



August 2019

Centering Civil Rights in the Privacy Debate

Becky Chao, Eric Null, Brandi Collins-Dexter, & Claire Park

Acknowledgments

The authors would like to thank Francella Ochillo, Erin Shields, Alisa Valentin, Miranda Bogen, Priscilla González, and Gaurav Laroia for participating in the event highlighted in this report and Lisa Johnson, Austin Adams, and Maria Elkin for communications support. Open Technology Institute would also like to thank Craig Newmark Philanthropies for generously supporting its work in this area.

About the Author(s)

Becky Chao is a policy analyst at New America's Open Technology Institute, where she works to promote equitable access to a fair and open internet ecosystem.

Eric Null is senior policy counsel at the Open Technology Institute, focusing on internet openness and affordability issues, including network neutrality, Lifeline, and privacy.

Brandi Collins-Dexter is the senior campaign director at Color Of Change and oversees the media, democracy and economic justice departments.

Claire Park was an intern at New America's Open Technology Institute, where she researched and wrote about technology policy issues including broadband access and competition, as well as privacy.

About New America

We are dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Open Technology Institute

OTI works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators.

Contents

Executive Summary	5
Introduction	7
Privacy is a Civil Right	8
For Marginalized Communities, the Stakes are High	11
Data Practices Can Facilitate Employment Discrimination	12
Data Practices Can Facilitate Housing Discrimination	13
Data Practices Facilitate Increased Surveillance of Marginalized Communities, Especially Communities of Color	14
Exploitation of Personal Data Perpetuates Socioeconomic Inequity	16
Protecting Personal Data Protects Personal Safety	17
There are Avenues for Change	18
Government Agencies Can Protect Civil Rights	18
Federal and State Legislation Can Protect Civil Rights	19
The Privacy Debate Needs Diverse Voices	20
Conclusion	21

Executive Summary

In our increasingly digitized world, it is critical to protect individuals' privacy. As policymakers consider passing meaningful privacy legislation, civil rights protections are a critical but mostly overlooked component. To have effective privacy legislation, we must ensure that companies' data practices do not violate individuals' civil rights—especially when it comes to marginalized communities. Problematic commercial data practices disproportionately harm people of color—especially Black and Brown communities—women, immigrants, religious minorities, members of the LGBTQ+ community, low-income individuals, and other marginalized communities. Centering these communities in this work helps us understand exactly how high the stakes are and underscores the need for solutions that directly mitigate these harms. Without civil rights protections adapted for the twenty-first century, the discriminatory data practices adopted by online companies will continue to have long-lasting, severe consequences.

Commercial data practices enable myriad forms of abuse. They facilitate voter suppression, digital redlining, discriminatory policing, retail discrimination, digital inequity, the amplification of white supremacy, identity theft, the endangerment of personal safety, and more. Experts have long known that data practices can lead to discriminatory outcomes in access to housing, jobs, and other critical aspects of our livelihood, yet these practices remain in place.

Data is used for discriminatory purposes, with even innocuous data points becoming proxies for protected classes. Policymakers cannot ignore these tangible bad outcomes. The stakes are particularly high for marginalized communities in five areas: employment discrimination, housing discrimination, disproportionate surveillance, socioeconomic inequality, and personal safety.

To ensure justice and equity, and to curtail these extensive harms, individuals need multiple avenues of redress when their privacy and civil rights are violated. The Department of Justice and the Department of Housing and Urban Development are already empowered to enforce existing civil rights statutes, and individuals' privacy and civil rights would be better protected if the Federal Trade Commission, too, were empowered with rulemaking authority. Additionally, Congress must ensure that privacy laws include strong civil rights protections and preserve the ability of states to play a vital role in protecting civil rights and consumer privacy. Further, to ensure that the debate on privacy centers perspectives from marginalized communities, the tech policy community needs to reflect the country's diversity. Including more voices in the policy debate leads to better policy solutions.

Civil rights protections must apply to the digital economy. Though we have a number of federal civil rights statutes that exist to protect individuals from unjust treatment by various institutions, these laws are insufficient for protecting

against the discriminatory practices that have expanded into the digital realm. As the fight for civil rights grapples with the harms posed by data and technology, these new developments are also making it increasingly challenging to enforce civil rights laws. Further guidance and broader policy changes are needed to resolve the ambiguities around applying civil rights laws to these novel means of discrimination.

Introduction

For the first time since the Children’s Online Privacy Protection Act in 1998, U.S. policymakers are having serious discussions about passing meaningful legislation to protect consumer privacy. Renewed congressional focus comes in the aftermath of multiple high-profile data breaches and privacy scandals, unexpected backlash when Congress overturned the broadband privacy rules implemented by the Federal Communications Commission,¹ and the European Union’s General Data Protection Regulation going into effect. While the debate is long overdue, it has focused myopically on requiring transparency and consent for certain data practices and whether federal legislation should preempt state laws like the California Consumer Privacy Act. Too little of the conversation has been dedicated to ensuring that companies do not violate individuals’ civil rights through their data practices. In this formative stage, it is vital to center civil rights issues in the privacy legislation debate. Otherwise, we will miss a golden opportunity to protect against data practices that lead to civil rights harms.

This report builds on an event hosted on May 9, 2019 by Color of Change and New America’s Open Technology Institute that explored how to protect civil rights through better privacy protections.² Francella Ochillo, then vice president and general counsel of the National Hispanic Media Coalition (NHMC), delivered opening remarks. A subsequent panel, moderated by Color of Change’s senior campaign director Brandi Collins-Dexter, brought together Erin Shields, national field organizer for internet rights at MediaJustice;³ Alisa Valentin, then communications justice fellow at Public Knowledge; Miranda Bogen, senior policy analyst at Upturn; Priscilla González, campaign director at Mijente; and Gaurav Laroia, policy counsel at Free Press. The panel discussed key questions regarding privacy, digital rights, and civil rights, including: what role does technology play in our society?; how are marginalized communities disproportionately harmed by data practices and privacy infringements?; and what are some of the ongoing efforts and interventions to address these concerns?

Privacy is a Civil Right

“Privacy is not just transactional. Privacy is a civil right,” Valentin stated on the panel.⁴ Historically, the concept of the right to privacy in the United States has been shaped by Louis Brandeis, who first articulated privacy in 1890 as “the right to be let alone.”⁵ Later, as a Supreme Court Justice, he explained how the principles of the Fourth Amendment include protection of privacy against the state, enabling all citizens to conceal their unexpressed beliefs, political dissent, thoughts, and emotions from government surveillance.⁶ Justice Brandeis saw anonymity as a precondition for freedom of thought.⁷ In today’s networked world, we continue to struggle with balancing the right to dissent, organize, and speak truth to power with the right to feel safe and protected, and to experience digital sanctuary. The right to privacy should include ensuring freedom from the predatory business practices that replicate outlawed models of discrimination.

Privacy should mean personal autonomy and agency, but commercial data practices increasingly impede the autonomy and agency of individuals who belong to marginalized communities.⁸ Black people, women, LGBTQ+ individuals, persons with disabilities, and immigrants and refugees have long fought for civil rights protections in the brick-and-mortar economy. Discriminatory practices have expanded into the online world, but enforcement against that inequity has been insufficient. Data is used for discriminatory purposes, with even innocuous data points becoming proxies for protected classes, and policymakers cannot ignore these tangible bad outcomes. Ultimately, everyone deserves the “right to determine what information is collected on you, how it’s stored, and what it’s used for,” as Shields argued. Our laws should be updated to recognize and address discrimination brought about through harmful commercial data and surveillance practices.⁹

Ultimately, everyone deserves the “right to determine what information is collected on you, how it’s stored, and what it’s used for.”

