports in 2014, and then many other companies followed. *See* Case Study, New America, *Case Study #3: Transparency Reporting* (May 8, 2024), https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-3-transparency-reporting/. Amazon was the last of the technology companies in the Fortune 500 to issue a transparency report, finally issuing its first report in 2015. *See* Zack Whittaker, *After Years of Silence, Amazon Releases First Transparency Report*, ZDNET (June 12, 2015), https://www.zdnet.com/article/after-years-of-silence-amazon-finally-discloses-govt-data-demands/; Lizzie Plaugic, A*mazon has Finally Released its First Transparency Report*, VERGE (2015), https://www.theverge.com/2015/6/12/8774857/amazon-transparency-report-2015.

310. Fact Sheet, Office of Senator Mark Leno, SB 178 (LENO and ANDERSON) (Sept. 2, 2015), https://www.aclunc.org/sites/default/files/SB%20178%20CalECPA%20Fact%20Sheet_1.pdf, citing transparency reports.

311. Thomas Claburn, *Google Hopes to End Tsunami of Data Dragnet Warrants with Location History Shakeup*, REGISTER (Dec. 15, 2023), https://www.theregister.com/2023/12/15/google_location_history_geofence/.

312. Supplement to Transparency Report, Google, *Supplemental Information on Geofence Warrants in the United States*, https://services.google.com/fh/files/misc/supplemental_information_geofence_warrants_united_states.pdf (last visited May 8, 2024); Jake Snow, *Cops Blanketed San Francisco In Geofence Warrants. Google Was Right to Protect People's Privacy*, ACLU OF N. CAL. (Jan. 7, 2024), https://www.aclunc.org/blog/cops-blanketed-san-francisco-geofence-warrants-google-was-right-protect-peoples-privacy. This transparency report information helped support the introduction of ACLU and EFF sponsored privacy legislation in California in 2022 to prohibit government use of geofence warrants. *Stop Reverse Demand Warrants (AB 793)*, ACLU OF N. CAL., https://www.aclunc.org/our-work/legislation/stop-reverse-demand-warrants-ab-793 (last visited May 8, 2024). Ultimately, Google instituted new privacy controls for the storage and retention of location history in Google maps that effectively makes it impossible for the company to be able to respond to geofence warrants. Cyrus Farivar & Thomas Brewster, *Google Just Killed Warrants That Give Police Access To Location Data*, FORBES (Dec. 14, 2023), https://www.forbes.com/sites/cyrusfarivar/2023/12/14/google-just-killed-geofence-warrants-police-location-data/.

The large-scale government surveillance shopping spree of personal information has been possible because the reach of constitutional privacy protections has been limited by the courts and statutory privacy laws have largely not been updated in recent decades. The Electronic Communications Privacy Act (ECPA), the federal privacy law that is supposed to protect electronic communications from government demands, still has not been meaningfully updated since 1986, back when cell phones were the size of bricks, the World Wide Web did not even exist, and Facebook's founder was still in diapers.[313] The Digital Due Process Coalition, a broad coalition of organizations including the Center for Democracy and Technology, Electronic Frontier Foundation, ACLU and major technology companies, engaged in an extensive policy effort from 2009–2014 to try to update ECPA for the modern digital age. The Digital Due Process coalition advocated for changes such as extending probable cause warrant protections to more electronic information, ensuring that illegally obtained information could not be used in court, and providing government record-keeping of all law enforcement requests.[314]

To support coalition efforts to update ECPA and other important legal and policy changes related to electronic privacy, the ACLU of Northern California developed a multi-year integrated advocacy campaign called Demand your DotRights. This campaign, which later became a national privacy campaign of the ACLU,[315] was developed to "connect the dots" so that the public and policymakers could better understand the interconnected issues of consumer privacy and government surveillance in the information ecosystem. The campaign engaged people about online privacy by making the issues personal, tangible, and accessible.[316] As of October 2024, federal ECPA

313. *MODERNIZING THE ELECTRONIC COMMUNICATIONS PRIVACY ACT (ECPA)*, ACLU, https://www.aclu.org/issues/privacy-technology/internet-privacy/modernizing-electronic-communications-privacy-act-ecpa?redirect=ecpa (last visited May 8, 2024); ACLU of Northern California, *Demand Your dotRights!*, YOUTUBE (2009), https://www.youtube.com/watch?v=OtQ9EBV8tTo (last visited May 8, 2024); *Demand Your dotRights*, ACLU OF N. CAL., https://www.aclunc.org/sites/default/files/demand_your_dotrights_an_online_privacy_fact_sheet_from_the_aclu.pdf.

314. Press Release, ACLU, ACLU Joins AT&T, Google And Privacy Groups To Urge Updates To Privacy Law (Mar. 30, 2010), https://www.aclu.org/press-releases/aclu-joins-att-google-and-privacy-groups-urge-updates-privacy-law.

315. I developed and led the ACLU's Demand your DotRights campaign from 2008-2012. Nicole Ozer, *Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. OF L. & SOC. CHANGE 215 (2012), https://socialchangenyu.com/review/putting-online-privacy-above-the-fold-building-a-social-movement-and-creating-corporate-change/.

316. Nicole Ozer, *Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. OF L. & SOC. CHANGE 215, 272–75 (2012), https://

has still not been updated. But the work of the Demand your DotRights campaign spurred the passage of two landmark California privacy laws—the California Reader Privacy Act in 2011[317] and the California Electronic Communication Privacy Act (CalECPA) in 2015.[318]

California statutory laws have helped to operationalize aspects of the constitutional right to privacy and provided some important privacy protection in the modern digital age. But the more limited reach of the California constitutional right to privacy after the *Hill* decision has allowed privacy invasions to flourish that are directly contrary to the fundamental right to privacy. The surveillance ecosystem of privacy invasions by government and business, the deep partnership between the two, and the harm that would result to individual rights and democracy, was nascent in 1972, but has become all too widespread today. The current reality of pervasive corporate and government surveillance in the modern digital world is what the California constitutional right to privacy was drafted and passed to prevent. It is critical to ensure that the proper reach of the California constitutional right to privacy is revitalized so it can be used as it was intended and better protect the rights of Californians and the fabric of democracy in the years ahead.

E. TECHNOLOGY AND BUSINESS MODELS HAVE CHANGED, BUT CALIFORNIANS HAVE BEEN STEADFAST IN WANTING PRIVACY PROTECTED

Technology and business practices have changed dramatically since the 1970s. The California Supreme Court's interpretation of what is necessary to bring a cognizable claim for a privacy invasion and the more limited burden needed of a privacy invader to justify an informational privacy intrusion also changed dramatically during this same period with the *Hill* case. But Californians have been unwavering in their strong desire for privacy rights and they want their courts and policymakers to protect and enforce these rights.

---

socialchangenyu.com/review/putting-online-privacy-above-the-fold-building-a-social-movement-and-creating-corporate-change/; Declan McCullagh, *Google, Facebook Go Retro in Push to Update 1986 Privacy Law*, CNET (Oct. 21, 2011), https://www.cnet.com/news/privacy/google-facebook-go-retro-in-push-to-update-1986-privacy-law/. Privacy coalition court Hill staffers at a retro-party intended to highlight how dated a key privacy law has become. Rekha Arulanantham, *ECPA: Online Privacy Stuck in the '80s*, ACLU (Oct. 17, 2011), https://www.aclu.org/news/national-security/ecpa-online-privacy-stuck-80s; *Online Privacy Law Stuck in 1986!*, YOUTUBE (2011), https://www.youtube.com/watch?v=paLwr1nHiHU (last visited May 8, 2024).

317. CAL. CIV. CODE § 1798.90, https://law.justia.com/codes/california/2011/civ/division-3/1798.90-1798.90.05/1798.90/.

318. Kim Zetter, *California Now Has the Nation's Best Digital Privacy Law*, WIRED (Oct. 8, 2015), https://www.wired.com/2015/10/california-now-nations-best-digital-privacy-law/.

The Privacy Amendment and its scope to safeguard both autonomy and informational privacy from both government and private party actions was passed by a hefty 62.9% of the voters in 1972. Thirty years later, a 2012 USC Dornsife/Los Angeles Times Poll found that 78% of California voters across the political and demographic spectrum—including 71% of voters between the ages of eighteen to twenty-nine—believed that the collection of personal information online was an invasion of their privacy.[319] In 2019, nine out of ten polled Californians voters across the political and demographic spectrum rejected the concept of paying for services with their privacy rights, saying that "even if I don't pay money for products like Google, Facebook or Twitter, I should have my right to privacy and my personal information should only be shared with my permission." In addition, an overwhelming majority of Californians—94%—wanted to make sure you can take a company to court if they violate your privacy rights.[320] In 2020, more than 56% of California voters supported the passage of Proposition 24[321] and the 2019 polling on consumer privacy showed overwhelming support for even stronger privacy protections.[322] In 2022, more than 66.8% of Californians voted to further reinforce their right to privacy and autonomy in decisions related to reproductive freedom by passing Proposition 1.[323] Californians consistently

319. *USC Dornsife Online Survey Experiment Results*, USC DORNSIFE (Apr. 12, 2012), https://dornsife.usc.edu/news/stories/usc-dornsife-online-survey-experiment-results/.

320. Polling, ACLU of Northern California & David Binder Research, David Binder Research Voter Support for Consumer Privacy (2019), https://www.aclunc.org/docs/20190327_DBR_Voter_Support_for_Consumer_Privacy_final.pdf.

321. *California Proposition 24, Consumer Personal Information Law and Agency Initiative (2020)*, BALLOTPEDIA (2020), https://ballotpedia.org/California_Proposition_24,_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020).

322. ACLU in California and other consumer privacy and civil rights groups opposed Proposition 24 because it did not do enough to properly protect privacy rights. *See* Proposition Rebuttal. Kevin Baker, Nan Brasmer & John Mathias, *REBUTTAL TO ARGUMENT IN FAVOR OF PROPOSITION 24*, In *AMENDS CONSUMER PRIVACY LAWS. INITIATIVE STATUTE California Proposition 24 (2020)*, UC L. SF SCHOLARSHIP REPOSITORY (2020), https://repository.uclawsf.edu/ca_ballot_props/1389/ (last visited Sept. 22, 2023); *ACLU of Northern California Statement on Prop. 24*, ACLU OF N. CAL. (Nov. 4, 2020), https://www.aclunc.org/news/aclu-northern-california-statement-prop-24; s*ee also* Jacob Snow, *Will California Lawmakers Vote to Protect Californians' Privacy or Tech Industry Profits?*, ACLU OF N. CAL. (Sept. 28, 2015), https://www.aclunc.org/blog/will-california-lawmakers-vote-protect-californians-privacy-or-tech-industry-profits; Polling, ACLU of Northern California & David Binder Research, David Binder Research Voter Support for Consumer Privacy (2019), https://www.aclunc.org/docs/20190327_DBR_Voter_Support_for_Consumer_Privacy_final.pdf.

323. Jackie Fortier, *California Voters Enshrine Right to Abortion and Contraception in State Constitution*, NPR (Nov. 9, 2022), https://www.npr.org/2022/11/09/1134833374/california-results-abortion-contraception-amendment-midterms.

and overwhelmingly, across the political and demographic spectrum, have demonstrated for more than fifty years that they want their privacy to be protected.

F. COMPANIES USE IMMENSE FINANCIAL AND POLITICAL POWER TO ATTACK PRIVACY PROTECTIONS

While Californians want their privacy to be protected, existing California privacy rights and attempts to advance these rights are under constant assault by ever-more powerful technology companies. Since the time the *Hill* case was decided in 1994, technology companies that power their profit through privacy invasions have become the largest and most lucrative companies not just in California, but around the world. Technology companies have immense financial and political power, and many of them have grown only more powerful since the global pandemic in 2020.[324] Technology companies use their astronomical wealth and power to attack efforts to pass new, robust privacy protections. It makes the existing California constitutional right to privacy an even more important legal lever that must now be applied appropriately to ensure that rights and society are properly protected.

California rose to the challenge in 1972 to address how advances in technology would affect privacy, rights, and democracy with the development and successful passage of the constitutional right to privacy. But without this constitutional right's full force in play since the mid-1990s, surveillance capitalism is now well out of control.[325] There have been some privacy laws passed since the dawn of surveillance business models in 2000, but most have only addressed privacy issues at the edges. Nothing has been able to get at the heart of surveillance capitalism.

1. Technology Industry Uses Power and Money to Lobby Against Strong Privacy Laws

Technology companies have used their massive profits to fund lobbying that props up and perpetuates their oppressive surveillance business model. The technology industry uses its power and money to influence legislation and stop strong privacy laws or pass weak laws that protect its bottom line and do

---

324. In 2023, Big Tech companies like Alphabet, Microsoft and Apple are now all ranked by Forbes in the top ten of the largest companies in the world in terms of sales, profits, assets and market value. List, Forbes, Global 2000 (June 8, 2023), https://www.forbes.com/lists/global2000/?sh=12e9eefd5ac0.

325. Shoshana Zuboff*, Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization*, 3 ORGANIZATION THEORY, 19 (2022), https://doi.org/10.1177/26317877221129290.

not actually protect rights.[326] Big Tech has already surpassed all prior lobbying records, including Big Oil and Big Tobacco. It lobbies aggressively on both the federal level and state level.[327] On the federal level, its lobbying includes work behind the scenes to try to pass a weak federal privacy law that could preempt and erase state privacy laws as well as threaten the reach of the California constitutional right to privacy.[328] Of members of Congress with jurisdiction over privacy and antitrust issues, 94% received Big Tech PAC or lobbyist contributions by 2020.[329] The five biggest technology companies spent sixty-eight million dollars in lobbying in 2023 alone,[330] and even more industry players joined the lobbying game as issues of artificial intelligence heated up.[331] Big Tech now uses the same anti-democratic playbook as Big Tobacco and Big Oil: denying facts and hiding their harmful practices behind false promises and slick marketing of corporate narratives. Certain corporate narratives have become pervasive and work hand-in-hand along with government narratives to undermine efforts to address how technology can impact individuals and society. These false corporate narratives include consistent themes such: (1) technology and technology companies are inherently good for the world;[332] (2)

326. *See* Carlton Fields, 2023 Class Action Survey 9 (2023), https://www.carltonfields.com/Libraries/CarltonFields/Documents/Class%20Action%20Survey/2023-carlton-fields-class-action-survey.pdf; Todd Feathers & Alfred Ng, *Tech Industry Groups Are Watering Down Attempts at Privacy Regulation, One State at a Time*, MARKUP (May 26, 2022), https://themarkup.org/privacy/2022/05/26/tech-industry-groups-are-watering-down-attempts-at-privacy-regulation-one-state-at-a-time.

327. *See* Brendan Bordelon & Alfred Ng, *Tech Lobbyists are Running the Table on State Privacy Laws*, POLITICO (Aug. 16, 2023), https://www.politico.com/news/2023/08/16/tech-lobbyists-state-privacy-laws-00111363.

328. *See Governor Newsom, Attorney General Bonta and CPPA File Letter Opposing Federal Privacy Preemption*, Office of Governor Gavin Newsom (Feb. 28, 2023), https://www.gov.ca.gov/2023/02/28/governor-newsom-attorney-general-bonta-and-cppa-file-letter-opposing-federal-privacy-preemption/.

