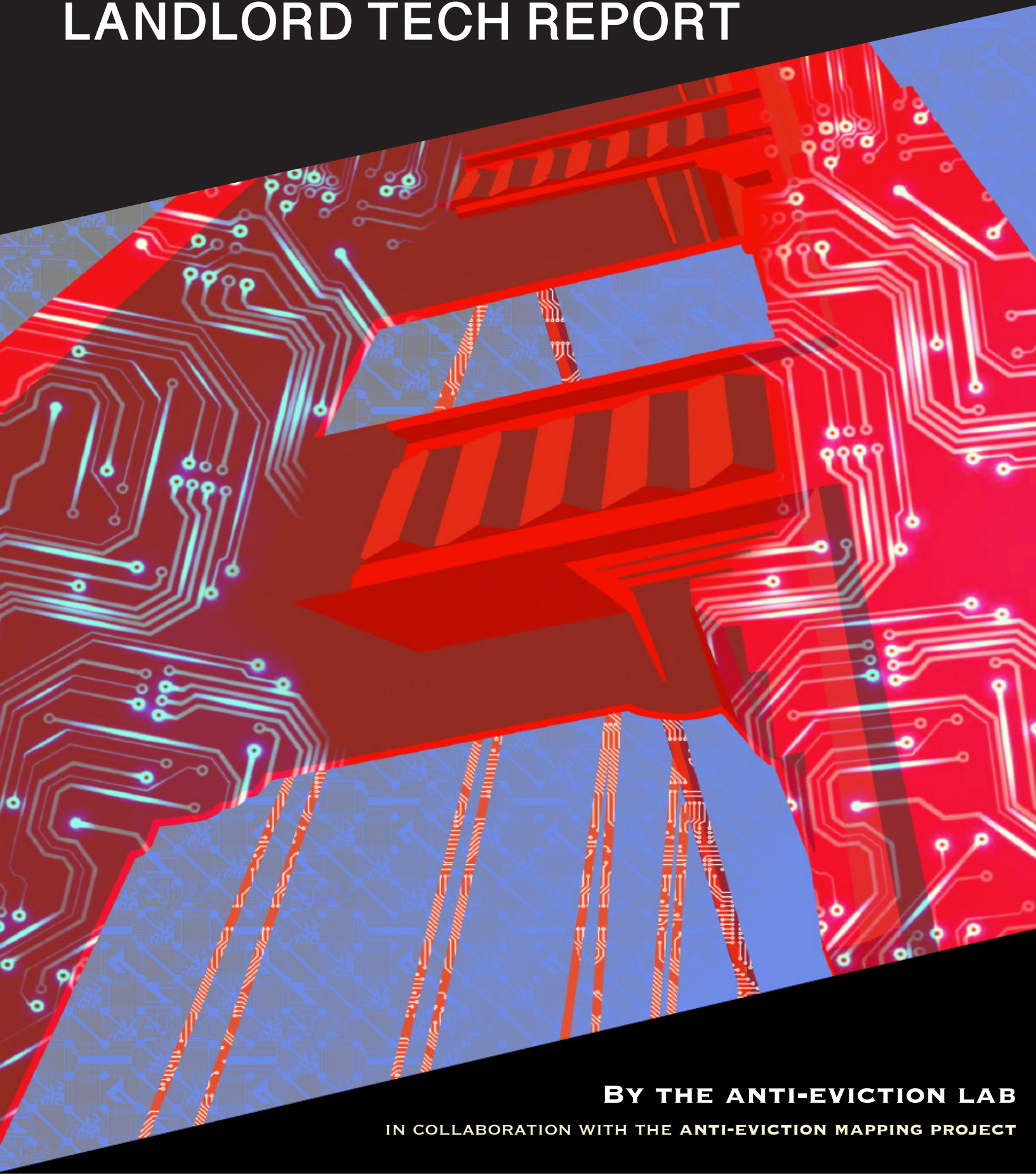
SAN FRANCISCO LANDLORD TECH REPORT



By the Anti-Eviction Lab

In collaboration with the **Anti-Eviction Mapping Project**

Cover image designed by Alyssa Ramirez
Layout and design by Noah Cohen and Alyssa Ramirez
Images created by Noah Cohen, Lulia Liu Pan, Alyssa Ramirez, and Shiyu Catherine Xu

Acknowledgements

This report is by Erin McElroy, Noah Cohen, Paula Garcia-Salazar, Gracie Harris, Andrew Liquigan, Matt Martignoni, Maggie McCarroll, Lulia Liu Pan, Alyssa Ramirez, and Shiyu Catherine Xu.