A number of federal civil rights statutes currently exist to protect individuals from unjust treatment by various institutions.¹⁰ These statutes prohibit different types of discrimination, are applied under different circumstances, and are intended to safeguard specific classes of individuals with legally protected

characteristics.¹¹ For instance, Title VII of the Civil Rights Act of 1964 prohibits discrimination in employment on the basis of race, color, religion, national origin, or sex, and Title II of the act bars discrimination on the basis of race, color, religion, or national origin in public accommodations.¹² The Fair Housing Act, enacted in 1968, prohibits discrimination in the sale or rental of housing on the basis of race, color, religion, national origin, sex, disability, or familial status.¹³ The Equal Credit Opportunity Act, enacted in 1974, prohibits discrimination against credit applicants on the basis of race, color, religion, national origin, sex, marital status, age, or source of income.¹⁴

These laws have been instrumental in addressing some of the injustices faced by marginalized communities in the United States, especially Black communities. As Ochillo explained in her opening remarks:

Landmark legislation of the civil rights movement that was passed in the 1960s was built on a movement of resistance and sacrifice that lasted for centuries since the first group of slaves arrived on American shores. Hundreds of years later, after people of all races were confronted with the brutality and leftover horrors of oppression, Congress passed civil rights laws to ensure that everyone had the right to be free from certain types of discrimination, ensuring that every American has the right to fair and equal treatment.

But the struggle to enforce these laws continues to this day, and data practices have enabled historical forms of oppression and discrimination to carry over into the digital realm with offline consequences. As Shields noted, “Like a virus, discriminations from before have mutated.”¹⁵ Commercial data practices enable, among other things, voter suppression, digital redlining, discriminatory policing, retail discrimination, digital inequity, the amplification of white supremacy, identify theft, and the endangerment of personal safety.¹⁶ By collecting and using data, companies can leverage new data and surveillance tools that enable racial profiling and discrimination.¹⁷ Further, automating decision-making using data and predictive tools can discriminate against marginalized communities¹⁸ and exacerbate hidden biases in data.¹⁹ Experts have long known that data practices can lead to discriminatory outcomes in access to housing, jobs, and more. Therefore, as Shields stated, protecting privacy is essential to “shift[ing] power imbalances in a mostly unregulated data space.”

Civil rights protections must also apply to the digital economy. As Ochillo elaborated,

When [civil rights] laws were codified, no one imagined a scenario where tech platforms would be able to discriminate online in ways that legislation intended to prevent in our neighborhoods. Today, my data

profile can determine whether I will have access to certain types of employment or housing opportunities, or whether I will be excluded. It will have an impact on how much I make or pay for a mortgage. And the profiles that companies create about me behind closed doors will live online indefinitely and remain difficult for me to change. That is why we need privacy laws that acknowledge enduring economic, political, and cultural consequences of discrimination that still exists in our country today.²⁰

Without incorporating civil rights protections into privacy legislation, the situation Ochillo described is unlikely to change.

Companies should be prohibited from using individuals' personal data to discriminate against members of marginalized communities. Many civil society organizations, including Color of Change and New America's Open Technology Institute, have called upon Congress to protect civil rights, equity, and equal opportunity in the digital ecosystem.²¹ In April 2019, 26 civil society organizations sent a letter to Congress on the need for federal privacy legislation to address the discriminatory effects of commercial data practices, arguing that "personal data are the raw materials that fuel discrimination. ... For too long, corporations have ignored the digital pollution that their commercial data practices generate; they must be held accountable for the negative externalities of their business models."

²² Privacy legislation must address these harms.

For Marginalized Communities, the Stakes are High

The idea of privacy as it is often discussed and understood has little value when it excludes certain communities. For hundreds of years, many people in the United States have not been granted true anonymity and autonomy.²³ Lantern laws in the eighteenth century dictated that Black, mixed-race, and Indigenous enslaved people had to carry candle lanterns with them after sunset.²⁴ Many enslaved people were tracked and documented meticulously, and slave branding was used as a precursor to modern biometric ID.²⁵

Today, many people still lack true anonymity and autonomy. Most public transportation is equipped with surveillance devices,²⁶ and individuals have to give up a certain amount of data to participate in social safety net programs.²⁷ While these trends impact more white people in terms of sheer numbers, Black and Indigenous people are disproportionately impacted per capita.²⁸ In any number of ways, details about your life that may seem innocuous become a handful of carefully chosen factors that can determine whether you are more likely to be surveilled by government or corporations—details like whether you use an Android phone or iPhone, attend public or private school, are incarcerated or in contact with a loved one who is incarcerated, or live in a neighborhood where the police are overly present. These details are also factors that are inextricably and tacitly linked to race, class, and cultural identity.

While these trends impact more white people in terms of sheer numbers, Black and Indigenous people are disproportionately impacted per capita.

Without bright-line, twenty-first century civil rights protections, the discriminatory data practices adopted by online companies will continue to have long-lasting, severe consequences. They disproportionately harm people of color—especially Black and Brown communities—women, immigrants, religious minorities, members of the LGBTQ+ community, low-income individuals, and other marginalized communities. Centering these communities in this work helps us understand exactly how high the stakes are, and underscores the need for solutions that directly mitigate these harms.

Our panel discussion covered five particular areas that exemplified the high stakes: employment discrimination, housing discrimination, increased surveillance, socioeconomic inequalities, and personal safety.

Data Practices Can Facilitate Employment Discrimination

Companies can use data in ways that facilitate gender- and race-based employment discrimination.³² Many hiring processes have moved online; not only do companies list ads for job openings online, but humans or computers (through algorithms built and programmed by humans) increasingly decide who sees the openings.³³ Algorithms may also screen job applicants' resumes, analyze job interviews, and more.³⁴ Employers are now trying to leverage new hiring tools with the stated goals of creating more efficiencies and improved personalization, such as reducing the cost per hire and optimizing the quality of hire.³⁵ However, is "personalization" actually just "discrimination," as Bogen argued? As companies attempt to maximize efficiency and personalization in the hiring process, it may be that they are actually just discriminating against people of color, women, and other underrepresented groups.

Advertising platforms, for instance, can enable employment discrimination by choosing who sees particular job ads, which has serious implications for job opportunity. When recruiters advertise positions, they often pay for digital advertising on large online platforms to maximize their reach and effectiveness.³⁶ These platforms in turn leverage the troves of user data they have amassed and give employers the ability to dictate audience parameters to target ad delivery. Facebook, for instance, used to allow targeting based on demographic data, and still allows targeting based on categories that may be highly correlated with race and other protected classes, such as inferred interests.³⁷ Though the employers set initial targeting parameters, the ad platforms may ultimately determine who within a target audience sees an ad based on their own prediction of how likely a user is to engage with the ad or apply for the position.³⁸

Online employment ads have been delivered in discriminatory ways. Numerous studies have established that Facebook's ad delivery algorithm has discriminated based on race and gender. In response, the platform has adopted several policies to avoid discrimination for certain types of ads, including eliminating the option to allow age-, gender-, or zip code-based targeting.³⁹ In 2018, *ProPublica* found that Facebook allowed employers to advertise jobs selectively to users of specific genders.⁴⁰ Fifteen employers, including Uber, advertised jobs exclusively to men, and a community health center in Idaho advertised job openings for nurses and medical assistants only to women.⁴¹ Another recent study found that this discrimination persists in job listings even when advertisers do not target specific demographics and are trying to reach a broad audience.⁴² Advertisers can also

still exclude users based on interests that are highly correlated with race by using custom audiences or location.⁴³ As Bogen explained on the panel, “All the data still exists in the infrastructure, they just took away some of the tools [used for explicit discrimination], but those algorithms look at historical information being pushed forward into the future.”⁴⁴

Predictive technologies also discriminate in hiring. Increasingly, predictive technologies that rely on data are used in recruiting, screening, interviewing, and selecting candidates. Without clear transparency and oversight, these technologies can lead to bias, thereby undermining equity in hiring.⁴⁵ In particular, Bogen highlighted that discrimination can occur as recruiters attempt to leverage the power of data toward streamlining candidate screening: “Amazon’s racist hiring AI was saying women were probably not good candidates because they didn’t resemble the candidates that the company had seen in the past. These are tangible outcomes that weren’t in the conversation before that are now becoming more clear.”⁴⁶ These outcomes, according to Bogen, make it obvious that machines, too, can be racist as they are often a reflection of society and can perpetuate and exacerbate biases.⁴⁷ Yet, the public lacks transparency into most of these practices.