329. Shoshana Zuboff, *Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization*, 3 ORGANIZATION THEORY, 17 (2022), https://doi.org/10.1177/26317877221129290 (citing Jane Chung, Public Citizen, *Big Tech, Big Cash: Washington's New Power Players* 34 (2021), https://www.citizen.org/article/big-tech-lobbying-update/).

330. Ashley Gold, *2023 Tech Lobbying in Review*, AXIOS (Jan. 23, 2024), https://www.axios.com/pro/tech-policy/2024/01/23/2023-tech-lobbying-in-review.

331. Hayden Field, *AI Lobbying Spikes 185% as Calls for Regulation Surge*, CNBC (Feb. 2, 2024), https://www.cnbc.com/2024/02/02/ai-lobbying-spikes-nearly-200percent-as-calls-for-regulation-surge.html.

332. John Naughton, *Power and Progress Review – Why the Tech-Equals-Progress Narrative Must be Challenged*, GUARDIAN (May 7, 2023), https://www.theguardian.com/books/2023/may/07/power-and-progress-daron-acemoglu-simon-johnson-review-formidable-demolition-of-the-technology-equals-progress-myth.

anyone who challenges technology is a backwards luddite;[333] (3) technology and any potential uses of it are inevitable;[334] and (4) technology is too complicated to regulate.[335] Finally, if the first four corporate narratives are not getting adequate traction, then one may see the industry regrouping to a narrative that is seemingly in contradiction to the first social good narrative, and claiming that: (5) technology is just a neutral tool and the technology companies who develop, build it, or deploy it are not responsible for how it is used or how it impacts people or society.[336]

Facebook's founder, Mark Zuckerberg has "apologized" so many times using this combination of false promises and slick marketing to dodge doing anything to substantially change his company practices and its impact on people and democracy.[337] Consumer protection leader Ralph Nader was asked in 2021 if he saw any parallels between the giant social media companies of today and the giant automobile companies of the 1960s and "putting profits over people."[338] Nader responded that it was not only a "valid comparison,"

333. *Id.*

334. As Margaret Heffernan discusses, "[a]ll assertions of inevitability have an agenda. Anyone claiming to know the future is just trying to own it." The goal of "that tone of inevitability" is not "participation, but submission" and that the "language of inevitability has to be called out for the propaganda that it is." *A Point of View: The Myth of Inevitability*, BBC (Oct. 11, 2019), https://www.bbc.co.uk/sounds/play/m0009522.

335. I call this narrative strategy by the tech industry "tech washing," or more recently, "AI washing"—where the tech industry slaps the term "AI" on something and tries to intimidate people against speaking up about the impact on issues that they work on and the people that they work with in communities every day. *Nicole Ozer*, STAN. PACS CTR. ON PHIL. & CIV. SOC'Y (May 9, 2024), https://pacscenter.stanford.edu/person/nicole-ozer/. As Professor Arvind Narayanan and Sayash Kapoor recently noted, "there is nothing exceptional about tech policy that makes it harder than any other type of policy requiring deep expertise." Arvind Narayanan & Sayash Kapoor, *Tech Policy is Only Frustrating 90% of the Time*, AI SNAKE OIL (Apr. 3, 2024), https://www.aisnakeoil.com/p/tech-policy-is-only-frustrating-90.

336. *See, e.g.*, Matt Day, *Amazon Officials Pitched Their Facial Recognition Software to ICE*, SEATTLE TIMES (Oct. 23, 2018), https://www.seattletimes.com/business/amazon/amazon-officials-pitched-their-facial-recognition-software-to-ice/ (reporting that then-Amazon CEO Jeff Bezos defended his company against widespread criticism of its face surveillance technologies, arguing that while face surveillance might be put to "bad uses," the solution was to wait for society's "immune response" to take care of the problem); *see also* Nicole Ozer, *Face Recognition Tech Presents a Surveillance Issue and Amazon is Running Amok*, USA TODAY (Jan. 23, 2019).

337. David Hamilton, *Mark Zuckerberg's Long Apology Tour: A Brief History*, AP NEWS (Feb. 1, 2024), https://apnews.com/article/mark-zuckerberg-facebook-apology-c7055b654f63a23d09b6a96388dfa2b4.

338. *Ralph Nader Reflects On His Auto Safety Campaign, 55 Years Later*, SCI. FRIDAY (Dec. 3, 2021), https://www.sciencefriday.com/segments/ralph-nader-auto-safety/.

but that the technology companies like "Facebook, Google, Instagram, all the rest" are even "worse."[339]

There are now twenty years of privacy invasions that are the very foundation for the business models of these technology business behemoths. Companies across the information industry ecosystem have externalized the costs of these "free" services to individuals and society to make massive profits and are willing to spend whatever it takes to defend against public and political challenges to its surveillance business model.[340]

2. *Technology Industry Uses Resources to Undermine Privacy Rights in the Courts*

Technology companies also use their incredible resources to aggressively try to undermine privacy laws in the courts and the ability of people to seek redress for privacy invasions. One of the early tactics of the technology industry was to try to undermine privacy laws by claiming that injuries related to privacy invasions, such as data breaches, did not meet requirements for Article III standing in the federal courts. Companies intensely litigated these cases in federal courts across the country about what constituted "injury in fact" and whether a plaintiff's injury was sufficiently concrete or too speculative in nature.[341] In recent years, the technology industry has largely been winning this fight to undermine privacy enforcement in the federal courts. After the U.S. Supreme Court decisions restricting standing in *Spokeo* and *TransUnion*, it can be very difficult for plaintiffs to be able to move privacy cases forward in federal court.[342]

A more recent tactic in the courts has been for companies to weaponize the First Amendment and use it as a cudgel against privacy laws. Emboldened by U.S. Supreme Court decisions in cases like 2011 *Sorrell v. IMS Health*, companies have increasingly argued that privacy protections limiting the use and sharing of people's personal information improperly infringe on their

339. *Id.*

340. *Business Primer*, ACLU OF N. CAL., www.aclunc.org/business/primer (last visited May 9, 2024).

341. Client Alert, Morrison Foerster, *No Injury, No Data Breach Claims? Recent Trends in Evaluating Standing in Data Breach Class Actions* (2023), https://www.mofo.com/resources/insights/230405-no-injury-no-data-breach-claims-recent-trends.

342. *See* Spokeo, Inc. v. Robins, 578 U.S. 330, 340 (2016) (Fair Credit Reporting Act plaintiff must show an injury that is both concrete and particularized); *see also* TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2197, 2214 (2021) (inaccuracies in credit files that violated Fair Credit Reporting Act but were not disseminated to third parties were not enough to establish Article III standing).

company's First Amendment rights.[343] Companies have even tried to use this argument to challenge long-established privacy laws like the Video Privacy Protection Act, which has been on the books for more than thirty years.[344] But these arguments are built on a very faulty premise. Buying a product or signing up for a service does not give a company the First Amendment right to share or use personal information they might collect however they want.[345]

When done right, strong privacy protections and speech rights are not in conflict, but mutually support each other. Together, they create spaces where people have the confidence to exercise their First Amendment rights to communicate freely, connect with others, and anonymously speak or access information on a wide range of topics.[346]

Westin discussed this connection between privacy and free speech rights in 1967. He wrote about his hopes for U.S. Supreme Court jurisprudence on privacy and that it would move away from being "mired in the technicalities of search and seizure law under the Fourth Amendment" and enunciate a new doctrine that connected more directly with First Amendment law and the rights to speak, publish, and associate.[347]

Gerhard Casper,[348] then a law and political science professor at the University of Chicago, shared his thoughts on the intersection between these two rights as well, in a letter to the Senate Chair of the Subcommittee on Constitutional Rights for the U.S. Senate Committee on the Judiciary in the

343. Sorrell v. IMS Health, Inc., 564 U.S. 552 (2011), https://supreme.justia.com/cases/federal/us/564/552/; *see also* G. S. Hans, *No Exit: Ten Years of "Privacy vs. Speech" Post-Sorrell*, 65 WASH. U. J. L. & POL'Y 19 (2021), https://scholarship.law.vanderbilt.edu/cgi/viewcontent.cgi?article=2230&context=faculty-publications.

344. Amicus Curiae Brief of EFF, CDT, ACLU of NorCal & ACLU In Support of The Video Privacy Protection Act's Facial Constitutionality, Stark v. Patreon, Inc., 3:22-cv-03131-JCS, no. 95-1, https://www.aclunc.org/sites/default/files/095-1%20Amicus%20Curiae%20Brief%20of%20EFF%2C%20CDT%2C%20and%20ACLU%20filed%2020223-12-20.pdf.

345. Elizabeth Gyori, Jacob Snow & Vera Eidelman, *How to Protect Consumer Privacy and Free Speech*, ACLU (May 11, 2024), https://www.aclu.org/news/privacy-technology/how-to-protect-consumer-privacy-and-free-speech.

346. *Id.*

347. *See ACLU of Northern California News, vol. 32, no. 6*, CAL, HIST. SOC'Y at 2 (June 1967), https://digitallibrary.californiahistoricalsociety.org/object/15616?islandora_paged_content_page=2 (last visited May 7, 2024).

348. 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*, STAN. UNIV., https://gcasper.stanford.edu/ (last visited May 9, 2024).

fall of 1970.[349] When asked to comment on the issues before the committee concerning "privacy and data banks," he took it upon himself to note 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. He noted that "the public discussions of the privacy question has suffered from a failure to focus on the fact that present and future intrusions into privacy bring the First Amendment directly, not just indirectly, into play."[350] He observed a dual interconnection—that "the right to privacy is a necessary condition, perhaps even the matrix of First Amendment freedoms" and that the First Amendment, through "protecting free speech and religion is to some extent protecting a person's autonomy (as does in a very physical sense the Fourth Amendment)."[351] He highlighted how the development of computers had changed the landscape and "the threats posed by unlimited data storage and data recall."[352] He reasoned that 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.[353] The 'central meaning' of the First Amendment requires no less."[354]

Shoshanna Zuboff has asserted that we need "democracy's Golden Sword," and "legal frameworks purpose-built for a democratic digital century" to tackle surveillance capitalism.[355] But fortunately, we do not need to muster the forces to pass an entirely new legal framework for this purpose. We already have the California constitutional right to privacy that was developed for this purpose, but that has not been used to its full potential as California's Golden State Sword.[356]

The benefits of California's Golden State Sword are not limited to its broad scope covering privacy intrusions by government and private parties. California's legal structures also help neutralize some of the avenues of attack against privacy protections. While there have been aggressive efforts to

349. *Federal Data Banks, Computers, and the Bill of Rights, February 23, 1971*, HATHITRUST, at 930, https://babel.hathitrust.org/cgi/pt?id=uc1.c051765460&view=1up&seq=956&q1=gerhard.

350. *Id.*

351. *Id.*

352. *Id.* at 930.

353. *Id.* at 930.

354. *Id.*

355. Shoshana Zuboff, *Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization*, 3 ORGANIZATION THEORY, 2, 54 (2022), https://doi.org/10.1177/26317877221129290.

356. *Id.*

undermine standing for privacy claims in federal court, California has a far more liberal standing doctrine, including taxpayer standing for cases against the government.[357] As a general matter, a party only lacks standing to sue in California courts "if it does not have an actual and substantial interest in, or would not be benefited or harmed by, the ultimate outcome of an action."[358] Finally, a corporate free speech attack against efforts to utilize the constitutional right to privacy would be a fight between two, fully articulated constitutional rights. As the ballot measure highlighted, "[t]he right of privacy is an important American heritage and essential to the fundamental rights guaranteed by the First, Third, Fourth, Fifth and Ninth Amendments to the U.S. Constitution. This right should be abridged only when there is a compelling public need."[359] When the constitutional right to privacy was enacted in 1972, it was thus understood that the First Amendment and privacy were in partnership, not in conflict. California constitutional privacy rights should and can be a particularly effective legal lever to address privacy threats in the modern digital age.

IV. WHAT SHOULD HAPPEN

Right now, it is more important than ever for California courts and policymakers to fully utilize the California constitutional right to privacy to properly support rights, equity, and justice in the modern digital age. The California constitutional right to privacy was developed and passed at a time when Californians knew how much was at stake, when movements for racial justice and reproductive rights were under attack, and when many activists were literally fighting for their lives in battling for civil rights, mobilizing against the Vietnam War, and seeking safe and accessible abortions. It was built at a time when many Californians did not feel confident that the federal courts or the federal government could protect their rights, their bodies, or their lives. It was a time when Californians had good reason to fear how advances in technology would be weaponized against social justice movements, individual

357. CAL. CIV. PROC. 526a (authorizes actions to stop "any illegal expenditure of, waste of, or injury to, the estate, funds, or other property of a county, town, city or city and county." The California Supreme Court held that taxpayers do not need a "special, personal interest in the outcome" of the case to have standing to sue.); *see also* Connerly v. State Personnel Board, 92 Cal. App. 4th 16 (2001). ("If an action meets the requirements of section 526a, it presents a true case or controversy."); Blair v. Pitchess, 5 Cal. 3d 258, 269 (1971). Taxpayer standing has been used in numerous Article I, Section 1 cases including *White v. Davis* and *Loder*.

358. City of Santa Monica v. Stewart, 126 Cal. App. 4th 43, 59 (2005).

359. *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), https://repository.uclawsf.edu/ca_ballot_props/762.

rights, and the foundations of democracy. We are again facing similar circumstances.

There was widespread surveillance and efforts to intimidate racial justice protesters who took to the streets in 2020 to speak out against the murders of George Floyd and the many other Black lives taken by police.[360] A year-long investigation by the ACLU of Northern California revealed that the California Highway Patrol engaged in aerial surveillance of people protesting against police brutality in cities throughout California.[361] One Sacramento community member described the police presence as "psychological warfare . . . the protests were very peaceful and it was mostly young people, kids in attendance . . . but many people got scared off by the police aggression and helicopters, and it felt like the goal of the low-flying choppers was to terrorize people."[362] Meanwhile, in Kenosha, Wisconsin, the FBI used dragnet geofence demands to try to identify protesters after local police shot Jacob Blake four times in the back.[363]

The U.S. Supreme Court has issued a series of rulings that undermine rights and threaten the rule of law and democracy. On June 24, 2022, the Court issued its shameful ruling overturning *Roe v. Wade*, the landmark decision of nearly fifty years recognizing the constitutional right to abortion.[364] Affirmative action policies were also struck down by the Court in June 2023 in a pair of decisions.[365] In 2024, the conservative-majority Supreme Court issued another

360. *Spies in the California Skies: New Records Expose State Police Aerial Surveillance of Racial Justice Protesters*, ACLU OF N. CAL. (Nov. 16, 2021), https://www.aclunc.org/article/spies-california-skies-new-records-expose-state-police-aerial-surveillance-racial-justice.

361. *Spies in the California Skies: New Records Expose State Police Aerial Surveillance of Racial Justice Protesters*, ACLU OF N. CAL. (Nov. 16, 2021), https://www.aclunc.org/article/spies-california-skies-new-records-expose-state-police-aerial-surveillance-racial-justice.