Thanks to Jessica Finkel, Terra Graziani, Jeantelle Laberinto, Priya Prabhakar, Joseph Smooke, and Ashley Xu for edits and feedback.

This report is based upon some prior research conducted with the AI Now Institute at New York University on landlord technologies in New York City that informed a report written by Erin McElroy, Manon Vergerio, and Paul Garcia-Salazar published by the Anti-Eviction Mapping Project and the AI Now Institute in 2022.[1]

We are grateful to the Anti-Monopoly Fund, the Calyx Institute, the Ford Foundation, and the Undergraduate Research Apprenticeship Program at the University of Texas at Austin for supporting this work.

Table of Contents

INTRODUCTION

This report examines the increasing deployment of landlord technologies in San Francisco (SF) housing and the problems this creates and intensifies. These technologies include facial recognition, closed-circuit television (CCTV) cameras, and other algorithmic, biometric, and app-based building access technologies specifically designed to be deployed in tenant housing and surrounding public and private space. As researchers with the Anti-Eviction Lab and the Anti-Eviction Mapping Project, we map the genealogies and geographies of these surveillance systems, looking at intersections of surveillance, carcerality, and gentrification.

While the real estate industry uses the term "property technology," or "proptech," to describe the new technologies deployed in residential, commercial, and industrial buildings, here in this report we use the term "landlord tech" to specify its use in tenant housing and neighborhoods as deployed by landlords. For us, landlord tech encompasses the platforms, systems, algorithms, and data regimes connecting the real estate and technology industries in residential, commercial, and industrial buildings. This collaborative renaming arose through meetings held at the AI Now Institute with members of the Anti-Eviction Mapping Project (which maintains chapters in the San Francisco Bay Area, New York City, and Los Angeles, [people.power.media] of San Francisco, the OceanHill-Brownsville Alliance based out of Brooklyn. Together, we produced a nomenclature of landlord technologies from a tenant harms perspective, as well as a survey, map, and a resource guide, all of which live today on our website, Landlord Tech Watch.[2] This work is now being led and maintained by the Anti-Eviction Lab based out of UT Austin and the University of Washington. On the site, we define and expose the systems, platforms, hardware, software, algorithms, and data collection that landlords and property managers use to automate landlordism. These include tenant screening services that provide reports about prospective tenants so that landlords can determine if the tenant is "good enough" to move in, as well as eviction and debt-recovery apps, property management apps and platforms, neighborhood surveillance apps, biometric building entry systems, and more.

This report focuses on the geographies, harms, and histories of surveillance and platform-based landlord tech in San Francisco housing. As we show, despite some progressive tenant and anti-surveillance legislation in place, tenants are nevertheless disproportionately subjected to the automation of gentrification through new landlord technologies. New collaborations between landlord technology companies, landlords, gentrifiers, and developers incite racial profiling, augmented policing, automated evictions and fines, gentrification, and real estate speculation, particularly in contexts of crisis. We write this in a moment of increased housing crisis augmented by the Covid-19 pandemic, alongside novel waves of carcerality in the city. With the eviction moratorium about to expire,[3] intersections between gentrification and policing have reached a new fever pitch. Accusations that San Francisco's former fire commissioner has terrorized unhoused people with bear spray have surfaced,[4] and the abolitionist District Attorney Chesa Boudin was recalled in a pro-police ouster, only to be replaced by Brooke Jenkins through a mayoral push to renew the war on crime and drugs.[5] We can't forget the propagandistic Atlantic hit piece (and similar articles) written against San Francisco's unruly unhoused population, in which the city is described as "failed."[6] In response, in 2022, the Board of Supervisors approved Mayor London Breed's experiment to allow law enforcement to access private surveillance footage in real time.[7] With this climate in mind, here we assess how increased surveillance is not the solution, but rather a tactic to augment the violence of gentrification upon tenants and the unhoused. We highlight how it is disproportionately poor, working-class, and racialized residents and the unhoused disproportionately subjected to policing and eviction through surveillance technology.