Data Practices Can Facilitate Housing Discrimination

Access to housing has been recognized as a basic human right, one that is a necessary condition for other economic, social, and cultural rights. The process for securing housing has moved increasingly online. Whereas, home buyers in the 1980s typically perused newspaper ads to find a home, 44 percent of home buyers in 2016 looked for properties online first.⁴⁸ This process is also vulnerable to discrimination.

Housing discrimination is not new. The Fair Housing Act prohibits certain types of housing discrimination. But online means of housing discrimination have supplemented offline means. Historically, Shields relayed on the panel, marginalized communities have engaged with the legal system to gain rights to material conditions like housing. “As our lives have become increasingly digitized,” she said, “discrimination from before has mutated... [An] example could be racial covenants and redlining in housing. This has mutated into Facebook allowing housing providers to select racial categories of who’s seeing ads for housing.”⁴⁹

Targeting online housing ads is already a civil rights issue. In 2016, *ProPublica* found that Facebook’s platform allowed advertisers to exclude Black, Hispanic, and other groups called “ethnic affinities” from seeing housing ads.⁵⁰ A recent study found that, in the same way that gender- and race-based discrimination persists in job listings, discrimination occurs in the targeting of housing ads even

when advertisers do not opt to target specific demographics.⁵¹ Further, advertisers can still discriminate by selecting audience parameters that are highly correlated with race, such as inferred interests or location.⁵²

Facebook’s platform allowed advertisers to exclude Black, Hispanic, and other groups called “ethnic affinities” from seeing housing ads.

Secondary, nonconsensual data collection on these large platforms can also lead to further housing discrimination, with some companies collecting personal information without clearly disclosing what is being collected and what it might be used for. This secondary use of data, in previous cases, has allowed companies to repurpose user data, without consent, to build tools that make segregation worse. As Laroia explained on the panel, “It is fundamentally immoral that companies are using information about your ordinary life online, and that information is being turned around and used to build tools that facilitate segregation—to fundamentally undo the important rights and progress we’ve made to build a more equitable society.”⁵³ Facebook, for instance, originally collected users’ phone numbers for two-factor authentication, but also used that information to deliver targeted advertising.⁵⁴ Using phone numbers, one can find a wide range of personal information, including names, education and career histories, and locations—all of which can be used as a proxy for facilitating housing discrimination through targeted ad delivery.⁵⁵

Data Practices Facilitate Increased Surveillance of Marginalized Communities, Especially Communities of Color

Digital surveillance disproportionately violates the privacy of those communities already marginalized and unreasonably suspected. The history of surveillance of marginalized communities in the United States dates back to colonial times. As media activist Malkia Cyril said at the 2017 Color of Surveillance conference, “Surveillance technologies have been used to separate the citizen from the slave, to protect the citizen from the slave.”⁵⁶ Records of slaves in plantation ledgers served as proto-biometric databases and, combined with slave passes, slave patrols, and fugitive slave posters, were the precursors to modern policing and tracking.⁵⁷ New technology and commercial data practices have continued this legacy of surveillance with a disparate impact on marginalized communities,

especially immigrants and communities of color. For instance, commercial databases have been accessed by government surveillance programs and law enforcement agencies, without a warrant or probable cause, and were used to target people of color.⁵⁸ Social media data can also be used for racial profiling.⁵⁹

Companies are utilizing commercial data practices that rely on privacy intrusions, leading to increased surveillance. Mijente, which has historically focused on immigrant rights, learned that Immigration and Customs Enforcement (ICE) used Palantir's services to track and detain undocumented immigrants.⁶⁰ ICE built profiles of immigrant children and their family members, logging relatives and guardians who showed up to claim unaccompanied minors in Palantir's investigative case management system.⁶¹ According to González, federal agencies and local law enforcement across the country were able to share surveillance data to locate, detain, and deport immigrants using Palantir's software, thereby circumventing sanctuary policies that prohibit cooperation between ICE and local police in certain cities, and exacerbating the family separation crisis. As González noted, "Immigrants, people of color, vulnerable communities usually serve as laboratories for testing new technologies," as companies leverage new ways of commodifying data, often without regard for civil and human rights.⁶²

There is a history of using personal information to surveil minorities in the United States.⁶³ In the aftermath of the September 11 attacks, the Bush administration enacted the National Security Entry-Exit Registration System (NSEERS) to register non-citizen visa holders, primarily from Muslim-majority countries.⁶⁴ While this system is now defunct, new practices have cropped up that continue to subject members of marginalized communities to undue surveillance. In June 2019, the U.S. State Department began collecting and reviewing all social media accounts and identities of people entering the country.⁶⁵ This practice "only further illustrates the extent to which social media is now being weaponized against immigrant and non-immigrant minority populations."⁶⁶ Individuals' personal data feeds into database screening and watchlists that determine who can work, vote, fly, and more—which in turn can enable discrimination and profiling, bearing significant risks to the civil rights and liberties of marginalized communities.⁶⁷

Data practices also disproportionately harm Black and Brown communities. Shields noted that there have been long-standing movements to acknowledge the discriminatory impact of data with Black- and Brown-led research, noting examples like Our Data Bodies and the Stop LAPD Spying Coalition. Our Data Bodies (ODB) has exposed how conviction and incarceration data on individuals can be used as a barrier to employment, services, and housing, and its disproportionate effect on Black residents.⁶⁸ The Stop LAPD Spying Coalition has publicized surveillance techniques and resources used by the Los Angeles Police Department to discriminate against people of color, including how the

department's use of predictive policing has criminalized spaces in Los Angeles mostly occupied by Brown and Black residents.⁶⁹

Exploitation of Personal Data Perpetuates Socioeconomic Inequity

Discriminatory data practices also perpetuate, and even escalate, socioeconomic inequities. Companies may use information about people in ways that entrench existing wealth disparities, such as using data on bill payments and credit scores to reject requests for bank loans.⁷⁰

Exploitation of data in these ways leads to socioeconomic harm for specific groups of people who have historically been subject to discrimination. Ochillo gave the example of companies using data on customers' income levels and zip codes to "personalize" prices and products for people living in specific neighborhoods. A person living in a wealthier neighborhood may have access to better prices or products than someone living in a poorer neighborhood. As Ochillo said, "Data that is originally collected with good intentions can easily be repurposed to discriminate or over-police in communities of color."⁷¹

Surveillance and violations of privacy also perpetuate digital inequality and the socioeconomic divide. Valentin pointed to Mary Madden's writings on how poor people "experience these two extremes: hypervisibility and invisibility,"⁷² lacking both the agency and resources to challenge undue harms.⁷³ Low-income individuals are subject to greater suspicion and monitoring when applying for government benefits, and live in heavily policed neighborhoods. They can be unfairly targeted by predictive policing tools. At the same time, if low-income individuals are not visible enough online, they can also lose out on education and job opportunities. Low-income communities are also most likely to suffer from surveillance and violations of their privacy and civil liberties, as low-income internet users are significantly less likely than those in high-income households to use privacy settings to limit who can see what they post online (57 percent vs. 67 percent).⁷⁴

"Data that is originally collected with good intentions can easily be repurposed to discriminate or over-police in communities of color."