362. Jennifer Jones & Matt Cagle, *Recordings Show the California Highway Patrol's Aerial Surveillance of Racial Justice Protests*, ACLU OF N. CAL. (Nov. 16, 2021), https://www.aclunc.org/blog/recordings-show-california-highway-patrol-s-aerial-surveillance-racial-justice-protests.

363. Russell Brandom, *How Police Laid Down a Geofence Dragnet for Kenosha Protestors*, VERGE (Aug. 30, 2021), https://www.theverge.com/22644965/kenosha-protests-geofence-warrants-atf-android-data-police-jacob-blake.

364. Press Release, ACLU, ACLU Comment on Supreme Court's Decision to Overturn Roe v. Wade (June 24, 2022), https://www.aclu.org/press-releases/aclu-comment-supreme-courts-decision-overturn-roe-v-wade.

365. Press Release, ACLU of North Carolina & ACLU of Massachusetts, ACLU Comment on Supreme Court's Ruling Against Harvard and UNC's Affirmative Action Policies (June 29, 2023), https://www.aclu.org/press-releases/aclu-comment-on-supreme-courts-ruling-against-harvard-and-uncs-affirmative-action-policies.

series of rulings undermining rights[366] and democracy, including embracing an expansive view of presidential immunity in *Trump v. United States*[367]—a case in which Justice Sonia Sotomayor wrote, '[w]ith fear for our democracy, I dissent."[368]

Berkeley Law Dean Erwin Chemerinsky sounded an alarm about the fate of privacy rights on the federal level in his keynote remarks at the Berkeley Technology Law Journal symposium in October 2023. He discussed the important role for California law and the California constitutional right to privacy in safeguarding and promoting rights in the years to come. Chemerinsky contended that for the three main aspects of privacy—protection from intrusion (Fourth Amendment), informational privacy, and autonomy: "it is to each of these aspects of privacy, the United States constitutional law is inadequate and getting worse. To each of these, the federal statutes are unlikely to write the answer. It is to each of these that focusing on California law becomes crucial."[369]

While Chemerinsky warned that the current majority on the Supreme Court will likely continue to further diminish Fourth Amendment protections, he pointed to the California Constitution as a source of privacy protection.[370] He commented, "if there's going to be protection of informational privacy, it's going to need to come from under the California Constitution."[371] He highlighted that most people do not even realize that "the Supreme Court has never protected a right of informational privacy under the United States Constitution"[372] and it is highly unlikely to find one now with the current makeup of the Supreme Court.[373] Moreover, he warned that the reasoning of Justice Alito in the majority opinion in *Dobbs* puts in doubt all of the privacy rights previously decided by the Court. As Chemerinsky articulated, "if there is going to be protection for privacy, it's not going to come from the Supreme Court, it's not likely to come from Congress. It's going to come from the states,

366. Press Release, ACLU, ACLU Responds to Supreme Court Decision that Cities Can Punish People for Being Homeless (June 28, 2024), https://www.aclu.org/press-releases/aclu-responds-to-supreme-court-decision-that-cities-can-punish-people-for-being-homeless; *see* City of Grants Pass v. Johnson, 144 S. Ct. 2202 (2024).

367. Trump v. United States, 144 S. Ct. 2312 (2024).

368. *See* Justin Jouvenal & Ann E. Marimow, *Key Takeaways from the Supreme Court Term That Upended Trump's Trial*, WASH. POST (July 2, 2024), https://www.washingtonpost.com/politics/2024/07/02/supreme-court-takeaways-2024-rulings/.

369. Erwin Chemerinsky, Dean, Berkeley L., 4th Annual BTLJ-BCLT Fall Symposium: Keynote Address, https://bk.webcredenza.com/watch?id=85344 at (2:10 – 2:28).

370. *Id.* at (10:54 – 11:07).

371. *Id.* at (15:15 – 15:37).

372. *Id.* at (12:22 – 12:42).

373. *Id.* at (14:29 – 14:46).

and California is so well positioned to be able to do this because of the protection of privacy in the California Constitution and because there are increasingly robust statutes in California."[374]

Dorothy Ehrlich, who spent fifty years working at the ACLU, from starting as an undergraduate intern at the time of the passage of the Privacy Amendment to retiring as the Deputy Executive Director of the ACLU in 2023, spoke eloquently at the same Berkeley Law symposium about the need to utilize integrated advocacy to defend and promote privacy rights. As she put it, "as we see the lights in the courthouse grow increasingly dim, in particular, in the federal courts and the United States Supreme Court, the importance of advancing other strategies must be elevated."[375]

A. CALIFORNIA COURTS SHOULD RECONSIDER *HILL'S* REASONING AND ASSUMPTIONS

There is a path forward for California courts to properly protect people's rights, starting with a careful reconsideration of *Hill* and its reasoning. California courts should recognize how the hurdles imposed for privacy claims in this California Supreme Court decision have undermined the ability of people to obtain their fundamental right to privacy. The voters unequivocally passed the California constitutional right to privacy and the *Hill* decision is inconsistent with both the language and legislative history of the Privacy Amendment. Further, the Court now has much more context for assumptions made in the *Hill* decision, which have not borne out in practice. It was already questionable in 1994 that: (1) private parties cannot pose as great a danger as the government; (2) that an individual generally has greater choice and alternatives in dealing with private actors than when dealing with the government; and (3) that there is a meaningful distinction between autonomy and informational privacy. In the modern digital world, these three arguments no longer hold water.

1. *Carefully Consider* Hill *and Its Impact on People to Obtain Their Fundamental Right to Privacy*

The California Supreme Court should carefully consider how *Hill* deviated from the language and intent of the California constitutional right to privacy, and how it has made it very difficult for people to actually obtain their fundamental right to privacy. After the *Hill* decision, the vast majority of

374. *Id.* at (00:44 – 1:20).

375. Dorothy Ehrlich, former Deputy Executive Director, ACLU, Panel at the Berkeley Technology Law Journal Symposium: California Constitutional Privacy at 50: Power of State Law and Promoting Racial Justice in the Digital Age (Oct. 27, 2023), https://bk.webcredenza.com/watch?id=85341 at (18:19).

California constitutional privacy cases have not been able to move forward. The elements for a privacy claim promulgated in *Hill*, which include the reasonable expectation of privacy in element two, and a serious invasion in element three, often stops privacy claims from moving forward, even when the intruding party has provided no justification for the conduct[376] and there has been no inquiry about any less intrusive means.[377] A 2021 analysis looked at privacy cases since 2009 and found that courts rejected 80% of constitutional privacy claims.[378] Informational privacy claims made up 77% of the total failed claims in ninety-two actions brought in state and federal court.[379] Also due to the weaker metric of countervailing interest that the current *Hill* analysis applies to privacy invasions for informational privacy claims, these claims failed at higher rates than autonomy privacy claims.[380] The high failure rate of informational claims suggested that the countervailing interest required to counterbalance a privacy interest in informational privacy cases is so low that the informational privacy claim is most often fatal in fact against plaintiffs.[381]

This very poor outcome for Californians to be able to pursue constitutional privacy claims and obtain their protected right to privacy is largely what Justice Mosk and Justice George both predicted and criticized in their separate opinions in *Hill*. Justice Mosk wrote in his dissent that "the majority's refusal to follow the law . . . all but renders the right of privacy nugatory."[382] Justice George wrote in his partial concurrence that, "the majority has, in my view, introduced an undesirable and unfortunate inflexibility into the constitutional analysis that, if faithfully applied, is likely to bar privacy claims that properly should be permitted to go forward.[383] Justice George specifically highlighted his concerns that the majority decision on its

376. Rodolfo Rivera Aquino, *California's Constitutional Privacy Guarantee Needs a Reset*, SCOCA BLOG (Apr. 9, 2021), https://scocablog.com/californias-constitutional-privacy-guarantee-needs-a-reset/.

377. In *Sheehan v. 49ers* in 2009, Justice Werdegar wrote a separate concurring opinion that harkens back to earlier case law and highlights the importance of the plaintiffs being afforded the opportunity to fully prove up a privacy claim, and not resolve privacy cases on demurrer, based solely on the initial portions of the *Hill* test. Sheehan v. San Francisco 49ers, 45 Cal. 4th 992, 201 (2009), https://scocal.stanford.edu/opinion/sheehan-v-san-francisco-49ers-33075.

378. Rodolfo Rivera Aquino, *California's Constitutional Privacy Guarantee Needs a Reset*, SCOCA BLOG (Apr. 9, 2021), https://scocablog.com/californias-constitutional-privacy-guarantee-needs-a-reset/.

379. *Id.*

380. *Id.*

381. *Id.*

382. Hill v. Nat'l Collegiate Athletic Assn., 7 Cal. 4th 1, 107 (1994).

383. *Id.* at 64.

face could limit privacy protection to only an egregious breach of privacy, even when the defendant is unable to provide any justification for an intrusion upon the constitutionally protected privacy interest. Justice George noted that privacy invasions like collection of unnecessary information by a business entity or government agency, or the use of properly obtained information for a purpose unrelated to its collection, "would not necessarily rise to the level of an 'egregious' breach of privacy, but, as the election pamphlet argument demonstrates, the Privacy Initiative clearly was intended to prohibit such conduct."[384]

This, is indeed, what has largely manifested in recent decades. By subverting the burden and including the elements of reasonable expectation of privacy in prong two and a serious invasion of privacy in prong three, very few informational privacy claims have been able to move forward in the courts. All the while, the personal information of Californians is now regularly collected, used, and shared in the very ways that the Privacy Amendment was meant to prohibit. With the rise of artificial intelligence, the stakes of properly protecting privacy will likely only increase.

It will be important for the California Supreme Court to truly reexamine the *Hill* decision when the opportunity presents itself. To consider how the decision deviated from the legislative history and language of the Privacy Amendment and existing precedent and interrogate how the assumptions that undergird the decision have not borne out in practice in the modern digital world. Namely that: (1) private parties cannot pose as great a danger as the government; (2) that an individual generally has greater choice and alternatives in dealing with private actors than when dealing with the government; and (3) that there is a meaningful distinction between autonomy and informational privacy in the digital world.

2. *Carefully Consider* Hill*'s First Premise*: *Private Parties Do Pose As Great a Danger and Have Coercive Power Like the Government*

In *Hill*, the majority opinion premised their decision to support a standard for nongovernmental actions that is lower than that of "compelling public need" based on an assertion that "the pervasive presence of coercive government power in basic areas of human life typically poses greater dangers to the freedoms of the citizenry than actions by private persons."[385] Justice Kennard's concurrence in *Hill* also discussed this premise and highlighted that "when the actions of a nongovernmental entity or person are alleged to have invaded constitutional privacy rights, the majority opinion properly demands

384. *Id.* at 68.
385. *Id.* at p. 38 (Maj. Opn., ante).

an additional degree of judicial caution" and should be tested by a "less rigorous" standard because the government has "greater coercive power."[386]

The decision to subject privacy invasions by private parties to a less rigorous standard than that of government actions is contrary to the ballot measure and its understanding of the power of both government and private parties to violate privacy in deeply harmful ways in the modern digital age. As Justice Mosk wrote in his dissent, "[t]he people who voted for Proposition 11 did not share that view. To judge from the ballot arguments on the measure, they deemed nongovernmental actors to be no less threatening than governmental actors."[387] "To quote, informational privacy is guaranteed against the 'collecting and stockpiling [of] unnecessary information about us' by 'government and business interests;' the 'proliferation of government and business records over which we have no control;' the 'loss of control over the accuracy of government and business records on individuals.'"[388] As Justice George also wrote in his separate opinion, "[t]he ballot argument in support of the Privacy Initiative demonstrates that the drafters of the provision believed that overreaching actions by private entities frequently will pose as significant a risk to an individual's privacy as actions by a governmental entity and intended that the constitutional guaranty protect an individual's privacy equally against both types of threats."[389]

Justice Mosk also elucidated that "even if the people who voted for Proposition 11 considered governmental actors to be more threatening than nongovernmental actors, such a fact would not matter for purposes here. The 'compelling public need' standard is "applied against actual abridgments of the right of privacy, not against the power to abridge." So even if "for argument's sake nongovernmental actors possess less of that power. Is that a reason to scrutinize their conduct more tolerantly when they successfully wield whatever power they have to affect an actual abridgment? The question answers itself."[390] Private actors have certainly taken advantage of any "judicial caution" in *Hill* to successfully wield their power to abridge and abridge since the early 2000s. As discussed in detail in Part III, the very surveillance capitalism business models used by most technology companies are based almost entirely at every step of the way on violating privacy rights and engaging in the very "principal mischiefs" at which the Privacy Amendment is directed.

386. *Id.* at 60–61.
387. *Id.* at 105.
388. *Id.* at 105.
389. *Id.* at 63.
390. *Id.* at 106–07.

Further, it is now quite apparent that the majority's belief that private parties do not pose the same type of dangers to the freedoms of the citizenry or have similar coercive power to the government was a faulty assumption about the power that could be wielded by businesses in the modern digital age. One only has to consider just a small sample of what has been happening in the last decade—from Cambridge Analytica[391] to misinformation[392]—to see that the impact of not fully holding private parties to account and forcing them to comply with the California constitutional right to privacy. It enabled technology companies to collect and use personal information in ways that endanger every aspect of our lives, rights, safety, social and economic opportunity, and the very fabric of our democracy.

Technology companies also have immense coercive power. The biggest technology companies are now richer than many countries in the world[393] and some believe they may become more powerful than nation states.[394] "The surveillance capitalist giants—Google, Apple, Facebook, Amazon, Microsoft, and their ecosystems—now constitute a sweeping political-economic institutional order that exerts oligopolistic control over most digital information and communication spaces, systems, and processes."[395] They can

391. Case Study, ACLU of Northern California, Cambridge Apocalyptica: Facebook's Platform-App Privacy Disaster, https://www.itsgoodfor.biz/case-study/cambridge-apocalyptica-facebook%E2%80%99s-platform-app-privacy-disaster (last visited May 9, 2024); *Meet Brittany Kaiser, Cambridge Analytica Whistleblower Releasing Troves of New Files from Data Firm* (Democracy Now! broadcast Jan. 7, 2020), https://www.democracynow.org/2020/1/7/the_great_hack_cambridge_analytica.

392. *Social Media Policies: Mis/Disinformation, Threats, and Harassment*, STATES UNITED DEMOCRACY (2023), https://statesuniteddemocracy.org/resources/social-media-policies/; Kristen Weir, *This Election Year, Fighting Misinformation is Messier and More Important Than Ever*, 55 MONITOR ON PSYCH. 40 (2024), https://www.apa.org/monitor/2024/01/trends-fighting-misinformation-disinformation-election-year; Shoshana Zuboff, *Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization*, 3 ORGANIZATION THEORY, 21 (2022), https://doi.org/10.1177/26317877221129290 ("Disinformation on Facebook is known to have distorted elections, produced violence, and degraded social discourse in nearly every world region.") (citing Akinwotu, 2021; Del Vicario et al., 2016; Hao, 2021a, 2021b; Mozur & Scott, 2016; Silverman et al., 2022; Wong, 2021).

393. Tom Valovic, Opinion, *Big Tech Companies Are Becoming More Powerful Than Nation-States*, COMMON DREAMS (Apr. 25, 2023), https://www.commondreams.org/opinion/big-tech-companies-more-powerful-than-nations.