We begin in Chapter 1 by examining the history of cameras in tenant housing in San Francisco. Here we focus on the introduction of cameras in public housing, and then look at how prevalent cameras are today. Chapter 2 looks at the phenomenon of "digital doormen" deployed in tenant housing in the city, focusing on the surveillance harms that new high tech intercom and smart home entrance systems impose upon tenants. We then in Chapter 3 turn platforms that enable neighborhood surveillance and policing such as Nextdoor and Citizen. Chapter 4 explores the history of Airbnb in San Francisco, exploring if there are best practices to think through regarding the regulation of private tech in private landlord-owned housing. Next in Chapter 5, we explore tenant screening and the algorithmic harms it imposes upon tenants. We then look at the policy landscape of landlord technologies more broadly in Chapter 6, exploring intersections of surveillance, privacy, and tenant law. We conclude in Chapter 7 by gesturing towards possibilities of organizing against landlord technologies and the automation of gentrification.

1
CAMERAS IN TENANT HOUSING IN SAN FRANCISCO

Here, we will explore the prevalence of surveillance cameras in multi-unit residential settings. In particular, we will investigate the history of surveillance in public and privately owned housing in San Francisco, as well as how surveillance technology gets used today.

Histories of Cameras in Urban Surveillance: From Policing to Public Housing

The prevalence of cameras in tenant housing today is linked to the encroachment of the police state in public housing and public space more generally. The 1960s saw the rise of closed-system television (CCTV) cameras deployed both in the public sector by police, and in the private sector by businesses and private landlords.[8] CCTV cameras were first designed in 1942 by the German company Siemens AG for Nazi Germany to monitor the launch of the first long-range guided ballistic missiles.[9] The US companies followed suit, and by 1949 the US contractor Vericon began using CCTV for private use. British police began using CCTV in the 1960s and US police began in 1971 in Mt. Vernon, New York, though it was not until the 1980s that police began relying heavily on cameras.[10]

Broad technological advances in urban management occurred simultaneously through the 1960s and 1970s, with urban administrations in the US beginning to utilize cybernetics, urban control rooms, geographic information systems (GIS), and urban planning software technologies.[11] In the 1980s, Mike Bloomberg's "Bloomberg Terminals" launched in New York City, pioneering new methods of dashboard governance.[12] Subsequently, numerous cities began adopting data management systems and CCTV-integrated data fusion centers, often in partnership with the private sector through companies such as Microsoft and IBM.[13]

In 1997, 13 US cities had their own public surveillance programs. By 2016, 49 percent of local police departments in the United States used CCTV.[14] The proliferation of CCTV and video surveillance in private residential buildings has been highly normalized despite the ongoing concerns of housing advocates.

In 2005, San Francisco launched what would become a widespread effort to surveil the city and public housing within it. That year had been one of numerous homicides, which then-mayor Gavin Newsom used as justification to launch a new surveillance program. He was inspired by a program that had been launched in Chicago, where in 2003, 30 surveillance cameras had been installed in "high-crime areas."[15] Newsom visited the US Mayors conference there in 2005–a visit that he cited as one that opened his mind to the idea of cameras in public space.

Newsom conceptualized a modest pilot program to assess community reactions to increased surveillance and determine whether privacy concerns would arise. The cameras he would go on to install in the pilot program were intended to be less intrusive than the ones in Chicago. They were not monitored in real time (police would have to file a request from the Department of Emergency Management to see them), no audio footage was recorded, and there was no gunfire detection. The trial lasted 90 days and coincided with substantial decreases in crime rates.

By the time the San Francisco public housing surveillance camera pilot program launched, cameras were already ubiquitous in Chicago, New York, New Orleans, Detroit, Los

Angeles and Baltimore.[16] In 2005, a pilot program in SF was launched in Western Addition, a historically Black neighborhood, by installing 33 cameras. Two bullet proof cameras were installed atop utility poles, and after Newsom chose six additional locations to experiment within the city–all areas marked by high rates of homicide and all predominantly Black neighborhoods.[17] These "community safety cameras" recorded 72 hours of visual material and not sound. All digital material was to be erased after being recorded unless the SFPD requested access. Despite these safeguards, the placement of cameras deeply worried the American Civil Liberties Union (ACLU), with Director for Technology and Civil Liberties in San Francisco, Nicole Ozer explaining, "Video cameras don't reduce crime. What they do have an impact on is personal privacy and peoples' civil rights. And if anything, they just move crime from one corner to another corner."[18] Similarly, as George Smith, director of Ella Hill Hutch Community Center in Western Addition described, "I know some people are really excited about the cameras because of what it represents. And it represents some hope that something's going to be done. But, at the same time, man, what is really being done? You know, what is the relationship between the community and the police? You know, right now there's not a really good relationship with the Police Department. That's why they can't get people to step up because there's no trust that, you know, people feel safe."[19]