Protecting Personal Data Protects Personal Safety

The collection and misuse of personal information can cause physical and emotional harm. Data is directly linked to personal safety, especially when that data is used to identify people or determine their location. In particular, data practices can facilitate and locate targets for hate campaigns, physically endangering individuals' lives.

Violent hate groups use online platforms and services to target specific populations. "Data manipulation techniques have been used to...stir hate and division within communities and against religious minorities," Ochillo pointed out. Civil rights groups like Muslim Advocates have called on social media platforms to rein in the amplification of white supremacist hate groups.⁷⁵ By using search engine optimization strategies to exploit "data voids," or search terms that lack robust results, bad actors can "hijack" certain issues and reach potential new audiences.⁷⁶ As this rhetoric spreads online, it can lead to real-life violence, as several incidents have demonstrated. For instance, Robert Bowers, who murdered worshippers at a Pennsylvania synagogue in October 2018, was active on Gab, a Twitter-like platform used by white supremacists.⁷⁷ And a recent study led by New York University found that online hate speech on Twitter predicts real-life racial violence.⁷⁸

In addition, there are significant risks to personal safety associated with the sharing of individuals' location data. *Motherboard* published an extensive report earlier this year on how major telecom companies like AT&T, Sprint, and T-Mobile sold access to their customers' real-time location data to location aggregators, who then resold the data to law enforcement agencies, car salesmen, property managers, bail bondsmen, and bounty hunters.⁷⁹ This data likely included "assisted GPS" data, which is used by first responders to locate 911 callers in emergency situations and can specify a person's location inside a building. The precise location data was allegedly used by two bounty hunters who tracked a man on the run from a first degree drug charge in Minnesota to a car dealership in Texas.⁸⁰ All three men died in the ensuing shootout, which also endangered other customers at the dealership.⁸¹

The civil rights implications of these data and surveillance tactics are many. Such data could be used to track undocumented immigrants and their families. It may be used to identify groups of people or communities and expose their meeting locations, information that could then be used to allow hate crimes and identity-based violence. For instance, Grindr, a popular LGBTQ+ dating app, disclosed the HIV status, GPS location, email addresses, and other profile information from its users to third parties without user consent.⁸² It is paramount, therefore, to protect members of marginalized communities in a way that accounts for the greater risk to their civil rights that privacy violations pose.

There are Avenues for Change

The lack of consumer privacy protections in the United States has given way to myriad harms to marginalized communities. Envisioning privacy as a civil right can help curtail the extensive discriminatory harms discussed above. Yet as the fight for civil rights grapples with the harms posed by data and technology, these new developments are also making it increasingly challenging to enforce civil rights laws.⁸³ To ensure justice and equity, it is crucial that voices from these communities are well represented as we debate policy solutions at government agencies and in federal and state legislation.

Government Agencies Can Protect Civil Rights

Government agencies should protect privacy and civil rights whenever possible. Agencies like the Department of Justice and the Department of Housing and Urban Development (HUD) are empowered to enforce existing civil rights statutes. In March 2019, HUD charged Facebook with housing discrimination, alleging that its targeted advertising platform violated the Fair Housing Act by “encouraging, enabling, and causing” unlawful discrimination by restricting who can view housing ads.⁸⁴ This action came after Facebook settled a series of civil rights lawsuits alleging housing and employment discrimination by the National Fair Housing Alliance and others.⁸⁵

Even agencies that do not have explicit civil rights mandates can help. For instance, the Federal Communications Commission (FCC) has rules protecting the privacy of cell phone users, and the rigorous enforcement of those rules can help protect civil rights. As referenced above, *Motherboard* found that the major wireless carriers were selling customer location data to third parties without requiring proof of lawful orders or customer consent. The FCC could enforce its privacy laws as argued in a recent complaint filed by New America’s Open Technology Institute, Georgetown Law Center on Privacy & Technology, and Free Press, which would provide more privacy protections against potentially discriminatory and dangerous uses of highly sensitive location information of cell phone users.⁸⁶

Nonetheless, further guidance and broader policy changes are needed given the ambiguities around how to apply civil rights laws to these novel means of discrimination. For instance, while the Voting Rights Act prohibits voter suppression by violence or intimidation, it does not prohibit voter suppression by deception, which is typically how voters are disenfranchised online.⁸⁷ We saw this in the 2016 election, where Russian interference efforts deliberately targeted Black Americans using personal information that was weaponized to deceive and disenfranchise voters.⁸⁸

To ensure that privacy enforcement captures these civil rights violations, one possibility is empowering the Federal Trade Commission (FTC) to protect privacy and civil rights with rulemaking authority. The FTC is the primary government agency responsible for protecting privacy, but its current privacy enforcement powers are limited to its authority to protect against deceptive and unfair practices, which does not sufficiently allow the agency to protect privacy.⁸⁹ Instead, the FTC should be empowered with rulemaking capacity that would sufficiently allow it to provide more guidance and regulatory certainty on what privacy laws require from companies as technology and business practices continue to evolve in the digital economy. However, relying exclusively on the FTC to enforce civil rights protections is insufficient, given that the agency is resource-constrained and cannot take every case.⁹⁰ Thus, individuals require additional avenues for recourse through other agencies, states, and courts, too.

Federal and State Legislation Can Protect Civil Rights

Congress must ensure that privacy laws include strong civil rights protections. Free Press and the Lawyers' Committee for Civil Rights Under Law recently published model legislation outlining how Congress can ensure that personal data is not used to discriminate against protected classes in areas like employment, housing, and education.⁹¹ They also propose classifying online businesses as public accommodations. As it stands, "The bar downstairs has more obligations regarding civil rights in general to the public than any online platform does," Laroia said on the panel.⁹² "That varies by state, but there's no federal consensus on that. ... By classifying online businesses as public accommodations, we [would] make it unlawful to process personal information in a manner that segregates, discriminates, or otherwise makes unavailable those goods and services."⁹³

This model legislation would require companies to audit algorithms for privacy risk and robust transparency.⁹⁴ It also gives the FTC the ability to enforce the law.⁹⁵ Lastly, it would give people a private right of action to protect their civil rights. A private right to action is critical because, as Laroia explained, the public cannot rely exclusively on government agencies to protect civil rights, "so it's important that ordinary people and advocates can protect their rights when government agencies are falling down on the job."⁹⁶

States play a vital role in protecting civil rights, and any legislation should preserve that role. For instance, in July 2018, the Washington State attorney general investigated Facebook for unfair and deceptive practices and ultimately agreed to a settlement that required Facebook to alter its advertising platform by removing the option for advertisers to exclude ethnic and religious minorities, immigrants, LGBTQ+ individuals, and other protected groups from seeing their

ads.⁹⁷ State civil rights laws in some cases, including the Washington case, are more protective than federal civil rights laws, making it inappropriate for any federal civil rights law to preempt state civil rights laws or for federal privacy laws to preempt state laws.