394. Audrey Cronin, *How Private Tech Companies Are Reshaping Great Power Competition*, KISSINGER CTR. PAPERS (2023), https://sais.jhu.edu/kissinger/programs-and-projects/kissinger-center-papers/how-private-tech-companies-are-reshaping-great-power-competition.

395. Shoshana Zuboff, *Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization*, 3 ORGANIZATION THEORY, 1 (2022), https://doi.org/10.1177/26317877221129290.

even shape the way people think.[396] And while it is true that a private company cannot yet physically put you behind bars, all the information that companies collect and how it is used can determine whether you get a job, a mortgage, or in the case of face recognition,[397] automated license plate readers,[398] and other surveillance and policing technology—whether you literally do end up in jail due to mistakes in the technology system.

The ways that technology companies and their unbridled collection and use of personal information have affected individuals and society in the last decade is just the tip of the iceberg of their coercive power and the dangers they pose to our freedom. Artificial intelligence (AI) further ups the ante for privacy invasion and dangers to the freedoms of the citizenry. Risks to privacy, freedom of expression, and democracy can be amplified with the integration of new AI systems that, as President Biden's 2023 Executive Order on AI acknowledged, will may it easier to "extract, re-identify, link, infer, and act on sensitive information about people's identities, locations, habits, and desires."[399] It is critical to deeply consider how AI systems that both government and business may try to develop and use intersects with the fundamental privacy right guaranteed to all Californians. The reality of AI is that it uses vast amounts of personal information, with very little transparency right now about when this personal information was collected or for what original purpose. These powerful technology systems are also poised to make decisions about everything from employment, to healthcare, and housing.[400]

People's rights are acutely implicated by the growth, development, and use of AI.[401] Many Americans already have some well-justified concerns and little trust in how companies will protect their rights in the era of AI. The Federal Trade Commission has already warned that they are watching out for companies deceiving people about "how their information is collected,

396. *Are Big Tech Companies Trying to Control Our Lives?*, PBS NEWSHOUR (Sept. 14, 2017), https://www.pbs.org/newshour/show/big-tech-companies-trying-control-lives.

397. Robert Williams, *I Did Nothing Wrong. I Was Arrested Anyway*, ACLU (July 15, 2021), https://www.aclu.org/news/privacy-technology/i-did-nothing-wrong-i-was-arrested-anyway.

398. Matt Cagle, *San Francisco - Paying the Price for Surveillance Without Safeguards*, ACLU OF N. CAL. (May 22, 2014), https://www.aclunc.org/blog/san-francisco-paying-price-surveillance-without-safeguards.

399. Exec. Order No. 14110, 88 Fed. Reg. 75191 (Oct. 23, 2023), https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

400. *Id.*

401. ACLU California Action Comment on Executive Order N-12-23 regarding Generative Artificial Intelligence, Part 3(b), ACLU OF N. CAL., https://www.aclunc.org/sites/default/files/ACLU%20Comment%20on%20GenAI%20Executive%20Order.pdf.

whether explicitly or implicitly, by inclusion or by omission."[402] A 2023 Pew study found that 81% of people who have heard of AI believe that the information companies collect will be used in ways that people are not comfortable with and 80% say it will be used in ways that were not originally intended.[403] Only about one in five people are confident that those with access to their personal information will treat it responsibly.[404] The growth of AI and its effect on people and society is just one of the reasons that the Court should interrogate the underlying premise in the *Hill* decision that actions by private parties cannot pose the same type of dangers to the freedoms of the citizenry or have similar coercive power.

When *Hill* was decided in 1994, it was already a dubious premise that private actors hold less coercive power in the basic areas of human life and pose fewer dangers to the freedoms of the citizenry in the modern digital age. Now, with the massive power of technology companies and the further growth of AI, this foundational premise in the *Hill* case is deeply suspect and should be reconsidered.

3. Carefully Consider Hill*'s Second Premise*: *There is No Greater Choice and Alternatives with Private Actors in the Digital Age*

The second related, now faulty, premise underlying the *Hill* decision is that "an individual generally has greater choice and alternatives in dealing with private actors than when dealing with the government."[405] Even in 1994, this premise could not be generally supported. As Justice George highlighted, this may be true only in "some circumstances," "for example where there are many private entities, offering the identical service, that do not condition their service on the same intrusive requirement."[406] But this factual question, that was already inconsistent across circumstances in 1994, should not have been used as a principle for determining the general reach of the constitutional right to privacy. Indeed, circumstances in today's rapidly changing modern world are that choice and alternatives to "avoid the same intrusive requirement" are

402. *AI Companies: Uphold Your Privacy and Confidentiality Commitments*, FTC: TECH. BLOG (Jan. 9, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/01/ai-companies-uphold-your-privacy-confidentiality-commitments.

403. Michelle Faverio, *Key Findings About Americans and Data Privacy*, PEW RSCH. CTR. (Oct. 18, 2023), https://www.pewresearch.org/short-reads/2023/10/18/key-findings-about-americans-and-data-privacy/.

404. *Id.*

405. Hill v. Nat'l Collegiate Athletic Assn., 7 Cal. 4th 1 (1994), Maj. Opn. at 38; *id.* at 60 (J. Kennard, concurring) ("generally wider range of choice available to individuals when dealing with private entities").

406. *Id.* at 63.

extremely limited. People in the "digital environment have highly limited options for consent, much less for bargaining."[407]

More often than not, the only option to avoid a privacy intrusion from a private party is to refrain from technological activity altogether, rather than find a private party alternative that does not invade privacy for profit. For example, there is no cell phone that you can use that does not collect location information in some way[408] and the U.S. Supreme Court has recognized that cell phones are a "pervasive and insistent part of daily life."[409] As the Court pointed out, "[p]eople cannot browse the web without being tracked, period."[410] Whether it be medical websites, websites for lawyers, websites for politicians, or newspaper websites, there are now very few things that "people don't seek out or share using a computer and nearly all of that is tracked, all the time, by the billion-dollar giants you see in the news as well as hundreds of companies you've never heard of."[411]

The reality is that almost every private company conditions their services on the same type of intrusive privacy invasions—there is very little choice and very few alternatives to their products. Other companies all saw that Google and Facebook were able to freely collect and use everyone's personal information for profit, and that they were not held to account under any privacy law, including the California constitutional right to privacy. So, surveillance capitalism flourished throughout the current economy. From cell phones and search engines to email and online documents, essential services for our daily lives now all regularly invade our privacy for profit. Further, many of these services are controlled by just a few, very powerful companies in monopoly and near monopoly. Microsoft, Apple, and Google have all been

407. See Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1487–88 (2019), https://openscholarship.wustl.edu/law_lawreview/vol96/iss6/11 ("consumers in the digital environment have highly limited options for consent, much less for bargaining.").

408. Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, FTC: BUS. BLOG (Jan. 9, 2024), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal.

409. Riley v. California, 573 U.S. 373, 385 (2014).

410. *Id.*

411. Nathalie Maréchal, *Targeted Advertising Is Ruining the Internet and Breaking the World*, VICE (Nov. 16, 2018) (quoting Tim Libert, who was at that time working at the CyLab Security and Privacy Institute at Carnegie Mellon University), https://www.vice.com/en/article/xwjden/targeted-advertising-is-ruining-the-internet-and-breaking-the-world.

sued by the Department of Justice for antitrust violations.[412] The Federal Trade Commission (FTC) has sued Facebook for its actions to squelch competitors.[413] The FTC and state attorneys general have sued Amazon.[414] Additionally, in January 2024, the FTC opened an inquiry into the big tech companies and their potential monopolistic dealings with new areas of AI.[415]

It is important to recognize that while a lack of choice and actual control affects all people in the digital age, it does not affect all people equally. Already, marginalized people can face compounding factors of discrimination, disproportionate policing and surveillance, interaction with the criminal justice system, and poverty and forced use of services that further affect whether people feel empowered to avoid a privacy intrusion. In the Our Data Bodies project, community members talked about being "haunted" by digital "profiles" that impact their ability to move forward from incarceration and debt.[416] Community members talked about desiring and caring about privacy, but feeling like "they have no choice but to give up information."[417] That the experience of pervasive data collection makes them feel dehumanized "like a number"[418] and "powerless."[419] They felt "set up," with "traps" or "moments in their lives of being forced or cornered into making decisions where human rights and needs are on a chopping board."[420] For many of the community members, pervasive law enforcement surveillance was also front and center in their lives.[421] The information collection, and whether people felt able to avoid

412. Kif Leswing & Rohan Goswami, *DOJ Sues Apple over iPhone Monopoly in Landmark Antitrust Case*, CNBC (Mar. 21, 2024), https://www.cnbc.com/2024/03/21/doj-sues-apple-over-iphone-monopoly.html.

413. Shannon Bond, *Federal Trade Commission Refiles Suit Accusing Facebook Of Illegal Monopoly*, NPR (Aug. 19, 2021), https://www.npr.org/2021/08/19/1029310979/federal-trade-commission-refiles-suit-accusing-facebook-of-illegal-monopoly.

414. Press Release, FTC, FTC Sues Amazon for Illegally Maintaining Monopoly Power (2023), https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-sues-amazon-illegally-maintaining-monopoly-power.

415. Scott Rosenberg & Ashley Gold, *FTC Opens Inquiry into Big Tech AI Investments*, AXIOS (Jan. 25, 2024), https://www.axios.com/2024/01/25/ai-chatpgt-ftc-investigation-openai.

416. Tawana Petty, Mariella Saba, Tamika Lewis, Seeta Peña Gangadharan & Virginia Eubanks, *Reclaiming Our Data*, *OUR DATA BODIES* 7 (June 15, 2018), https://www.odbproject.org/wp-content/uploads/2016/12/ODB.InterimReport.FINAL_.7.16.2018.pdf.

417. *Id.*

418. *Id.*

419. *Id.*

420. *Id.*

421. *Id.*

it, was also enmeshed with a culture of fear that was promulgated by over-policing and surveillance in their communities.[422]

Looking at the bigger picture, as Justice Mosk wrote in his *Hill* dissent, even if an individual had more initial choice with private parties, that still does not support allowing private parties to justify an actual privacy intrusion pursuant to a weaker standard. He contended, even if individuals had greater initial choice and alternatives in dealing with private actors, then "so what?"[423] While it is possible that an individual could possibly have more flexibility in engaging with a private actor and perhaps there ends up being no privacy intrusion, "it does not mean that the individual should be forced to bear an actual abridgment of his right of privacy with more tolerance simply because it was effected by a nongovernmental actor."[424]

Justice George explored a similar theme in his separate opinion. He articulated that whether the entity is a government or private actor should not affect how the privacy harm itself is adjudicated. What was important was "the nature and extent of the intrusion upon privacy resulting from the challenged conduct and the nature and strength of the justifications supporting that conduct."[425]

The factual question as to whether an individual had greater choice to be subjected to the privacy intrusion should not matter to the inquiry of whether a cognizable privacy intrusion has actually occurred and if it was properly justified. Nevertheless, if one were to actually consider this *Hill* premise that people have greater choice and alternatives with private parties, in the context of the digital business ecosystem today, this assumption from 1994 does not continue to hold up today.

4. *Carefully Consider* Hill*'s Third Premise: There is No Meaningful Distinction That Supports Different Standards for Invasions of Autonomy and Informational Privacy*

The third, related, now-faulty premise in the *Hill* decision is that there is a meaningful distinction between autonomy and informational privacy in the modern digital world, and that only privacy invasions related to autonomy interests should continue to be weighed against a compelling interest. This is a legal distinction that was tacked on after-the-fact to the constitutional right to privacy in the *Hill* case, more than twenty years after the passage of the

422. *Id.*
423. Hill v. Nat'l Collegiate Athletic Assn., 7 Cal. 4th 1, 106 (1994).
424. *Id.*
425. *Id.* at 63–64.

Privacy Amendment. There is no support for it in the amendment's legislative history.

As Justice Mosk discussed in his dissent, the ballot arguments on the Privacy Amendment have a "single standard for use against all abridgments of the right of privacy, that of "compelling public need," and "demonstrate that such abridgments may involve not only autonomy privacy but also informational privacy."[426] The legislative history of the Privacy Amendment makes it clear that protecting against broad types of privacy intrusions was purposeful and its drafters had no desire or intent to have a different standard to adjudicate autonomy privacy and informational privacy claims.

The Court's decision in *Hill* to manufacture a lower countervailing interests standard to justify informational privacy claims was both legally unsupported and already did not make factual sense in 1994. It really does not make sense today when we live digital lives and there are so few lines between our physical self and our information self. We live in a world where almost everyone has a smartphone that they carry everywhere they go, many people have devices like Apple Watches that they wear on their bodies, and others have devices like Google Nest thermostats and Amazon Ring doorbells installed at their homes. There are even numerous direct-to-consumer genetic testing companies.[427] *Roe v. Wade* has now been overturned by the U.S. Supreme Court, reproductive rights are being criminalized in many states, and the personal information collected by cell phones, through internet browsing history, and social media private messages can betray people seeking and obtaining reproductive healthcare.[428]

426. *Id.* at 107.

427. Report, Catherine Roberts, Consumer Reports, The Privacy Problems of Direct-to-Consumer Genetic Testing (2022), https://www.consumerreports.org/health/dna-test-kits/privacy-and-direct-to-consumer-genetic-testing-dna-test-kits-a1187212155/.

428. Dobbs v. Jackson Women's Health Organization, 597 U.S. 215 (2022), https://www.oyez.org/cases/2021/19-1392; Press Release, ACLU, ACLU Comment on Supreme Court's Decision to Overturn Roe v. Wade (Sept. 26, 2023), https://www.aclu.org/press-releases/aclu-comment-supreme-courts-decision-overturn-roe-v-wade.; Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 U. BALTIMORE L. REV., Iss. 1, Article 2, https://scholarworks.law.ubalt.edu/ublr/vol50/iss1/2 ("In the decades since Roe, smartphone and other surveillance technology has been introduced and is available to individuals, anti-abortion advocates, employers, and the government, making pregnant people vulnerable to surveillance of their whereabouts, their physical health, and their decision-making process regarding their bodies in multiple new ways."); *see also* Jon Keegan & Dara Kerr, *Online Abortion Pill Provider Hey Jane Used Tracking Tools That Sent Visitor Data to Meta, Google, and Others*, MARKUP (July 1, 2022), https://themarkup.org/pixel-hunt/2022/07/01/online-abortion-pill-provider-hey-jane-used-tracking-tools-that-sent-visitor-data-to-meta-google-and-others.

As Jacob Snow discussed in his article, many now-called "informational" privacy violations are "in fact ruinous to people's ability to exercise bodily, intellectual, democratic, and financial autonomy."[429] The collection, sharing, and use of personal information can cause people to be incarcerated, deported, to suffer bodily injury, and be vulnerable to economic harms like identity theft, higher prices and the inability to access new jobs, homes, and credit. Scott Skinner Thompson has also grappled with the deep interconnection of informational privacy and individual dignity and autonomy in his article, *Outing Privacy*. He contended that since privacy is "creating space for the formation and nurturing of political thoughts and preventing intimate, personal information from serving as the basis of potential discrimination," it is also proper to evaluate informational privacy claims using heightened scrutiny.[430] Californians continue to experience a changing technological landscape and a world in which both electronic and physical surveillance by both government and business diminishes people's autonomy. The California legislature and the people of California properly understood in 1972, and it has become even more apparent now, that the burden should be on the privacy invader to demonstrate a compelling interest for intruding upon any type of cognizable privacy interest.