In 2006, the ACLU launched opposition to the program, citing privacy concerns. Subsequently, the Board of Supervisors unanimously passed the Community Safety Camera (CSC) Ordinance to limit the installation and use of public security cameras. Provisions stated that footage could only be stored for 30 days, that police make annual reports about usage, and that cameras could only be installed at "locations experiencing substantial crime."[20]

In 2006, 50 new cameras costing between $4,000-$7,000 apiece were installed in public housing paid by federal funds.[21] By 2007, up to 178 cameras had been deployed in public housing developments such as Sunnydale, Bernal Dwellings, Yerba Buena Plaza, Alemany and Plaza East, all managed by the SF Housing Authority, totalling $203,603 in costs.[22] Yet the Housing Authority, at least at the time, did not keep track of how its cameras were used by the police. There were also plans to install 81 additional cameras. Many community members and tenants found this intrusion unsettling, leading Gavin Newsom (then SF mayor to say "If the community demands the cameras be removed, they'll be removed. . . "We're not forcing this on anyone." This has been far from the case.

Also in 2006, 22 new cameras were set up in the Mission, Civic Center, and Chinatown neighborhoods. Then, 70 city-owned cameras were installed in "high crime" spots in 2007 throughout the city. These were not installed in public housing but rather on housing complexes' borders. While the city-funded cameras weren't monitored and while they erased images automatically after 72 hours (though they could be accessed by police), housing authority cameras were continuously monitored and images were saved for 30 days.[23]

In 2008, the city commissioned a report on the cameras' efficacy (as stipulated by the CSC), and found they did essentially nothing to stop crime. To the extent they helped solve crimes, the image quality was so poor that they essentially just facilitated profiling.

The only meaningful impact was a decrease in petty theft in proximity to the cameras (displaced by an increase in other areas). There were cases of murders occurring in front of the cameras and not being caught because the cameras were pointed towards the sky. After this report was released, the Board of Supervisors called into question the budget being dedicated to the cameras and ended up voting to continue maintaining the current cameras, but cut off future funding for installation and maintenance. As a result the cameras were simply never upgraded and have become largely useless.

It was in 2009 that Heather Fong, who had been helping lead the city's surveillance program, stepped down from being chief of the San Francisco Police Department (SFPD). She was replaced by George Gascón. As he described early on into his tenure, although the camera program was flawed, it could be improved by using real-time monitoring, as Chicago was already doing. Gascón had previously been involved in a similar initiative in Los Angeles that involved real-time monitoring. In his words,"One of the values of the camera system, assuming that it's appropriately deployed and you have the right safeguards to protect people's rights, is that there has to be clear consequences when you commit criminal violations that are within the [view] of the camera. In order to do so you have to have real-time monitoring."[24] Yet he claimed to not be ready to implement such real-time systems in San Francisco yet.

After a handful of political moves, with Newsom filing to run as Lieutenant Governor (he is now Governor), Ed Lee becoming Mayor (he has since passed away), and Gascón becoming SF District Attorney (he is now the DA of LA County), attention seemed to fade from upgrading the city's camera system. According to SFPD Northern Station Captain Greg McEachern in 2012, "The cameras were put in place almost ten years ago and it is the same technology from that time… Obviously, camera pixels and quality have improved over the years with new camera systems but this is an original system. Thus, the quality is as good as it can be for a ten-year-old system."[25] Similarly, Vallie Brown (the previous Supervisor for District 5), then aide to Supervisor London Breed (now SF Mayor), reported that the city was unlikely to upgrade the cameras in the near future. In her words, "Unfortunately the quality of the cameras [is] so poor that even when the police have a case that warrants viewing the feed, it's hard to get a good ID. That's why the City is not spending the $25K each for more cameras. The police are getting better quality video and no civil liberties conflicts by accessing private cameras from businesses and residents."[26] As of 2012, there were 71 so-called Community Safety Cameras linked to the San Francisco Police Commission, which as of 2012 researchers at UC Berkeley found to have no impact on mitigating violent crime.[27]

Given the inadequacies of the existing public camera network, SFPD began turning to private camera systems in their attempts to solve crimes. As Hoodline reported in 2014:

> "San Francisco's camera program remains in its 2005-era state, underfunded and unreviewed. Ironically, a system that was intentionally limited due to civil liberty concerns now lacks any oversight to ensure that those civil liberties are actually being protected. And in the absence of a robust public network, police are increasingly turning to private video sources, which have no government-mandated oversight whatsoever."[28]