The Privacy Debate Needs Diverse Voices

Ultimately, to ensure that the debate on privacy centers perspectives from marginalized communities, the tech policy community needs to reflect the country's diversity. Valentin has written about #TechPolicySoWhite to underscore the importance of diversifying the tech policy space.⁹⁸ Impacted communities—especially Black communities—must be included in discussions about privacy, she said on the panel, particularly because stakeholders define “privacy” differently, depending on the community and cultural background. As Valentin wrote:

If someone is not a person of color, they are likely to lack the experience to find policy solutions that positively impact communities of color. Therefore, I believe it is important to get in the practice of passing the microphone to individuals who can accurately identify the issues and subsequent solutions that will benefit these communities. The same applies to people who attempt to speak on behalf of women, low-income communities, disabled communities, or the LGBTQ community...pass the mic. It is important to recognize that there are gaps in the knowledge of every well-intentioned, non-marginalized ally. Thus, it is important to identify those gaps in one's knowledge, speak with the affected parties to gain more understanding, and subsequently uplift their voices during these important debates.⁹⁹

Laroia echoed that including more voices in the policy debate also leads to better policy solutions:

By genuinely thinking about the most affected communities in the work we do, we're actually able to solve the problems. We think the privacy conversation has moved not just because the downside risks have become more apparent, but because the circle of people who care about these issues is becoming wider, giving the privacy debate a different kind of moral center than it had before.¹⁰⁰

For privacy legislation to fully protect against the wide array of civil rights harms that come about from commercial data practices, we must center the communities most directly affected by those practices.

Conclusion

No legislation can truly be comprehensive or effective at protecting privacy unless it addresses civil rights. Problematic data practices have severe implications for employment discrimination, housing discrimination, increased surveillance, socioeconomic inequities, and personal safety. They are particularly damaging for marginalized communities, with both public and private organizations using data to discriminate based on race, gender and sexual identity, citizenship status, ethnic and religious affiliations, socioeconomic status, health, and disability. Some of this can be observed in the use of technology and data analytics techniques by law enforcement to surveil and target people believed to be higher security risks, which are often racially biased and rest on existing prejudices about certain communities.

There are a variety of avenues for change, discussed above, that can help prevent these harmful civil rights violations arising from problematic data practices. Federal agencies should enforce civil rights and privacy laws. Congress must ensure that privacy laws include strong civil rights protections and preserve the ability of states to play a vital role in protecting civil rights and consumer privacy. All of these avenues for change, however, must center civil rights perspectives.

Notes

- 1 Matthew Yglesias, “Republicans’ rollback of broadband privacy is hideously unpopular,” *Vox*, April 4, 2017, <https://www.vox.com/policy-and-politics/2017/4/4/15167544/broadband-privacy-poll>.
- 2 Francella Ochillo, Gaurav Laroia, Erin Shields, Miranda Bogen, Alisa Valentin, Priscilla Gonzalez, Brandi Collins-Dexter, “Centering Civil Rights in the Privacy Debate,” (Panel, Washington, DC, May 9, 2019), <https://www.newamerica.org/oti/events/centering-civil-rights-privacy-debate/>.
- 3 Formerly known as the Center for Media Justice (CMJ).
- 4 Francella Ochillo, Gaurav Laroia, Erin Shields, Miranda Bogen, Alisa Valentin, Priscilla Gonzalez, Brandi Collins-Dexter, “Centering Civil Rights in the Privacy Debate,” (Panel, Washington, DC, May 9, 2019), <https://www.newamerica.org/oti/events/centering-civil-rights-privacy-debate/>.
- 5 Samuel D. Warren, Louis D. Brandeis, “The Right to Privacy,” *Harvard Law Review*, 4, (December 1890), <https://faculty.uml.edu/sgallagher/Brandeisprivacy.htm>.
- 6 *Olmstead v. United States*, 277 U.S. 438 (1928) (Brandeis, L., dissenting).
- 7 *Olmstead v. United States*, 277 U.S. 438 (1928) (Brandeis, L., dissenting).
- 8 See, e.g., Michele Gilman and Rebecca Green, “The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization,” *NYU Review of Law and Social Change* 42 (2018): 253-307, <https://socialchangenyu.com/review/the-surveillance-gap-the-harms-of-extreme-privacy-and-data-marginalization/>.
- 9 Francella Ochillo, Gaurav Laroia, Erin Shields, Miranda Bogen, Alisa Valentin, Priscilla Gonzalez, Brandi Collins-Dexter, “Centering Civil Rights in the Privacy Debate,” (Panel, Washington, DC, May 9, 2019), <https://www.newamerica.org/oti/events/centering-civil-rights-privacy-debate/>.
- 10 Jody Feder, *Federal Civil Rights Statutes: A Primer*. Congressional Research Service, March 26, 2012, https://digital.library.unt.edu/ark:/67531/metadc85457/m1/1/high_res_d/RL33386_2012Mar26.pdf.
- 11 Meghan Droste. “What are ‘Protected Classes’?” *Subscript Law*, December 4, 2018, <https://www.subscriptlaw.com/blog/protected-classes>.
- 12 42 U.S.C. §§1973 et seq. Public accommodations are defined as establishments that serve the public with a connection to interstate commerce. They include hotels and motels, restaurants and bars, and entertainment venues like movie theaters and sports arenas.
- 13 42 U.S.C. §§3601 et seq.
- 14 15 U.S.C. §§1691 et seq.
- 15 Francella Ochillo, Gaurav Laroia, Erin Shields, Miranda Bogen, Alisa Valentin, Priscilla Gonzalez, Brandi Collins-Dexter, “Centering Civil Rights in the Privacy Debate,” (Panel, Washington, DC, May 9, 2019), <https://www.newamerica.org/oti/events/centering-civil-rights-privacy-debate/>.
- 16 “Letter to Congress on Civil Rights and Privacy,” (Letter from Access Now et al., to the Federal Communications Commission, April 19, 2019), https://newamericadotorg.s3.amazonaws.com/documents/Letter_to_Congress_on_Civil_Rights_and_Privacy_4-19-19.pdf.
- 17 See, e.g., Caroline Haskins, “Amazon’s Home Security Company Is Turning Everyone Into Cops,” *Motherboard*, February 7, 2019, https://motherboard.vice.com/en_us/article/qvyvzd/amazons-home-securitycompany-is-turning-everyone-into-cops.