The reasoning of the majority in *Hill* on these three points in 1994—(1) private parties cannot pose as great a danger as the government and hold less coercive power; (2) that an individual generally has greater choice and alternatives in dealing with private actors than when dealing with the government; and (3) that there is a meaningful distinction between autonomy and informational privacy in the digital world—does not reflect current reality. These premises and their bearing on the decision in *Hill* need to be reconsidered by the California Supreme Court.

In large part because of the *Hill* decision, the constitutional right to privacy has not been able to be used in the ways that it was intended to protect against privacy invasions by government and business in the modern digital world. It is time for the California Supreme Court to look critically at *Hill* and how it radically departed from the language and intent of the California constitutional right to privacy. It should reexamine how it subverted the burdens by imposing new elements for privacy claims and undermined the constitutionally mandated default to protect privacy and put the onus on the government and

429. Jacob Snow, *Not Just Bodies and Homes: Autonomy Privacy Under Article I, Section 1*, 2023 BCLT-BTLJ Symposium (2023), https://btlj.org/2023/10/not-just-bodies-and-homes-autonomy-privacy-under-article-i-section-1/.

430. Scott Skinner-Thompson, *Outing Privacy*, 110 NW. U. L. REV. (Nov. 17, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2691422.

private parties to have a compelling interest to justify a privacy intrusion. Finally, it should reconsider, how the *Hill* decision was premised on three already-questionable assertions in 1994, which are not supportable in the modern digital age. Hopefully, the California Supreme Court will thoughtfully consider all these factors when the opportunity presents itself to review a privacy case, and it will fully restore the constitutional rights of Californians to pursue and obtain privacy in the digital age.

B. WHAT POLICYMAKERS SHOULD DO—PROTECT CURRENT PRIVACY LAWS & PASS ROBUST NEW LAWS

California and national policymakers who represent this state also need to fulfill their duty to the people of California, make sure that constitutional privacy rights are protected, and properly safeguard the rights and safety of people in the modern digital age.[431] First, California policymakers must safeguard existing powerful, legal levers like the California constitutional right to privacy and strong California statutory laws from industry efforts to undermine the reach of existing privacy law through channels such as federal preemption. Second, California policymakers should ensure policy debates recognize that protecting people's privacy is a constitutionally-required default, and it must take steps to consistently support and enact more laws and policies that faithfully help to operationalize the California constitutional right to privacy. The burden should be on the government or business to show a compelling interest for a privacy invasion, rather than on the people seeking to protect their privacy. Third, policymakers must guarantee that people can actually obtain privacy by ensuring that all personal information is covered and there is robust enforcement of privacy rights through private rights of action and government enforcement resources.

1. Policymakers Must Protect Current Privacy Protections From Preemption

The first, most concrete step for state and national policymakers to take today is to act in full force to protect current privacy protections. They cannot allow federal preemption to undermine the California constitutional right to privacy or any state privacy statutes. Recently proposed federal privacy bills have included language that would preempt state privacy protections, and thus

431. CAL. CONST. ART. XX § 3, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CONS&sectionNum=SEC.%203.&article=XX.

endanger constitutional rights.[432] Preemption cannot be allowed to move forward in any potential federal privacy law.

Preemption of state law is the holy grail for technology companies because they want to erase current state privacy laws and bottleneck any additional progress on privacy. Preemption is "the prize most desired by industry lobbyists."[433] After stonewalling any federal advances on consumer privacy for the past twenty years, the technology industry has now been working behind the scenes to pass a weak federal privacy law that will not address the core issues of the surveillance business model; instead, it would limit state action to protect and advance privacy by preempting existing and future state privacy law.[434] Any federal privacy law must be a floor, not a ceiling. States must be free to enforce existing laws and continue to enact new privacy laws that are stronger than any federal baseline.[435] Congress has historically given states room to enact stronger privacy laws[436] and for good reason. Technology can advance quickly, and Congress often moves slowly—as previously noted, Congress has still not updated the Electronic Communications Privacy Act of 1986. States serve a particularly critical function in an area of law as rapidly evolving as privacy. Barring continuing and efficient attention to the issue of

---

432. H.R.8152, 117TH CONG. § 404(b) (2021-2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/text ("No State or political subdivision of a State may adopt, maintain, enforce, prescribe, or continue in effect any law, regulation, rule, standard, requirement, or other provision having the force and effect of law of any State, or political subdivision of a State, covered by the provisions of this Act, or a rule, regulation, or requirement promulgated under this Act."). Discussion Draft, American Privacy Rights Act of 2024 § 20 (2024), https://d1dth6e84htgma.cloudfront.net/American_Privacy_Rights_Act_of_2024_Discussion_Draft_0ec8168a66.pdf ("Except as provided in paragraph (3), no State or political subdivision 30 thereof may adopt, maintain, enforce, or continue in effect any law, regulation, rule, or 31 requirement covered by the provisions of this Act or a rule, regulation, or requirement 32 promulgated under this Act.").

433. Daniel Solove, *A Faustian Bargain: Is Preemption Too High a Price for a Federal Privacy Law?*, TEACH PRIV. (2022), https://teachprivacy.com/a-faustian-bargain-is-preemption-too-high-a-price-for-a-federal-privacy-law/.

434. Neema S. Giuliani, *The Tech Industry is Suddenly Pushing for Federal Privacy Legislation. Watch Out.*, WASH. POST. (Oct. 13, 2018), https://www.washingtonpost.com/opinions/the-tech-industry-is-suddenly-pushing-for-federal-privacy-legislation-watch-out/2018/10/03/19bc473e-c685-11e8-9158-09630a6d8725_story.html.

435. *ACLU, Affiliates Lead Coalition Letter with Local, State, and National Advocacy Organizations, Raising Concerns About APRA's Approach to Preemption*, ACLU (June 17, 2024), https://www.aclu.org/documents/aclu-affiliates-lead-coalition-letter-with-local-state-and-national-advocacy-organizations-raising-concerns-about-apras-approach-to-preemption; *ACLU Statement on American Data Privacy Protection Act, Ahead of Committee Markup*, ACLU (July 18, 2022), https://www.aclu.org/documents/aclu-statement-american-data-privacy-protection-act-ahead-committee-markup.

436. For example, the Graham-Leach-Bliley Act preempts state laws only where they fail to provide greater protection than that Act. 15 U.S.C. § 6807(b).

privacy, preemption would freeze the current regime in place. Professor Dan Solove characterized preemption as a "Faustian bargain."[437] The United States would finally have a federal privacy law, but "we'll end up with an antiquated privacy law that will preempt a main engine for change—the possibility of state legislative action through legislatures and especially referendums."[438] Allowing a federal law with preemption would be a net loss for people's privacy rights, if not immediately (which I firmly believe it would be), then definitely over time.

In support of preemption and a concerted attack on efforts to actually advance much-needed privacy change, the technology industry utilizes a narrative that a "patchwork" of privacy laws will stifle innovation, break the internet, and kill jobs. I know from experience leading state-based work in privacy that the technology industry has consistently pushed this narrative, at every opportunity. It is ubiquitous. Just search online for "patchwork" and "privacy" and tens of millions of results come up. Never mind that the United States is well, fifty states, knit together, with significant lawmaking powers left to the states by design.[439] Using the parlance of the technology industry, this is a feature, not a bug, of democracy so the states can, in Justice Brandeis' famous words, function as a "laboratory" of democracy.[440] Companies regularly comply with broad differences of statutes and codes in other areas of the law, such as criminal law, which consists of different state criminal codes across the country.[441] They also comply with state laws on fair employment and workplace safety, where most state laws "offer more protections than the federal ones."[442] Further, to avoid any issues with differences in privacy laws between states, companies can just comply with all the most stringent provisions of each law, and then different state laws together function as a

437. Daniel Solove, *A Faustian Bargain: Is Preemption Too High a Price for a Federal Privacy Law?*, TEACH PRIV. (July 22, 2022), https://teachprivacy.com/a-faustian-bargain-is-preemption-too-high-a-price-for-a-federal-privacy-law/.

438. Daniel Solove, *Further Thoughts on ADPPA, the Federal Comprehensive Privacy Bill*, TEACH PRIV. (July 30, 2022), https://teachprivacy.com/further-thoughts-on-adppa-the-federal-comprehensive-privacy-bill/.

439. U.S. CONST. *amend.* X, https://constitution.congress.gov/constitution/amendment-10/.

440. New State Ice Co. v. Liebmann, 285 U.S. 262 (1932) to describe how "a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country.

441. *Criminal Code By State*, *Legal Information Institute*, CORNELL L., https://www.law.cornell.edu/wex/table_criminal_code (last visited May 10, 2024).

442. *Workplace Laws*, USA.GOV, https://www.usa.gov/workplace-laws#:~:text=Each%20state%20sets%20laws%20related,labor%20laws%20in%20your%20state (last updated Dec. 11, 2023).

baseline for them to follow nationwide. Finally, there is no evidence that any of this technology industry narrative is true. The sky has not fallen, and the technology industry has not gone dark, when any state or the European Union passed new privacy laws or enforced privacy protections. In fact, their actions often encouraged innovation, with technology companies finding new ways to do what they do, without invading privacy in the same ways.[443] This "patchwork" narrative in support of preemption efforts is just part and parcel of the same toxic, anti-democratic playbook that powerful industries like Big Tobacco and others have used time and time again to try to stop consumer protection.[444] Policymakers on the state and national level need to expose the technology industry's efforts to preempt state privacy laws as an anti-democratic, anti-privacy, pro-surveillance capitalism power grab, and make sure no federal privacy bill includes preemption.

2. Policymakers Must Support Robust Privacy Laws that Operationalize the California Constitutional Right to Privacy and Neutralize Efforts That Legitimize Privacy Invasions

Policymakers also need to fully discharge their duty to defend and support the constitutional right to privacy. They need to do much more to support robust privacy laws that help operationalize this right and neutralize efforts that do not prevent privacy invasions or otherwise legitimize privacy invasions.

The Privacy Amendment created a self-executing fundamental right to privacy,[445] and this fundamental right means that there is a constitutionally-mandated default that the starting point for any legal or policy debate should be that privacy is protected. The legal and policy burden should be on the government or business to prove a compelling interest for a privacy invasion. The passage of the constitutional right to privacy served "notice on the Legislature . . . that the public will not permit the continual abrogation of their rights" and that "the right to privacy must be clearly spelled out and must be

443. Google first said that they could not blur faces in Streetview, but then when pressured by Europeans, innovated the technology to do so. *Investigations of Google Street View*, EPIC, https://epic.org/documents/investigations-of-google-street-view/ (last visited May 10, 2024); see also Stephen Shankland, *Google Begins Blurring Faces in Street View*, CNET (May 13, 2008), https://www.cnet.com/culture/google-begins-blurring-faces-in-street-view/.

444. The "tobacco industry's relentless pursuit of preemption to weaken, impede or defeat tobacco control efforts." Fact Sheet, Tobacco Control Consortium, *Preemption: The Biggest Challenge to Tobacco Control* (2014), https://publichealthlawcenter.org/sites/default/files/resources/tclc-fs-preemption-tobacco-control-challenge-2014.pdf.

445. White v. Davis, 13 Cal. 3d 757, 775 (1975).

firmly adhered to."[446] California policymakers seem to have lost this note over the subsequent years and too often let technology companies, law enforcement, and their money-powered narratives hold sway in the legislative debate. They are failing to protect privacy as the default and put the burden on the privacy invaders to have to demonstrate a compelling public interest to invade people's fundamental rights.

When there is a policy debate, California policymakers need to go back to first principles of constitutional protections and interrogate bills and other policy efforts with these types of questions:

- Does it help to operationalize and support the constitutional right to privacy?
- Does it protect a person's fundamental privacy rights? And if so, how?
- What privacy mischief does it address? And how does it prevent it from occurring?
- Does it prevent a privacy invasion unless the government or business can justify a privacy invasion with a compelling public interest?
- Can people easily enforce the law and make sure that their rights are protected?

OR

- Does it legalize or otherwise legitimize a privacy invasion by authorizing it or implementing weak rules that allow it to go forward?
- Is the policy debate improperly subverting the power balance mandated by the California constitutional right to privacy and putting the burden on an individual to justify their rights, rather than requiring a government or business to justify its invasion with a compelling public interest?
- Is it undermining the full scope of the California constitutional right to privacy by only protecting privacy of a limited category of personal

446. *Staff report of Assembly Constitutional Committee on ACA 51 (before April 24)*, ACLU OF N. CAL. (1972), at 5, https://www.aclunc.org/sites/default/files/Staff%20report%20of%20Assembly%20Constitutional%20Committee%20on%20ACA%2051%20%28before%20April%2024%29.pdf (last visited Sept. 21, 2023).

information or including exemptions that limit which Californians get privacy protections?

- Is it actually preventing a privacy invasion? Or is it putting the burden on an individual to have to take steps to protect their rights (often in practically impossible ways)?
- Is it undermining the inalienable right to privacy by allowing companies to penalize people—like charging them more or downgrading their service—if they try to use their privacy rights?
- Can all the provisions of the law be easily enforced? Or does it lack a private right of action and cannot be easily enforced by people to protect their rights?

Bills and other policy efforts at the local and state level that truly help to operationalize constitutional privacy rights by preventing privacy violations and can be efficiently and effectively enforced by people to protect their rights should be introduced by policymakers, broadly supported, and enacted into law. Bills and other policy efforts that undermine the full intent or scope of the constitutional right to privacy, legalize or otherwise legitimize privacy violations, improperly put the burden on individuals to try to protect their rights, or cannot be enforced by people, are not real privacy protections and should not move forward. Policymakers need to take their duty to protect the constitution seriously and properly protect Californians by supporting efforts that advance privacy rights and opposing efforts that undermine its strong protections.

3. California Has a History of Enacting Robust Privacy Law

Over the years, California has enacted strong statutory laws that help operationalize the California constitutional right to privacy. There are important laws that protect privacy by default and put the burden on the government to justify any privacy invasions. This legacy includes laws like the California Information Practices Act of 1977, which was specifically designed to help "implement the privacy amendment" by placing strict limits on the maintenance and dissemination of personal information by state agencies.[447] State agencies are required to limit the collection and retention of personal information to that necessary to accomplish the agency's specific purpose[448]

447. CAL. CIV. CODE § 1798.
448. CAL. CIV. CODE § 1798.24.

and all disclosures of personal information are restricted.[449] "Personal information" is also broadly defined.[450] The law also includes complementary transparency and information control provisions, providing that if an agency maintains a record, individuals must be able to inquire and be informed about its existence,[451] request amendments to correct any inaccurate information,[452] and obtain an accounting of disclosures, including disclosures pursuant to subpoena or search warrant.[453]

Landmark surveillance laws have also helped support the California constitutional right to privacy, including laws that I spearheaded like the California Reader Privacy Act and the California Electronic Communications Privacy Act. The California Reader Privacy Act robustly protects reading records in the digital age. It supports people's constitutional right to privacy[454] by requiring that government and civil litigants demonstrate a compelling interest in obtaining reader records and show that the information contained in those records cannot be obtained by less intrusive means.[455] The law also includes complementary transparency and reporting requirements for the provider to compile an annual report about demands for personal information from both the government and civil litigants.