And indeed, police began working with the private sector not just to access footage from existing cameras, but also to install new ones. In 2012, tech executive Chris Larsen began investing $4 million to install over 1,000 cameras across 135 city blocks.[29] In doing so, he partnered with the city's Community Benefit Districts (CBDs),[30] controlling access to footage on private property–allegedly to identify individuals linked to property crime and car break-ins. There are currently 18 CBDs and Business Improvement Districts (BIDs) in the city,[31] several of which have surveillance networks installed. The EFF has mapped over 2,700 cameras in these districts across the city.[32] They determined that the ten most surveilled neighborhoods in the city are: Union Square, Civic Center/Tenderloin, SOMA, Chinatown/Jackson Square/Historic North Beach, Bayview/Portola, the Mission, South of the I-80, Western Addition, Russian Hill, and the Embarcadero.

The city adopted a new Surveillance Technology Ordinance in 2019, which prohibits municipal agencies including the SFPD from acquiring or utilizing surveillance technology without preapproval from the Board of Supervisors and then an open process which includes public participation.[33] Yet despite this, in 2020, the SFPD surveilled Black-led protests in the aftermaths of George Floyd's murder, tapping into a network of 400 cameras owned by Union Square's Business Improvement District (USBID).[34] In the words of organizer Hope Williams, plaintiff in the case led by the Electronic Frontier Foundation (EFF) and the American Civil Liberties Union (ACLU) of Northern California against the SFPD, "It was a tactic to provoke fear and keep people from speaking out. We have the right to organize, speak out, and march without fear of police surveillance. SFPD's spying on our protests was also a blatant disregard of the Surveillance Technology Ordinance here in San Francisco. I am a plaintiff in this lawsuit because I want to defend the rights of protestors and hold the police accountable for breaking the law."[35]

In the fall of 2022, the Board of Supervisors passed a law permitting police access to privately owned surveillance cameras and surveillance networks in their investigations. They are also now permitted to live monitor "significant events with public safety concerns" and visual records related to active misdemeanor and felony violations.[36] While law enforcement must obtain permission from camera owners, they do not need to obtain a warrant.

In January of 2023, the EFF discovered that the SFPD requested live access to 450 surveillance cameras in USBID as a precaution against possible protests in the aftermath of the murder of Tyre Nichols in Memphis, Tennessee.[37] They had hoped to obtain live 12-hour access monitoring. As the EFF suggests, this indicates the SFPD are likely interpreting the city's Surveillance Technology Policy too broadly. The current policy states, "SFPD is prohibited from accessing, requesting, or monitoring any surveillance camera live feed during First Amendment activities unless there are exigent circumstances or for placement of police personnel due to crowd sizes or other issues creating imminent public safety hazards."[38] Yet the police department requested footage in a context in which there were no imminent hazards or exigent circumstances.

Today, San Francisco maintains a surveillance technology inventory of its own cameras, which outlines the various surveillance methods used in city public spaces, from museums to City Hall to the Department of Homelessness and Supportive Housing, the

latter of which uses biometric fingerprinting to enroll single adult shelter clients.[39] Yet the majority of cameras used to surveil San Franciscans are privately owned and deployed by landlords and property owners, as we continue to explore.

Surveilled in Public and Private Housing

Like cameras in public spaces, cameras installed in housing that law enforcement agencies have come to rely upon are rarely if ever installed in service of the public good. On one hand, they help private landlords profit–both by appealing to high-paying tenants as a security feature and by helping landlords collect information that can be used to facilitate evictions, displacement, and gentrification. On the other, they abet cycles of carcerality by providing direct access to law enforcement. While police access to private surveillance feeds poses new dangers and deep discomfort for many residents, this intrusion is the icing on the cake of a broader and growing private surveillance state that landlords and law enforcement work together to employ in a number of different ways to keep tenants and the unhoused vulnerable.

From law enforcement utilizing cameras in public and private housing to landlords spying on and gathering data about tenants to automate gentrification and eviction processes, the carceral state has long been linked to domestic space in complex and entangled ways. In particular, law enforcement has both aided exclusionary practices in housing and inflicted disproportionate harm on those who have been excluded by these practices. On one hand, evictions themselves are carceral processes involving sheriffs departments. On the other, upon being evicted, numerous tenants end up unhoused and become disproportionately subjected to incarceration. Also there is the phenomenon in which gentrifiers call the police on their neighbors or report them as nuisances–a highly racialized genre of eviction in which residents take on policing power.[40] Increasingly this process mobilizes both privately and publicly sanctioned surveillance footage.