- 18 See, e.g., Miranda Bogen and Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, (Washington, DC: Upturn, December 2018), <https://www.upturn.org/reports/2018/hiring-algorithms/>.
- 19 See, e.g., John Logan Koepke and David G. Robinson, "Danger Ahead: Risk Assessment and the Future of Bail Reform," *Washington Law Review*, Vol. 93, (December 25, 2018), <https://ssrn.com/abstract=3041622>. Predictive tools like pretrial risk assessments in the criminal justice system may reinforce racial disparities.
- 20 Francella Ochillo, Gaurav Laroia, Erin Shields, Miranda Bogen, Alisa Valentin, Priscilla Gonzalez, Brandi Collins-Dexter, "Centering Civil Rights in the Privacy Debate," (Panel, Washington, DC, May 9, 2019), <https://www.newamerica.org/oti/events/centering-civil-rights-privacy-debate/>.
- 21 See, e.g., "OTI and Over 40 Civil Rights, Civil Liberties, and Consumer Groups Call on Congress to Address Data-Driven Discrimination," New America, February 13, 2019, <https://www.newamerica.org/oti/press-releases/oti-and-over-40-civil-rights-civil-liberties-and-consumer-groups-call-congress-address-data-driven-discrimination/>.
- 22 "Civil Rights, Civil Liberties, and Consumer Groups Urge Congress to Protect Marginalized Communities from Discriminatory Privacy Abuses," New America, April 19, 2019, <https://www.newamerica.org/oti/press-releases/civil-rights-civil-liberties-and-consumer-groups-urge-congress-protect-marginalized-communities-discriminatory-privacy-abuses/>.
- 23 See, e.g., Alvaro M. Bedoya, "The Color of Surveillance," *Slate*, January 18, 2016, <https://slate.com/technology/2016/01/what-the-fbis-surveillance-of-martin-luther-king-says-about-modern-spying.html>
- 24 Claudia Garcia-Rojas, "The Surveillance of Blackness: From the Trans-Atlantic Slave Trade to Contemporary Surveillance Technologies," *Truthout*, March 3, 2016, <https://truthout.org/articles/the-surveillance-of-blackness-from-the-slave-trade-to-the-police/>.
- 25 Simone Browne, "Digital Epidermalization: Race, Identity and Biometrics," *Critical Sociology* 36 (2009), <https://pdfs.semanticscholar.org/b21b/dfd46a5c7ab3c6b71401762ed986bb0571c3.pdf>
- 26 Lindsey Mancini, Andrea Soehnchen, Phillip Soehnchen, Patrik Anderson, Johan Wallén, *Video Surveillance in Public Transport*, (International Association of Public Transport, November 2015), <https://www.uitp.org/sites/default/files/cck-focus-papers-files/151113-VS-full-report-final.pdf>
- 27 Emma Coleman and Myacah Sampson, "The Need to Regulate AI Implementation in Public Assistance Programs," *The Ethical Machine: Big Ideas for Designing Fairer AI and Algorithms*, (Cambridge, MA: Shorenstein Center, April 12, 2019), <https://ai.shorensteincenter.org/ideas/2019/4/3/the-need-to-regulate-ai-implementation-in-public-assistance-programs>.
- 28 Michele Gilman and Rebecca Green, "The Surveillance Gap: The Harms of Extreme Privacy and Data Marginalization," *NYU Review of Law and Social Change* 42 (2018): 253-307, <https://socialchangenyu.com/review/the-surveillance-gap-the-harms-of-extreme-privacy-and-data-marginalization/>
- 29 Shaka McGlotten, "Black Data," (from the colloquia series "Feminist & Queer Approaches to Technoscience," University of Toronto, ON, February 13, 2004). <https://sfoonline.barnard.edu/traversing-technologies/shaka-mcglotten-black-data/>
- 30 Boris Lubarsky, "Re-Identification of 'Anonymized' Data," *Georgetown Law Technology Review* 1, (April 2017): 202-213, <https://perma.cc/86RR-JUFT>.

- 31 See, e.g., “Kari Paul, “Protesters demand Amazon break ties with Ice and Homeland Security,” *The Guardian*, July 11, 2019, <https://www.theguardian.com/us-news/2019/jul/11/amazon-ice-protest-immigrant-tech>.
- 32 See, e.g., Miranda Bogen and Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, (Washington, DC: Upturn, December 2018), <https://www.upturn.org/reports/2018/hiring-algorithms/>.
- 33 Bogen and Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*.
- 34 See, e.g., Aaron Smith, “Public Attitudes Toward Computer Algorithms,” *Pew Research Center*, November 16, 2018, <https://www.pewinternet.org/2018/11/16/public-attitudes-toward-computer-algorithms/>.
- 35 Erica Volini et al., *Leading the social enterprise: Reinvent with a human focus*, (Deloitte Insights, 2019), https://www2.deloitte.com/content/dam/insights/us/articles/5136_HC-Trends-2019/DI_HC-Trends-2019.pdf
- 36 See, e.g., “Don’t Post and Pray—Control Your Job Posting Results,” *Recruiting.com*, <https://www.recruiting.com/blog/dont-post-pray-control-job-posting-results>.
- 37 Muhammad Ali et al., “Discrimination through optimization: How Facebook’s ad delivery can lead to skewed outcomes,” *Computers and Society*, (April 19, 2019), <https://arxiv.org/abs/1904.02095>.
- 38 Miranda Bogen and Aaron Rieke, *Help Wanted: An Examination of Hiring Algorithms, Equity, and Bias*, Upturn, (Washington, D.C., December 2018), <https://www.upturn.org/reports/2018/hiring-algorithms/>.
- 39 Sheryl Sandberg, “Doing More to Protect Against Discrimination in Housing, Employment and Credit Advertising,” Facebook, March 19, 2019, newsroom.fb.com/news/2019/03/protecting-against-discrimination-in-ads/.
- 40 Ariana Tobin and Jeremy B. Merrill, “Facebook is Letting Job Advertisers Target Only Men,” *ProPublica*, September 18, 2018, <https://www.propublica.org/article/facebook-is-letting-job-advertisers-target-only-men>.
- 41 Tobin and Merrill, “Facebook is Letting Job Advertisers Target Only Men.”
- 42 Muhammad Ali et al., “Discrimination through optimization: How Facebook’s ad delivery can lead to skewed outcomes,” *Computers and Society*, (April 19, 2019), <https://arxiv.org/abs/1904.02095>
- 43 Muhammad Ali et al., “Discrimination through optimization: How Facebook’s ad delivery can lead to skewed outcomes.”
- 44 Francella Ochillo, Gaurav Laroia, Erin Shields, Miranda Bogen, Alisa Valentin, Priscilla Gonzalez, Brandi Collins-Dexter, “Centering Civil Rights in the Privacy Debate,” (Panel, Washington, DC, May 9, 2019), <https://www.newamerica.org/oti/events/centering-civil-rights-privacy-debate/>.
- 45 Muhammad Ali et al., “Discrimination through optimization: How Facebook’s ad delivery can lead to skewed outcomes,” *Computers and Society*, (April 19, 2019), <https://arxiv.org/abs/1904.02095>.
- 46 Rachel Goodman, “Why Amazon’s Automated Hiring Tool Discriminated Against Women,” American Civil Liberties Union, October 12, 2018, <https://www.aclu.org/blog/womens-rights/womens-rights-workplace/why-amazons-automated-hiring-tool-discriminated-against>. In 2014, Amazon started a project to automate internal hiring with the goal of building an algorithm that could review resumes and select candidates. The project was terminated when staff realized that the tool systematically discriminated against women applying for technical jobs like software engineer positions.

47 For more on the diversity crisis in the AI sector, see Sarah Meyers West, Meredith Whittaker, and Kate Crawford, *Discriminating Systems: Gender, Race, and Power in AI*, AI Now Institute (April 2019), <https://ainowinstitute.org/discriminatingystems.html>.

48 Jessica Lautz, Meredith Dunn, Brandi Snowden, Amanda Riggs, and Brian Horowitz, Real Estate in a Digital Age 2017 Report, National Association of Realtors, (2017), <https://www.nar.realtor/sites/default/files/reports/2017/2017-real-estate-in-a-digital-age-03-10-2017.pdf>.

49 Francella Ochillo, Gaurav Laroia, Erin Shields, Miranda Bogen, Alisa Valentin, Priscilla Gonzalez, Brandi Collins-Dexter, “Centering Civil Rights in the Privacy Debate,” (Panel, Washington, DC, May 9, 2019), <https://www.newamerica.org/oti/events/centering-civil-rights-privacy-debate/>.

50 Julia Angwin and Terry Parris Jr., “Facebook Lets Advertisers Exclude Users by Race,” *ProPublica*, October 28, 2016, <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race>

51 Muhammad Ali et al., “Discrimination through optimization: How Facebook’s ad delivery can lead to skewed outcomes,” *Computers and Society*, (April 19, 2019), <https://arxiv.org/abs/1904.02095>

52 Muhammad Ali et al., “Discrimination through optimization: How Facebook’s ad delivery can lead to skewed outcomes.”

53 Francella Ochillo, Gaurav Laroia, Erin Shields, Miranda Bogen, Alisa Valentin, Priscilla Gonzalez, Brandi Collins-Dexter, “Centering Civil Rights in the Privacy Debate,” (Panel, Washington, DC, May 9, 2019), <https://www.newamerica.org/oti/events/centering-civil-rights-privacy-debate/>.