The California Electronic Communications Privacy Act (CalECPA) broadly protects the privacy of electronic communications information and electronic devices from government privacy invasions. It supports people's constitutional right to privacy by requiring that any government entity must justify a privacy intrusion of demanding electronic communications information from a provider or accessing electronic device information, by demonstrating probable cause and obtaining a search warrant or wiretap

449. CAL. CIV. CODE § 1798.14.

450. CAL. CIV. CODE § 1798.3, subd. (a). The term "personal information" means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, the individual's name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.

451. CAL. CIV. CODE § 1798.32.

452. CAL. CIV. CODE §§ 1798.35–1798.37.

453. CAL. CIV. CODE § 1798.25.

454. Protection for reading records also supports people's free speech rights pursuant to Article I, Section 2 of the California Constitution, by allowing people to freely seek and receive information. CAL. CONST. art. I § 2, https://law.justia.com/constitution/california/article-i/section-2/.

455. CAL. CIV. CODE § 1798.90, https://law.justia.com/codes/california/2011/civ/division-3/1798.90-1798.90.05/1798.90/; *Reader Privacy Act Signed into Law*, ACLU OF N. CAL. (Oct. 3, 2011), https://www.aclunc.org/blog/reader-privacy-act-signed-law.

order.[456] CalECPA also further supports people's privacy rights, by including heightened particularity requirements for the warrant and preventing any information that is unrelated to the objective of the warrant to be used for other purposes without a further court order.[457] CalECPA also reinforces California jurisprudence that rejects the "third party doctrine" under search and seizure law. The California Supreme Court issued two opinions in the 1970s that specifically rejected the United States Supreme Court's third party doctrine and held that Californians do not forfeit their reasonable expectation of privacy related to government searches when businesses have their information.[458] The California Supreme Court determined that information sufficient to form a "virtual current biography" is subject to a reasonable expectation of privacy and thus protected under the search and seizure protections of Article I, Section 13 of the California Constitution.[459]

Other California privacy laws prohibit the government and private entities from engaging in certain conduct outright due to the seriousness of the privacy invasion. These include laws enacted like the Radio Frequency Identification (RFID) law that prohibits any person or entity from remotely reading any person's identification document without their knowledge[460] or another

456. *California Electronic Communications Privacy Act (CalECPA) – SB 178*, ACLU OF N. CAL., https://www.aclunc.org/our-work/legislation/california-electronic-communications-privacy-act-calecpa-sb-178 (updated Apr. 2018); CAL. PEN. CODE § 1546, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=PEN&division=&title=12.&part=2.&chapter=3.6.&article.

457. See Susan Freiwald, *CalECPA at the Privacy Vanguard*, 33 BERKELEY TECH. L.J. 131, 154 (2018), https://btlj.org/data/articles2018/vol33/33_1/Freiwald_Web.pdf.

458. *See id.* "The California Supreme Court issued two opinions in the 1970's that specifically rejected the United States Supreme Court's "third party doctrine," under which the Court had found no reasonable expectation of privacy, and therefore no Fourth Amendment protection, in business records and telephone numbers dialed. In contrast, the California Supreme Court held that people do not forfeit their reasonable expectations of privacy by using third parties to store their records. California's highest court determined that information sufficient to form a "virtual current biography" is subject to a reasonable expectation of privacy and California constitutional protection. Because a list of telephone numbers could create such a virtual current biography, the Court found a California constitutional right to privacy in an early form of metadata." *See* People v. Blair, 25 Cal. 3d 640, 653–54 (1979) (protecting telephone numbers); Burrows v. Superior Court, 13 Cal. 3d 238, 243 (1974) (protecting bank records).

459. CAL. CONST. art. I § 13, https://law.justia.com/constitution/california/article-i/section-13/.

460. CAL. CIV. CODE § 1798.79-1798.795, https://law.justia.com/codes/california/2010/civ/1798.79-1798.795.html#:~:text=(a)%20Except%20as%20provided%20in,person's%20knowledge%20and%20prior%20consent%2C; *see also Governor Takes Important Step To Protect Privacy and Safety*

privacy law that prohibits anyone from requiring, coercing or compelling any other individual to undergo the implanting of an identification device.[461] Important privacy laws have also been enacted related to surveillance technology, including local laws to prohibit face surveillance and state laws to prohibit biometric surveillance with police body cameras[462] and prohibit sharing of automated license plate reader information with out-of-state entities.[463]

Some California privacy laws also strictly limit how certain personal information can be collected, used, or shared. This includes privacy laws that prohibit the use, display or sale of social security numbers[464] or prohibit the collection of information in conjunction with a credit card purchase.[465]

4. Many Recent California Privacy Laws Are Not True Privacy Protections

However, many other privacy-related laws that have been enacted by California policymakers in recent years do not unilaterally prevent a privacy invasion, but rather utilize a transparency, notice, or consent framework. Laws that require online privacy policies,[466] data breach notifications,[467] and transparency about personal information collection and use like California's Shine the Light[468] can be an important complement to substantive privacy protections. California also has laws like the California Consumer Privacy Act (CCPA) which provide transparency and some opt-out and deletion rights for

---

of Californians; Signs RFID Anti-Skimming Legislation Into Law, ACLU OF N. CAL. (Oct. 2, 2008), https://www.aclunc.org/news/governor-takes-important-step-protect-privacy-and-safety-californians-signs-rfid-anti-skimming.

461. CAL. CIV. CODE § 52.7, https://codes.findlaw.com/ca/civil-code/civ-sect-52-7/.

462. In 2019, a local surveillance ordinance that the ACLU of Northern California developed and worked to pass in San Francisco included the first local ban on face surveillance in the country. Nicole Ozer, Kate Ruane & Matt Cagle, *Grassroots Activists are Leading the Fight to Stop Face Recognition. It's Time for Congress to Step Up, Too.*, ACLU (June 17, 2021), https://www.aclu.org/news/privacy-technology/grassroots-activists-are-leading-the-fight-to-stop-face-recognition-its-time-for-congress-to-step-up-too; *The Body Camera Accountability Act (AB 1215)*, ACLU OF N. CAL., https://www.aclunc.org/our-work/legislation/body-camera-accountability-act-ab-1215 (last visited May 10, 2024).

463. *Lagleva v. Doyle (License Plate Surveillance)*, ACLU OF N. CAL. (June 2, 2022), https://www.aclunc.org/our-work/legal-docket/lagleva-v-doyle-license-plate-surveillance.

464. CAL. CIV. CODE § 1798.85, https://codes.findlaw.com/ca/civil-code/civ-sect-1798-85/.

465. CAL. CIV. CODE § 1747.08, https://codes.findlaw.com/ca/civil-code/civ-sect-1747-08/.

466. CAL. BUS. & PROF. CODE §§ 22575–22579.

467. CAL. CIV. CODE §§ 1798.29, 1798.82, 1798.84.

468. CAL. CIV. CODE §§ 1798.80–1798.84, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=1798.83.&lawCode=CIV.

people,[469] and the Genetic Information Privacy Act, which requires that companies provide notice and consent, and provides people with deletion rights for the collection and use of genetic information from direct to consumer genetic testing companies.[470] The California Delete Act, signed in 2023, also makes it possible for any person to make one request to delete their personal information held by all data brokers registered in California.[471]

But true substantive privacy protections do not put the burden on people to digest complex information and take steps to try to protect their privacy. True California privacy protections should operationalize the constitutional right to privacy by actually prohibiting a privacy invasion from ever happening.

5. California Privacy Law Must Reject a Broken Notice and Consent Regime and Return to its Roots of Strong Privacy Protections

California was on the vanguard of properly protecting privacy in the modern digital age in the 1970s when it passed the Privacy Amendment and other robust laws that put the onus on privacy invaders to justify their actions, rather than put the burden on people to try to protect their rights. It must return to its roots and again be a true leader, by rejecting efforts that perpetuate a broken notice and consent approach.

There has been important scholarly work over the years about the inadequacy of the "notice and consent" framework of privacy laws by Helen Nissenbaum, Solon Barocas, Neil Richards, Woodrow Hartzog, Dan Solove,

469. CAL. CIV. CODE §§ 1798.110, 1798.105, 1798.120; *id.* at § 1798.140(ah)(1), https://oag.ca.gov/privacy/ccpa. The CCPA used some of the foundational transparency concepts developed for the Right to Know Act, but the ACLU did not support CCPA and opposed Proposition 24 because of its loopholes and that it too heavily put the burden on people to protect themselves. Jacob Snow & Chris Conley, *Californians Should Vote No on Prop 24*, ACLU OF N. CAL. (Oct. 16, 2020), https://www.aclunc.org/blog/californians-should-vote-no-prop-24. I helped develop and the ACLU in California supported the 2019 Privacy for All (AB 1760 – Wicks), https://www.aclunc.org/news/aclu-supports-new-california-bill-ensure-privacy-all.

470. CAL. CIV. CODE § 56.18, https://casetext.com/statute/california-codes/california-civil-code/division-1-persons/part-26-confidentiality-of-medical-information/chapter-26-genetic-privacy/section-5618-title-definitions-general-provisions; *see also Genetic Information Privacy Act (California)*, PRIVACYRIGHTS.ORG (2022), https://privacyrights.org/resources/genetic-information-privacy-act-california#:~:text=The%20Genetic%20Information%20Privacy%20Act,with%20access%20and%20deletion%20rights.

471. CAL. CIV CODE § 1798.99.86, https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.48.&part=4.&chapter=&article. There have been multiple California legislative efforts attempting to pass data broker transparency and information controls going back as far as 2005. Mark Lifsher, *State Lawmakers Grill ChoicePoint Over Privacy Concerns, Potential for ID Theft*, L.A. TIMES (Mar. 31, 2005), https://www.latimes.com/archives/la-xpm-2005-mar-31-fi-identity31-story.html; *In re Choicepoint*, EPIC, https://epic.org/documents/choicepoint-2/ (last visited May 10, 2024).

and many others.[472] In Solove's latest work, *Murky Consent*, he contended that "consent in privacy is beyond broken; it is a complete fiction."[473] I agree and I always have. The reality has always been that "[p]rivacy issues are too complex for people to understand sufficiently, dependent on things people can't find out, and impossible to scale. Most approaches to privacy consent try to fix it, to turn fiction into fact."[474] It has been clear for a very long time that privacy policies do not do anything to protect people's privacy.[475] The notice and consent regime is plagued with challenges and invites "unwitting and coerced consent."[476] Most basically, people are misled by the very term, privacy policy, thinking it promises that the company will protect their privacy.[477] When in fact, a privacy policy is regularly many pages of often legalese or otherwise confusing writing, describing all the ways that a company will invade privacy by collecting, using, and sharing information. Barocas and Nissenbaum have found "various types of complexity render current notice practically and inherently insufficient" in the behavioral advertising space, and concluded that

472. Solon Barocas & 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://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf. Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019), https://openscholarship.wustl.edu/law_lawreview/vol96/iss6/11; Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593 (2024), http://dx.doi.org/10.2139/ssrn.4333743.

473. 16th Annual BCLT Privacy Lecture (Sept. 22, 2023), https://www.law.berkeley.edu/research/bclt/bcltevents/16th-annual-bclt-privacy-lecture/; *see also* Solove, *supra* note 472 at 631–32 ("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.").

474. *Id.*

475. *See generally*, Joseph Turow, Yphtach Lelkes, Nora Draper & Ari E. Waldman, *Americans Can't Consent to Companies' Use of Their Data*, U. PA. ANNENBERG SCH. FOR COMMC'NS 13 (2023), https://perma.cc/J3ZR-RBG6 citing Paul M. Schwartz (1999), *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1609–1701 (1999) ("As early as 1999, Paul Schwartz warned that consent garnered through privacy notices was unlikely to be either informed or voluntarily given, that notices are generally meaningless since they are often ignored by individuals, written in vague legalistic language, and fail to present meaningful opportunities for individual choice.").

476. Joseph Turow, Yphtach Lelkes, Nora Draper & Ari E. Waldman, *Americans Can't Consent to Companies' Use of Their Data*, U. PA. ANNENBERG SCH. FOR COMMC'NS 13 (2023), https://perma.cc/J3ZR-RBG6; Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461 (2019), https://openscholarship.wustl.edu/law_lawreview/vol96/iss6/11.

477. Joseph Turow, Michael Hennessy & Nora Draper, *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation*, SSRN ELEC. J. (June 26, 2015), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820060.

even an opt-in consent regime "would lack legitimacy" in a climate of "confusing disconnects," the "fickle nature of privacy policies," and flows of data that are "opaque to users."[478] Meanwhile, Richards and Hartzog have written about the privacy paradox, observing that people do care about protecting their privacy, but can often be "nudged and manipulated by powerful companies against their actual interests, and that this process is easier when consumer protection law falls far from the gold standard.[479] Especially in the digital goods and services space, they found that consent has been relied upon too much and "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."[480]

But it is also particularly critical to recognize and address how the notice and consent framework, an approach based on the Fair Information Practices (FIPS) principles of the late 1970s (a framework developed by a federal government advisory board chaired by an engineer at the RAND Corporation),[481] does not properly take into account race, education, money, and other power structures that make this system even more broken for many people. As Anita Allen has explored, many current privacy laws, largely designed to implement FIPS concepts, are "inadequate for digital-privacy protection and equitable platform governance."[482] There must be an additional focus on the experiences of marginalized populations and to craft privacy interventions to address compounding vulnerabilities. For African Americans, Allen terms this the "Black Opticon" and it includes: (1) multiple forms of excessive and discriminatory surveillance; (2) targeted exclusion through differential access to online opportunities; and (3) exploitative online financial

478. Solon Barocas & 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://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf.

479. Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1463 (2019), https://openscholarship.wustl.edu/law_lawreview/vol96/iss6/11.

480. *Id.* at 1464.

481. Robert Gellman, *Fair Information Practices: A Basic History - Version 2.30* (Apr. 9, 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2415020. Willis Ware was a longtime engineer at the RAND Corporation and his research focused on the use of computer technology by both the military and society at large. W*illis Ware, Computer Pioneer, Helped Build Early Machines and Warned About Security Privacy*, RAND (Nov. 27, 2023), https://www.rand.org/pubs/articles/2013/willis-ware-computer-pioneer-helped-build-early-machines.html.

482. Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race, Equity, and Online Data-Protection Reform*, 131 YALE L.J. (Nov. 16, 2021), https://www.yalelawjournal.org/forum/dismantling-the-black-opticon.

fraud and deception.[483] Our Data Bodies, a research justice project that examined the impact of data collection and data-driven systems on the ability of marginalized peoples to meet their human needs, forcefully demonstrated the critical need to recognize and address sociopolitical power dynamics in policymaking and other privacy interventions.[484] During first person interviews in Charlotte, North Carolina; Detroit, Michigan; and Los Angeles California, community members described 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 . . . their experience of being caught in a cycle of injustice and the impact this feedback loop has on their livelihoods."[485] For community members, "data collection and data-driven systems represented unequal power dynamics in their lives. People described being in various situations of control and of having to give up one human right for another."[486] Khiara Bridges' extensive work on poverty and privacy and how poor mothers are stripped of their privacy rights[487] and Ruha Benjamin's work on the "New Jim Code," which "allows racist habits and logics to enter through the backdoor of tech design,"[488] is also important work about the current reality of privacy for many people in the digital age.

There are just too many privacy bills and laws, including California laws, that just tinker with solutions in ways that are impossible to actually work, due to both the economic dynamics that affect people, as well as more specific sociopolitical dynamics that affect many people far more than others. What is true across the board is that the "economic imperatives of this new capitalism produce extreme asymmetries of knowledge and the power that accrues from that knowledge"[489] People did not have to read a bunch of long documents and have check boxes and be asked to decide about whether or not to wear a seatbelt or consent to buying known dangerous products. Policymakers passed

483. *Id.*

484. Tawana Petty, Mariella Saba, Tamika Lewis, Seeta Peña Gangadharan & Virginia Eubanks, *OUR DATA BODIES, RECLAIMING OUR DATA* (June 15, 2018), https://www.odbproject.org/wp-content/uploads/2016/12/ODB.InterimReport.FINAL_.7.16.2018.pdf.

485. *Id.*

486. *Id.*

487. KHIARA M. BRIDGES, THE POVERTY OF PRIVACY RIGHTS (2017), https://books.google.com/books/about/The_Poverty_of_Privacy_Rights.html?id=V9RIvgAACAAJ.

488. Ruha Benjamin, *Race After Technology* 160 (2019).

489. Nathalie Maréchal, *Targeted Advertising Is Ruining the Internet and Breaking the World*, VICE (Nov. 16, 2018), https://www.vice.com/en/article/xwjden/targeted-advertising-is-ruining-the-internet-and-breaking-the-world.

laws ensuring baseline protection for people and funded agencies to understand complex issues and promulgate regulations. This is what is also needed for the information industry. But in addition to policy steps that must be taken to address how everyone is being affected by the surveillance ecosystem, the work of Allen and others reinforces that policymaking must also be explicitly antiracist to address compounding vulnerabilities and help to ensure that the interests of marginalized racial minorities are not overlooked.[490]

It is far from a radical new approach to pass real, privacy laws that affirmatively protect people. The public interest community has long recognized the fact that privacy consent is "futile."[491] Organizations that work on public interest technology legislation have tried to introduce and pass substantive privacy laws with clear prohibitions on information collection, use and disclosure. But weaker notice and consent frameworks have been the laws to move forward because the powerful forces of both the government and technology companies have used their resources to stymy more robust laws that impose any strict limits on the surveillance ecosystem. Further, some in the public interest community, including myself, believed that transparency, notice, and consent laws could function as a means to build more public understanding and support for substantive laws that actually prohibited privacy invasions.

My strategy in developing and supporting potential transparency laws like the California Right to Know Act in 2013 was not that these laws were the privacy end game.[492] I never saw the Right to Know Act of 2013 (and any of its base ideas that were then incorporated into the California Consumer Privacy Act) as a comprehensive privacy law. I always viewed these legislative efforts as simply a means to building more public knowledge and power so that the public interest community could gain the momentum to overcome the powerful forces of the surveillance lobby—both the technology companies who profit from it and government entities who want the information for surveillance—and pass real, robust, privacy laws that hit at the heart of the surveillance ecosystem. As I have previously written, passing these types of transparency laws could hopefully support this path by: (1) continuing to make privacy issues personal and common to a growing segment of people; (2)

490. Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race, Equity, and Online Data-Protection Reform*, 131 YALE L.J. (Nov. 16, 2021), https://www.yalelawjournal.org/forum/dismantling-the-black-opticon.

491. Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 597 (2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4333743.

492. *Right to Know Act (AB 1291)*, ACLU, https://www.aclunc.org/our-work/legislation/right-know-act-ab-1291.

making corporate information practices more visible and building pressure for company privacy change; (3) providing compelling stories for continued technology and mainstream press coverage; (4) illustrating privacy harms for regulatory, legislative, and court actions; and (5) creating momentum to interest philanthropic foundations and individual donors in providing sustaining resources for the public interest community's work in this area.[493] Knowing the flow of one's own information could also help counteract some information asymmetries, behavioral tendencies, and societal pressures. Such knowledge could help people better understand how privacy issues affect their daily lives, comprehend the information "costs" related to particular services, and not be as likely to overvalue benefit and underestimate risk with "free" online services. Some people would also hopefully be less susceptible to the "nothing to hide" argument[494] by understanding how information that they consider personal can wind up in the hands of others. This could all help to address challenges to developing and sustaining a social movement to defend and promote rights in the digital age and build the necessary power to pass robust privacy protections.

6. The Need to Pass Strong Privacy Laws is Not a New Idea

It would be a "paradigm shift" to successfully pass strong privacy laws that truly protect people, rather than notice and consent laws that put the burden on people to try to protect their own privacy and do not affect the technology company business model.[495] But I do not see a call to do so as a paradigm shift in how the public interest community has long seen these issues. The public interest community has deeply understood the faulty nature of notice and consent and consistently tried to pass substantive limitations for decades. It was well understood already in the 1970s, with the passage of the California constitutional right to privacy, that bold steps were needed to protect against the surveillance ecosystem and how it affected communities and movements. That is why the California constitutional right to privacy put the burden on the

493. Nicole Ozer, *Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. OF L. & SOC. CHANGE 215, 272–76 (2012), https://socialchangenyu.com/review/putting-online-privacy-above-the-fold-building-a-social-movement-and-creating-corporate-change/.

494. Daniel J. Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007), https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1159&context=faculty_publications.

495. Joseph Turow, Yphtach Lelkes, Nora Draper & Ari E. Waldman, *Americans Can't Consent to Companies' Use of Their Data*, U. PA. ANNENBERG SCH. FOR COMMC'NS 13 (2023), https://perma.cc/J3ZR-RBG6.

government and business to justify a privacy intrusion, not on people to demonstrate a reasonable expectation of privacy.

The potential privacy interventions discussed around the time of the development and passage of the California constitutional right to privacy also included laws and policies that prohibited what personal information could be collected and how it could be used. As John Pemberton, the ACLU Executive Director articulated at a law symposium in 1968, we can no longer rely on corporate and government inefficiency to protect our privacy and protect us from these dangers. These dangers will persist until "we take steps to discriminate about the kinds of information that are gathered and stored."[496] Arthur Miller, presenting at the same symposium, asserted that we must "regulate the character of information that private agencies can collect."[497] 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!"[498] The public interest community also focused on substantive protections in the late 1990s and early 2000s, as technology companies started to grow in earnest.[499] I have led state privacy and technology work in California since 2004 and I know personally of many efforts to introduce and pass substantive privacy laws that have flat out prohibited the collection, retention, use, or disclosure of personal information. In 2012, the FTC also held a series of roundtables around the

496. Richard Ruggles, John Pemberton & Arthur R. Miller, *Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 223 (1968), https://scholarship.law.umn.edu/mlr/2164/.

497. *Id.* at 240.

498. *Id.* at 244, emphasis in original. 499. *Testimony and Statement for the Record of Marc Rotenberg, Director, Electronic Privacy Information Center, on Communications Privacy before the Subcommittee on Courts and Intellectual Property*, Electronic Privacy Information Center (1998), https://archive.epic.org/privacy/internet/rotenberg-testimony-398.html (last visited May 10, 2024) (discussing Franken bill); California Financial Information Privacy Act, S. 1 (2003); Press Release, ACLU, California Privacy Act a Key Victory in Ongoing Financial Privacy Battle, ACLU Says (2003), https://www.aclu.org/press-releases/california-privacy-act-key-victory-ongoing-financial-privacy-battle-aclu-says.

499. *Testimony and Statement for the Record of Marc Rotenberg, Director, Electronic Privacy Information Center, on Communications Privacy before the Subcommittee on Courts and Intellectual Property*, Electronic Privacy Information Center (1998), https://archive.epic.org/privacy/internet/rotenberg-testimony-398.html (last visited May 10, 2024) (discussing Franken bill); California Financial Information Privacy Act, S. 1 (2003); Press Release, ACLU, California Privacy Act a Key Victory in Ongoing Financial Privacy Battle, ACLU Says (2003), https://www.aclu.org/press-releases/california-privacy-act-key-victory-ongoing-financial-privacy-battle-aclu-says.

country[500] and submitted a report to the United States Congress sounding the alarm and arguing for much stricter curbs on information collection. But in 2022, former FTC Chairman Leibowitz "observed with dismay that in the years since that report, 'surveillance capitalism has only gotten worse,' yet 'legislation has languished.'"[501]

Policymakers just have been unwilling to really wade in and address the core issues of surveillance capitalism. As Ralph Nader explained, "this is what we've got to get over, that it's when government does nothing that so much bad happens, not just when government does some things that are wrong."[502] In a nutshell, as Zuboff has said, "surveillance capitalism is what happened when U.S. democracy stood down."[503]

Much bolder action on privacy is essential to prohibit certain information collection outright and prevent information from being used for certain purposes, thus addressing how the surveillance economy is affecting people, movements for justice, and democracy. If policymakers are concerned about everything from how online activity affects mental health, to the rise of misinformation, to the growth of AI and its implications on racial justice, economic justice, gender, sexuality, and reproductive justice, and more, then passing robust privacy laws that get at the core of surveillance capitalism is the critical intervention.[504]

There is no shortage of actual policy steps to take, with some considerable consensus on the privacy community side of the ledger. The Electronic Frontier Foundation has called out the need for policymakers to prohibit online behavioral advertisements.[505] Zuboff has said we need to interrupt and even outlaw "behavioral futures markets"[506] and Turow has said lawmakers

500. Press Release, FTC, FTC Issues Final Commission Report on Protecting Consumer Privacy (Mar. 2012), https://www.ftc.gov/news-events/news/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.

501. Shoshana Zuboff, *Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization*, 3 ORGANIZATION THEORY, 17 (2022), https://doi.org/10.1177/26317877221129290 (citing Leibovitz).

502. *Ralph Nader Reflects On His Auto Safety Campaign, 55 Years Later*, SCI. FRIDAY (Dec. 3, 2021), https://www.sciencefriday.com/segments/ralph-nader-auto-safety/.

503. Shoshana Zuboff, *Surveillance Capitalism or Democracy? The Death Match of Institutional Orders and the Politics of Knowledge in Our Information Civilization*, 3 ORGANIZATION THEORY, 1 (2022), https://doi.org/10.1177/26317877221129290.

504. *See, e.g.*, Corynne McSherry, Mario Trujillo, Cindy Cohn & Thorin Klosowski, *Privacy First: A Better Way to Address Online Harms*, EFF (Nov. 14, 2023), https://www.eff.org/wp/privacy-first-better-way-address-online-harms.

505. *Id.*

506. Robert Hackett, *Advertising Markets—Just Like the Trade of 'Organs, Babies, or Slaves'*, FORTUNE (2019), https://fortune.com/2019/11/18/google-facebook-online-advertising-ban-surveillance-capitalism/.

should "ban[] information-driven advertisements" and the sale of data about individuals for marketing use.[507]

There need to be baseline consumer privacy laws that prohibit the collection of personal information and severely limit how it can be used. Policymakers also need to properly address the scourge of data brokers. Laws like the California Delete Act, that provide a one stop shop for people to delete information from all data brokers, are an important first step to give some control.[508] But policymakers need to consider legislation that prohibits the actual privacy invasion—limiting what information can be initially collected by data brokers and how it can be used, as well as other ways that the data broker industry could be even more limited.

Where there is continued information collection, there needs to be true data minimization—companies should only be able to collect and use information as strictly necessary (with the definition of what is necessary not in the hands of the companies) to provide the service that is asked for and not use it for any other purposes.[509] People must also have the ability to access any of their information, move it somewhere else, correct it, and delete it. Laws need to prohibit companies from using "dark patterns"[510] and other means to undermine privacy controls. Laws must also clearly prohibit companies from trying to implement pay-for-privacy schemes that make privacy a luxury for those who can afford it, rather than an inalienable right for all.[511]

---

507. Joseph Turow, Yphtach Lelkes, Nora Draper & Ari E. Waldman, *Americans Can't Consent to Companies' Use of Their Data*, U. PA. ANNENBERG SCH. FOR COMMC'NS 19 (2023), https://perma.cc/J3ZR-RBG6.

508. CAL. CIV. CODE § 1798.99.86 (2), https://legiscan.com/CA/text/SB362/id/2845350.

509. EPIC also discusses the need for data minimization. Electronic Privacy Information Center, RELEASE: Report: State Laws are Failing to Protect Privacy (2024), https://epic.org/release-report-state-laws-are-failing-to-protect-privacy/; EFF does too. Corynne McSherry, Mario Trujillo, Cindy Cohn & Thorin Klosowski, *Privacy First: A Better Way to Address Online Harms*, EFF (Nov. 14, 2023), https://www.eff.org/wp/privacy-first-better-way-address-online-harms.

510. Sara Morrison, *Dark Patterns, the Tricks Websites Use to Make You Say Yes, Explained*, VOX (Apr. 1, 2021), https://www.vox.com/recode/22351108/dark-patterns-ui-web-design-privacy.

511. A significant concern of the ACLU in California and the organization's opposition to Proposition 24 in 2020 was that it did not properly protect privacy as an inalienable right for the most vulnerable Californians. "Black and immigrant communities need strong privacy rights to protect themselves from corporate discrimination as well as state violence. But Prop 24 threatens to make privacy a luxury available only for the most privileged Californians. By forcing Californians to opt-out and potentially pay for their privacy, it places the burden of privacy on the individual, a load those in working families and marginalized communities cannot bear." Jacob Snow & Chris Conley, *Californians Should Vote No on Prop 24*, ACLU OF N. CAL. (Oct. 16, 2020), https://www.aclunc.org/blog/californians-should-vote-no-prop-24.

Policymakers need to introduce and support thoughtful and robust bills that really address the surveillance ecosystem and its impact on marginalized communities. Policymakers must push proposals that actually prevent privacy invasions to a vote and create the public record to move these necessary privacy protections forward.

7. Policymakers Need to Ensure People Can Pursue and Obtain Privacy With Broad Definitional Scope and Robust Enforcement

Policymakers also need to craft and enact laws work that work in practice for people to actually obtain privacy. Any privacy law is only as strong as its beginning (its definitional scope) and its end (its enforcement mechanisms). Policymakers need to ensure that definitions cover the full scope of personal information and that there are robust, efficient, and effective public and private enforcement mechanisms.

a) Importance of definitional scope

In terms of a privacy law's definitional scope, Dan Solove has recently written about the trendiness of including "sensitive data" categories in privacy law.[512] Solove eschews this distinction, contending that "personal data is akin to a grand tapestry, with different types of data interwoven to a degree that makes it impossible to separate out the strands." That with big data and algorithms, information not deemed sensitive in the law can give rise to inferences related to information that is characterized as sensitive and it can also be used in ways that cause harm, as much, if not more than information deemed sensitive. I agree that "sensitive information" is a "sinking ship" because it has no solid principle, and it is disconnected from the way that modern technology works and impacts people.[513] But additionally, "sensitive information" is also a very bad route because it is inconsistent with the California constitutional right to privacy, which broadly protects "personal information."