54 Natasha Lomas, “Yes Facebook is using your 2FA phone number to target you with ads,” *TechCrunch*, September 2018, <https://techcrunch.com/>

2018/09/27/yes-facebook-is-using-your-2fa-phone-number-to-target-you-with-ads/; The Federal Trade Commission recently prohibited Facebook from engaging in that practice. *United States of America v. Facebook, Inc.*, July 24, 2019, D.D.C. 7, https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf. Facebook has also used artificial intelligence to learn more about users’ hobbies, preferences, and interests by mining users’ photos to train its facial recognition software toward the goal of creating new platforms to place more focused targeted ads, which the FTC also recently prohibited. Jared Bennett, “Facebook: Your Face Belongs to Us,” *Daily Beast*, July 31, 2017, <https://www.thedailybeast.com/how-facebook-fights-to-stop-laws-on-facial-recognition>.

55 Steven Petrow, “With my cell-phone number, a private eye found 150 pages on me,” *USA Today*, July 24, 2017, <https://www.usatoday.com/story/tech/columnist/2017/07/21/my-cell-phone-number-private-eye-found-150-pages-me/472993001/>.

56 Malkia Cyril, “We Are the Color of Freedom: To Win Migrant Rights, Demand Digital Sanctuary,” presentation at Color of Surveillance Conference, Georgetown Law Center, June 22, 2017, <https://www.youtube.com/watch?v=o95iyQt31zs>.

57 Barton Gellman and Sam Adler-Bell, The Disparate Impact of Surveillance, (The Century Foundation, December 21, 2017), <https://tcf.org/content/report/disparate-impact-surveillance/?session=1#easy-footnote-bottom-28>

58 See, e.g., Eli Rosenberg, “Motel 6 will pay \$12 million to guests whose personal data was shared with ICE,” *Washington Post*, April 8, 2019, https://www.washingtonpost.com/nation/2019/04/06/motel-leaked-personal-data-guests-ice-officials-say-now-it-owes-them-million/?utm_term=.d6775c0fd3be.

59 Koustubh “K.J.” Bagchi, “Privacy in the Digital World: Breaches Underscore Need for Federal Action,” *Medium*, July 3, 2018, <https://medium.com/>

advancing-justice-aajc/privacy-in-the-digital-world-breaches-underscore-need-for-federal-action-21c8ea122e62.

60 While Amazon does not directly contract with ICE, the company has been heavily criticized for providing critical support to companies like Palantir through its Amazon Web Services cloud storage platform. Rachel Sandler, “Internal Email: Amazon Faces Pressure From More Than 500 Employees to Cut Ties with Palantir for Working with ICE,” *Forbes*, July 11, 2019, <https://www.forbes.com/sites/rachelsandler/2019/07/11/internal-email-amazon-faces-pressure-from-more-than-500-employees-to-cut-ties-with-palantir-for-working-with-ice/#4dd1a5137539>.

61 Manish Singh, “Palantir’s software was used for deportations, documents show,” *TechCrunch*, May 2019, <https://techcrunch.com/2019/05/03/palantirs-software-was-used-for-deportations-documents-show/>.

62 Francella Ochillo, Gaurav Laroia, Erin Shields, Miranda Bogen, Alisa Valentin, Priscilla Gonzalez, Brandi Collins-Dexter, “Centering Civil Rights in the Privacy Debate,” (Panel, Washington, DC, May 9, 2019), <https://www.newamerica.org/oti/events/centering-civil-rights-privacy-debate/>.

63 Koustubh “K.J.” Bagchi, “Privacy in the Digital World: Breaches Underscore Need for Federal Action,” Medium, July 3, 2018, <https://medium.com/advancing-justice-aajc/privacy-in-the-digital-world-breaches-underscore-need-for-federal-action-21c8ea122e62>.

64 Nadeem Muadi, “The Bush-era Muslim registry failed. Yet the U.S. could be trying it again,” *CNN*, December 22, 2016, <https://www.cnn.com/2016/11/18/politics/nseers-muslim-database-qa-trnd/index.html>.

65 Sandra E. Garcia, “U.S. Requiring Social Media Information from Visa Applicants,” *New York Times*,

June 2, 2019, <https://www.nytimes.com/2019/06/02/us/us-visa-application-social-media.html>.

66 Koustubh “K.J.” Bagchi, “Privacy in the Digital World: Breaches Underscore Need for Federal Action,” Medium, July 3, 2018, <https://medium.com/advancing-justice-aajc/privacy-in-the-digital-world-breaches-underscore-need-for-federal-action-21c8ea122e62>.

67 Margaret Hu, “Big Data Blacklisting,” *Florida Law Review* 67 (March 2016): 1735-1809. <https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=1289&context=flr>.

68 “Charlotte,” *Our Data Bodies*, <https://www.odbproject.org/our-cities/charlotte/>. In a state like North Carolina, this data practice has significant implications for racial equity, since Black residents are five times more likely than white counterparts to be incarcerated.

69 Stop LAPD Spying Coalition, *Before the Bullet Hits the Body*. (Los Angeles, CA: May 8, 2018). <https://stoplapdspying.org/wp-content/uploads/2018/05/Before-the-Bullet-Hits-the-Body-Report-Summary.pdf>.

70 Mikella Hurley and Julius Adebayo. “Credit Scoring in the Era of Big Data,” *Yale Journal of Law and Technology* (2017). Vol. 18 (1), Article 5. <https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1122&context=yjolt>.

71 Francella Ochillo, Gaurav Laroia, Erin Shields, Miranda Bogen, Alisa Valentin, Priscilla Gonzalez, Brandi Collins-Dexter, “Centering Civil Rights in the Privacy Debate,” (Panel, Washington, DC, May 9, 2019), <https://www.newamerica.org/oti/events/centering-civil-rights-privacy-debate/>.