Any California privacy law that cuts the corners of protections, with either narrower terms like "PII" or creates bifurcated definitions that elevate only some types of personal information for privacy protection, can do damage to the overall comprehensive, inalienable right to privacy. This is not strategic for the long term, big picture fight for strong privacy rights. I have been steadfast in ensuring that privacy laws I have spearheaded protect personal information

512. Daniel J. Solove, *Data Is What Data Does: Regulating Based on Harm and Risk Instead of Sensitive Data*, 118 N.W. L. REV. 1081, 1081 (2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4322198.

513. *Id.* At 1136.

writ broadly and to craft the legislative language in a thoughtful way to address potential risks and harms. For example, the definition of "personal information" in the California Reader Privacy Act includes "any information that identifies, relates to, describes, or is associated with a particular user. . . ."[514] CalECPA's covered information includes all electronic communication information, including IP address and metadata.[515]

The definitional scope of policy interventions should protect all "personal information" broadly defined. To be a real privacy law, the legislative language must do more than protect narrow versions of "PII" that are pushed by the technology industry or perpetuate bifurcated versions of "sensitive information" or other constructs that slivers information about us into what is protected and what is not protected.

b) Importance of strong enforcement

The enforcement mechanism in any privacy law is equally critical. A law that cannot be enforced in practice is really just worthless paper. Policymakers must ensure that privacy laws have robust enforcement mechanisms, both public and private.

A privacy law should provide for government entities like an agency, attorney general, or city attorney to be to take action to enforce all provisions of the law. But it is important to recognize that government enforcers have limited bandwidth and sometimes-conflicting internal interests related to government surveillance and consumer privacy. Policymakers must also ensure that there is a private right of action so that regular people can go to court, both to seek redress for violations that have occurred, and to incentivize entities to follow the law in the first place.

It is also important to articulate that any violation of a provision of the law constitutes an injury in fact and provides standing for a person to be able to go to court. The law should provide for statutory fines and penalties as well as real damages and reasonable attorney's fees. Further, it should clearly articulate in the language of the law and the legislative history that a violation of any provision in the law triggers the full enforcement mechanism and a defendant cannot try to claim that some provisions are procedural and not subject to the same accountability processes. Too often, privacy laws are made completely unusable because the covered entities just do not comply with certain

514. CAL. CIV. CODE § 1798.90 (b)(5), https://law.justia.com/codes/california/2011/civ/division-3/1798.90-1798.90.05/1798.90/.

515. CAL. PEN. CODE § 1546 (d), https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=PEN&division=&title=12.&part=2.&chapter=3.6.&article.

requirements of the law, and the enforcement provision is not scoped to cover this violation, or the legislative history is not robust enough to clearly support the proper privacy-protective interpretation.[516]

California statutory law has a long history of robust public and private enforcement provisions, including civil fines and even misdemeanor penalties, to ensure that privacy laws are followed, and privacy rights are properly protected. As a foundational matter, to challenge government actions, California has provisions for taxpayer standing, with liberal rules that allow any California taxpayer to initiate an action to stop government conduct related to illegal expenditure, waste of, or injury to, the estate, funds, or other property of a county, town, city or city and county. The taxpayer does not need a special, personal interest in the outcome of the case to have standing to sue.[517] Taxpayer standing has been used in many government surveillance cases, including *White v. Davis*.[518] For business actions, the general provisions of the California Uniform Commercial Code confer standing for both public and private parties to sue for unfair competition.[519]

Further, many privacy laws have additional, standalone enforcement provisions. The Information Practices Act provides for both public enforcement as well as a private right of action for an individual to bring a civil suit for failing to comply with specific provisions and any other provision, or any rule promulgated thereunder, in "such a way as to have an adverse effect

516. The California Shine the Light law is an example of a law where covered entities just fail to comply with core requirements like publicly posting where to send Shine the Light requests, and the law could not be effectively enforced to address these violations, and just could not be used by people; *see* Nicole Ozer & Matt Cagle, *Losing the Spotlight: A Study of California's Shine the Light Law* 9–10, ACLU OF N. CAL. (2013), https://www.aclunc.org/sites/default/files/Losing%20the%20Spotlight%20-%20A%20Study%20of%20California%27s%20Shine%20the%20Light%20Law%20final.pdf.

517. CAL. CODE CIV. PROC. § 526a authorizes actions to stop "any illegal expenditure of, waste of, or injury to, the estate, funds, or other property of a county, town, city or city and county." The California Supreme Court held that taxpayers do not need a "special, personal interest in the outcome" of the case to have standing to sue. *Id.*; *see also* Connerly v. State Personnel Board, 92 Cal. App. 4th 16 (2001). "If an action meets the requirements of section 526a, it presents a true case or controversy." Blair v. Pitchess, 5 Cal. 3d 258, 269 (1971). Taxpayer standing has been used in numerous Article I, Section 1 cases including *White v. Davis*.

518. White v. Davis, 13 Cal. 3d 757, 762 (1975) ("Plaintiff Hayden White, a professor of history at the University of California at Los Angeles and a resident taxpayer of the City of Los Angeles, instituted this taxpayer's suit against defendant Edward M. Davis, Chief of Police of the City of Los Angeles, seeking to enjoin the alleged illegal expenditure of public funds in connection with the police department's conduct of covert intelligence gathering activities at UCLA").

519. CAL. BUS. & PROF. CODE §§ 17200–17210, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?sectionNum=17200.&lawCode=BPC.

on an individual."[520] The private right of action provides for both injunctive relief, actual damages, including damages for "mental suffering," and reasonable attorney's fees and other litigation costs reasonably incurred in any suit under this section in which the complainant has prevailed (or partially prevailed).[521] There are also additional monetary penalties and potential jail time for any person who requests or obtains any record containing personal information under false pretenses.[522] The penalty for intentional disclosure of medical, psychiatric, or psychological information in violation of the law and not otherwise required or permitted by law and that results in economic loss or personal injury to the individual is also punishable as a misdemeanor.[523]

The Song Beverly Credit Card Act, which protects the privacy of information in conjunction with a credit card purchase, provides for both public enforcement and a private right of action for both injunctive relief and a civil penalty of up to two hundred and fifty dollars ($250) for the first violation and one thousand dollars ($1,000) for each subsequent violation.[524] The privacy law prohibiting the remote reading or skimming of identification documents includes both a civil and criminal remedy, with a fine of up to fifteen hundred dollars ($1,500) and imprisonment in a county jail for up to one year. It also specifically sets forth that these penalties are independent of, and do not supersede, any other penalties provided by state law, and in the case of any conflict, the greater penalties shall apply.[525]

CalECPA also provides for a variety of both public and private enforcement mechanisms. Any individual whose information is targeted by a warrant, order, or other legal process that is inconsistent with the law, or a service provider, may petition to void or modify the warrant, order, or other legal process or order the destruction of any information obtained in violation of the law. The law provides for a suppression remedy for any violations, permitting any person in a trial, hearing or proceeding to move to suppress any electronic information obtained or retained in violation of the law. Additionally, the Attorney General may also commence a civil action to compel any government entity to comply with the provisions of this chapter.[526]

---

520. CAL. CIV. CODE § 1798.45.

521. CAL. CIV. CODE § 1798.46.

522. CAL. CIV. CODE § 1798.56.

523. CAL. CIV. CODE § 1798.57.

524. CAL. CIV. CODE § 1747.08, https://codes.findlaw.com/ca/civil-code/civ-sect-1747-08/.

525. CAL CIV. CODE §§ 1798.79–1798.795, https://law.justia.com/codes/california/2010/civ/1798.79-1798.795.html.

526. CAL. PEN. CODE § 1546.4, https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PEN&sectionNum=1546.4.

Finally, the Reader Privacy Act includes both evidence suppression remedies and provides for both public enforcement and a private right of action with civil penalties. No evidence obtained in violation of the Reader Privacy Act is admissible in any civil or administrative hearing. A provider that knowingly provides personal information about a person in violation of the Reader Privacy Act is also subject to a civil penalty of up to five hundred dollars ($500) for each violation, which shall be paid to the person in a civil action, or may be assessed and recovered in a civil action brought by the Attorney General, by any district attorney or city attorney, or by a city prosecutor in any court of competent jurisdiction.

Strong public and private enforcement provisions in privacy laws, with statutory fines, is critical. There are also other important enforcement remedies that can be included in privacy laws, including destruction of ill-gotten information. Recently, the FTC has utilized deletion and disgorgement in several of its consumer privacy settlements. When the FTC settled its action against Everalbum for deceiving consumers about its use of facial recognition technology and its retention of the photos and videos of users who deactivated their accounts,[527] the company was forced to delete the ill-gotten information and the algorithm trained on that information.[528] More recently, in the Rite Aid FTC settlement, the company was prohibited from using facial recognition technology for surveillance purposes for five years. It was also required to delete (and direct third parties to delete) any images or photos they collected because of Rite Aid's facial recognition system, as well as any algorithms or other products that were developed using those images and photos.[529]

Finally, when developing robust privacy laws, policymakers should ensure that there are resources for state and federal agencies to cut through the complexities and promulgate regulations and processes that will protect people. Whether on the state or federal level, agencies can be an important component of the legal regime to protect rights in the modern digital age. I have always envisioned an agency akin to the Food and Drug Administration (FDA) or some combination of the FDA and the Consumer Product Safety

527. Case Study, ACLU of Northern California, Never Again, Ever Album (2020), https://www.itsgoodfor.biz/case-study/never-again-everalbum.

528. Press Release, FTC, FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology (May 7, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/05/ftc-finalizes-settlement-photo-app-developer-related-misuse-facial-recognition-technology.

529. Press Release, FTC, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards (Dec. 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.

Commission,[530] charged with protecting rights in the technology context. It would be an agency that can wade through the complexities, help equalize the massive information asymmetries, and be responsible for making decisions in a situation where people can never know what they would need to know. It would create structures that proactively protect the public from harm.[531] This is not a new idea. Clair George Maple, the Director of the Computation Center at Iowa State University, called for an independent regulatory agency whose function would be to "protect and defend the privacy rights of individual citizens" way back in 1970.[532] But ideas about an agency do finally seem to be picking up more steam with the development of the California Privacy Protection Agency,[533] the introduction of a 2021 bill to create a Federal Data Protection Agency with a Civil Rights Office to "regulate high-risk data practices and the collection, processing, and sharing of personal data,"[534] and substantial conversations about AI and the role of an agency in addressing its potential impacts.[535]

Despite the fact that we are still faced with so many privacy issues related to government and business that were already recognized in the 1970s, which should have been addressed by the development and proper enforcement of robust privacy laws many decades ago, it is critical to push forward. As Alan Reitman, the ACLU Associate Director concluded in a 1971 address, "do not

530. *Consumer Product Safety Commission (CPSC)*, USA.GOV, https://www.usa.gov/agencies/consumer-product-safety-commission (last visited May 10, 2024).

531. Anita Allen discussed the idea and legislative efforts underway for a Federal Data Protection Agency in her 2021 article *Black Opticon": Privacy, Race, Equity, and Online Data-Protection Reform.* Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race, Equity, and Online Data-Protection Reform*, 131 YALE L.J. (Feb. 20, 2022), https://www.yalelawjournal.org/forum/dismantling-the-black-opticon. Dan Solove also discussed this idea of an agency in his 2024 paper, *Murky Consent*, and that "other regulatory areas can lend helpful ideas," such as the Food and Drug Administration and The National Highway Traffic Safety Administration. Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 638 (Jan. 23, 2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4333743.

532. Clair G. Maple, The Privacy Problem, 13. American Civil Liberties Union Records MC#001 Box 1097 Folder 12 Invasion of Privacy by Technological Means Date(s): 1970.Clair George Maple was a professor of computer science at the Iowa State University and served as Director of ISU's Computation Center from 1963 until his death in 1985. https://findingaids.lib.iastate.edu/spcl/arch/rgrp/6-2-12.html.

533. *California Privacy Protection Agency*, CAL. PRIV. PROTECTION AGENCY, https://cppa.ca.gov/ (last visited May 10, 2024).

534. Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race, Equity, and Online Data-Protection Reform*, 131 YALE L.J. (Nov. 16, 2021), https://www.yalelawjournal.org/forum/dismantling-the-black-opticon.

535. AI Now Institute, *What Can We Learn From the FDA Model for AI Regulation?* (Jan. 31, 2024), https://ainowinstitute.org/publication/what-can-we-learn-from-the-fda-model-for-ai-regulation.

lose heart when the odds seem insurmountable. Liberty—privacy—the right to be let alone is indeed a precious right. And anything precious is well worth fighting for."[536] Similarly, as Senator Sam Ervin said in 1971, "[i]f Americans can harness computers to get to the moon, surely we can harness them to protect our liberty."[537] Or in the inimitable words of both the *Isley Brothers* in 1975 and *Public Enemy* in 1989, "Fight the Power."[538]

V. CONCLUSION

While the arc of history is long and it bends toward justice, history also repeats itself when we do not take lessons from the past and learn to do better. Like in the 1970s, we are again in a time of rapid technological change and amidst critical fights for justice. Decisions made today in the courts, legislatures, companies, and communities will determine whether we can finally build a world where technology supports access, equity, and justice in the digital age. Otherwise, technology will continue to be used by the government and big business to prop up oppressive systems—from invasive surveillance tech that fuels racist systems of policing, mass incarceration, and immigration, to biased algorithms and inhumane business models that prioritize profit over people's lives, health, and safety. Now is the time to ensure that the Golden State Sword of the California constitutional right to privacy, a modern, inalienable right to privacy forged from movements for intersectional justice and passed to protect our fundamental rights in the modern digital age, rises to the challenge of the times and works for the people.

The fiftieth year of the California constitutional right to privacy and the Berkeley Technology Law Journal symposium have been an important moment to reflect and fully consider what the California constitutional privacy was intended to be and how it can and must now do more to promote intersectional justice in the digital age. We are fortunate that so many committed lawyers, political leaders, and activists came together more than fifty years ago to make the California constitutional right to privacy a legal reality. Now we must rededicate ourselves to also making it a lived reality and

536. Alan Reitman, Address on Privacy and Civil Liberties at Oregon State College of Education (Feb. 16, 1971), American Civil Liberties Union Records MC#001 Box 1092 Folder 5 Reitman, Alan: Speech on privacy issues. Date(s) 1971.

537. *Federal Data Banks, Computers, and the Bill of Rights, February 23, 1971*, HATHITRUST at 6, https://babel.hathitrust.org/cgi/pt?id=uc1.c051765460&view=1up&seq=19&q1=aclu (last visited May 3, 2024).

538. *'Fight The Power': A Tale Of 2 Anthems (With The Same Name)*, NPR (Dec. 7, 2018), https://www.npr.org/2018/12/07/673845242/fight-the-power-american-anthem-public-enemy-isley-brothers.

using the Golden State Sword to its full effect to truly power social justice in the modern digital age.