72 Ochillo, Laroia, Shields, Bogen, Valentin, Gonzalez, Collins-Dexter, “Centering Civil Rights in the Privacy Debate.”

- 73 Mary Madden, “The Devastating Consequences of Being Poor in the Digital Age,” *New York Times*, April 25, 2019, <https://www.nytimes.com/2019/04/25/opinion/privacy-poverty.html>.
- 74 Mary Madden, *Privacy, Security, and Digital Inequality*, (New York, NY: Data & Society, September 27, 2017), https://datasociety.net/pubs/prv/DataAndSociety_PrivacySecurityandDigitalInequality.pdf. Communities of color also suffer from lack of education and training with digital tools, leaving them vulnerable to breaches in privacy and attacks on their data, as well as online scams and fraud.
- 75 “Civil Rights Groups Call on Social Media Platforms to Better Address Hate Violence and Groups,” *Muslim Advocates*, February 22, 2018, <https://www.muslimadvocates.org/civil-rights-groups-call-on-social-media-platforms-to-better-address-hate-violence-and-groups/>.
- 76 Michael Golebiewski and Dana Boyd, *Data Voids: Where Missing Data Can Easily Be Exploited*, (New York, NY: Data & Society, May 2018), https://datasociety.net/wp-content/uploads/2018/05/Data_Society_Data_Voids_Final_3.pdf and Rebecca Lewis, *Alternative Influence: Broadcasting the Reactionary Right on Youtube*, (New York, NY: Data & Society, September 2018), https://datasociety.net/wp-content/uploads/2018/09/DS_Alternative_Influence.pdf.
- 77 Rachel Hatzipanagos, “How Online Hate Turns into Real-Life Violence,” *Washington Post*, November 30, 2018, https://www.washingtonpost.com/nation/2018/11/30/how-online-hate-speech-is-fueling-real-life-violence/?utm_term=.5876c76a231b.
- 78 Kunal Relia, Zhengyi Li, Stephanie H. Cook, and Rumi Chunara, “Race, Ethnicity and National Origin-based Discrimination in Social Media and Hate Crimes Across 100 U.S. Cities,” *Computers and Society*, (Submitted January 31, 2019 for peer review), <https://arxiv.org/abs/1902.00119>.
- 79 Joseph Cox, “I Gave a Bounty Hunter \$300. Then He Located Our Phone,” *Motherboard Tech by Vice*, January 8, 2019, https://www.vice.com/en_us/article/nepxbz/i-gave-a-bounty-hunter-300-dollars-located-phone-microbilt-zumigo-tmobile.
- 80 Joseph Cox, “Black Market T-Mobile Location Data Tied to Spot of a Triple Murder,” *Motherboard Tech by Vice*, June 26, 2019, https://www.vice.com/en_us/article/vb9nzx/black-market-tmobile-phone-location-data-bounty-hunter-murder.
- 81 Joseph Cox, “Black Market T-Mobile Location Data Tied to Spot of a Triple Murder.”
- 82 Alison Bateman-House, “Why Grindr’s Privacy Breach Matters to Everyone,” *Forbes*, April 10, 2018, <https://www.forbes.com/sites/alisonbatemanhouse/2018/04/10/why-grindr-privacy-breach-matters-to-everyone/#36d40a1067f4>.
- 83 See, e.g., Aaron Rieke and Corrine Yu, “Discrimination’s Digital Frontier,” *The Atlantic*, April 15, 2019, <https://www.theatlantic.com/ideas/archive/2019/04/facebook-targeted-marketing-perpetuates-discrimination/587059/>.
- 84 Department of Housing and Development, *Charge of Discrimination: Assistant Secretary for Fair Housing and Equal Opportunity versus Facebook, Inc.*, HUD ALJ No. FHEO No. 01-18-0323-8. https://www.hud.gov/sites/dfiles/Main/documents/HUD_v_Facebook.pdf
- 85 Tracy Jan and Elizabeth Dwoskin, “Facebook agrees to overhaul targeted advertising system for job, housing and loan ads after discrimination complaints,” *Washington Post*, March 19, 2019, https://www.washingtonpost.com/business/economy/facebook-agrees-to-dismantle-targeted-advertising-system-for-job-housing-and-loan-ads-after-discrimination-complaints/2019/03/19/7dc9b5fa-4983-11e9-b79a-961983b7e0cd_story.html?utm_term=.42d0ac377423.

86 Georgetown Law Center on Privacy & Technology, New America's Open Technology Institute, and Free Press, Informal Complaint against AT&T Corporation, T-Mobile U.S., Sprint Corporation, Verizon Wireless for Unauthorized Disclosure and Sale of Customer Location Information, Before the Federal Communications Commission, June 14, 2019, https://newamericadotorg.s3.amazonaws.com/documents/Informal_Complaint_re_Unauthorized_Disclosure.pdf.

87 Gaurav Laroia and David Brody, "Privacy Rights are Civil Rights. We Need to Protect Them," *Free Press*, March 14, 2019, <https://www.freepress.net/our-response/expert-analysis/insights-opinions/privacy-rights-are-civil-rights-we-need-protect-them>.

88 Scott Shane and Sheera Frenkel, "Russian 2016 Influence Operation Targeted African-Americans on Social Media," *New York Times*, December 17, 2018, <https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html>. See also, e.g., Scott Detrow, "What Did Cambridge Analytica Do During The 2016 Election?," *NPR*, March 20, 2018, <https://www.npr.org/2018/03/20/595338116/what-did-cambridgeanalytica-do-during-the-2016-election>.

89 "Your Equal Credit Opportunity," Federal Trade Commission, January 2013, <https://www.consumer.ftc.gov/articles/0347-your-equal-credit-opportunity-rights>. The FTC has some experience protecting civil rights, as it is responsible for enforcing the antidiscrimination sections of the Equal Credit Opportunity Act. It is also arguably an "unfair" practice for a company to engage in discriminatory conduct. However, the FTC has not brought any such cases.

90 "FTC Testifies on Its Work to Protect Consumers and Promote Competition As the Agency Approaches Its 100th Anniversary," Federal Trade Commission, December 3, 2013, <https://www.ftc.gov/news-events/press-releases/2013/12/ftc-testifies-its-work-protect-consumers-promote-competition>.

91 *The Online Civil Rights and Privacy Act of 2019*, (Washington, DC: Free Press and Lawyers' Committee for Civil Rights Under Law, March 11, 2019), https://www.freepress.net/sites/default/files/2019-03/online_civil_rights_and_privacy_act_of_2019.pdf.

92 Francella Ochillo, Gaurav Laroia, Erin Shields, Miranda Bogen, Alisa Valentin, Priscilla Gonzalez, Brandi Collins-Dexter, "Centering Civil Rights in the Privacy Debate," (Panel, Washington, DC, May 9, 2019), <https://www.newamerica.org/oti/events/centering-civil-rights-privacy-debate/>.

93 Ochillo, Laroia, Shields, Bogen, Valentin, Gonzalez, Collins-Dexter, "Centering Civil Rights in the Privacy Debate."

94 *The Online Civil Rights and Privacy Act of 2019*, (Washington, DC: Free Press and Lawyers' Committee for Civil Rights Under Law, March 11, 2019), https://www.freepress.net/sites/default/files/2019-03/online_civil_rights_and_privacy_act_of_2019.pdf.

95 *The Online Civil Rights and Privacy Act of 2019*.

96 Francella Ochillo, Gaurav Laroia, Erin Shields, Miranda Bogen, Alisa Valentin, Priscilla Gonzalez, Brandi Collins-Dexter, "Centering Civil Rights in the Privacy Debate," (Panel, Washington, DC, May 9, 2019), <https://www.newamerica.org/oti/events/centering-civil-rights-privacy-debate/>.

97 *AG Ferguson investigation leads to Facebook Making Nationwide Changes to Prohibit Discriminatory Advertisements on its Platform*, (Olympia, Washington: Washington State Office of Attorney General, July 28, 2018), <https://www.atg.wa.gov/news/news-releases/ag-ferguson-investigation-leads-facebook-making-nationwide-changes-prohibit>.

98 Alisa Valentin, "#TechPolicySoWhite," *Public Knowledge*, February 1, 2019, <https://>

www.publicknowledge.org/news-blog/blogs/techpolicysowhite.

99 Valentin, “#TechPolicySoWhite.”

100 Francella Ochillo, Gaurav Laroia, Erin Shields, Miranda Bogen, Alisa Valentin, Priscilla Gonzalez, Brandi Collins-Dexter, “Centering Civil Rights in the Privacy Debate,” (Panel, Washington, DC, May 9, 2019), <https://www.newamerica.org/oti/events/centering-civil-rights-privacy-debate/>.



This report carries a Creative Commons Attribution 4.0 International license, which permits re-use of New America content when proper attribution is provided. This means you are free to share and adapt New America’s work, or include our content in derivative works, under the following conditions:

- **Attribution.** You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

For the full legal code of this Creative Commons license, please visit **creativecommons.org**.

If you have any questions about citing or reusing New America content, please visit **www.newamerica.org**.

All photos in this report are supplied by, and licensed to, **shutterstock.com** unless otherwise stated. Photos from federal government sources are used under section 105 of the Copyright Act.