At the same time and across the United States, there has been a trend of public housing agencies purchasing biometric and algorithmic surveillance technologies, adding new devices to spaces that have long been overly surveilled by CCTV cameras.[41] Systems today are being financed by the U.S. Department of Housing and Urban Development (HUD) through federal crime fighting grants.[42] There are currently 13 cities that use facial recognition in public housing in the US. Of those, six plan to utilize such systems to identify blacklisted and banned tenants, assist in police investigations, grant or deny tenants access to buildings, and monitor lease violations.

Increased surveillance has been worrisome for tenants worried that they might be evicted for petty lease violations caught on camera. While HUD spokeswoman Christina Wilkes reported that the agency never intended for new surveillance systems to penalize residents for lease violations, she noted that such usage would not violate grant terms.[43] Though San Francisco became the first state to ban government use of facial recognition, the EFF discovered violations of the ban by the SFPD as soon as the following year.[44] Further, this does not prohibit public housing authorities from implementing other

surveillance. HUD did issue a public notice in April 2023 that it would cease to fund "automated surveillance and facial recognition technology," though this does not impact those who already purchased such tools.[45] Meanwhile, other cities that have banned use of facial recognition have been walking protections back, which doesn't bode well.[46]

In a 2023 exploration of surveillance in public housing across the US,[47] Doug MacMillan noted that "in many cases, I've found the residents are not aware of the cameras or any kind of policies around them. And in most of the cases I found the housing authorities haven't really kind of laid out policies around how they are going to use these cameras."[48] As he also noted, once tenants are evicted from public housing, including for violations caught on camera, it becomes more difficult for people to find future housing. This is due to tenant screening, which we outline in Chapter 5. As MacMillan reports, "A woman who was kicked out of her housing for smoking outside of the property, among other reasons. And she's living on her sister's couch. And she told me that when she's applying for housing now, when she goes to kind of apply for the next stop, she keeps getting into this barrier of they're running a reference check. And they're rejecting her based on her eviction from public housing. And so, you know, one instance like that of the cameras catching you doing something wrong could end up having lifetime consequences for you."[49]

With such dystopian living situations in mind, in 2020, the federal Facial Recognition and Biometric Technology Moratorium Act was introduced to ban the use of facial recognition systems in public housing.[50] The act was reintroduced in March 2023. As Representatives Maxine Waters of California and Ayanna Pressley of Massachusetts wrote to HUD Secretary Marcia Fudge in May 2023, "the use of facial-recognition technology in public and HUD-assisted housing for surveillance purposes . . causes harm to the very residents it is meant to protect. . . These policies run directly counter to the goal of increasing housing stability and fairness through HUD-provided housing, which is all the more critical in light of the devastating housing crisis facing our nation."[51]

Initiatives such as the Facial Recognition and Biometric Technology Moratorium Act and facial recognition bans more broadly are crucial in protecting tenants from the invasive harms of surveillance technology. Yet again, these do nothing to curb existing non-facial recognition CCTV cameras already installed in public housing. They also do nothing to address the widespread use of surveillance in privately owned housing. It is indeed legal for landlords to utilize surveillance cameras in common areas of rental properties. However, according to tenant law, when camera use is mobilized with bad intent or used incorrectly it can constitute a form of tenant harassment.[52] Indeed, per the Rent Ordinance Section 37.10B (a)(13), "No landlord, and no agent, contractor, subcontractor or employee of the landlord shall do any of the following in bad faith" can "interfere with a tenant's right to privacy."[53] Similar ordinances exist in other cities such as Oakland. Landlords may not install cameras that allow viewing of interior spaces that warrant a reasonable expectation of privacy, such as bedrooms and bathrooms. That said, landlords are legally allowed to place cameras in hallways, shared entryways, garages, and laundry rooms since there is no expectation of privacy in such spaces. Technically, landlords cannot point cameras at front doors or inside homes, yet this does indeed happen. If it does, it can be a case of harassment in violation of legally enshrined tenant protections. Several mechanisms in

mechanisms in California's legal system enshrine privacy rights, such as California's Invasion of Privacy Act which originates as a wiretapping law and has found increased scope as a regulation of eavesdropping technologies more broadly (see Chapter 6 for more detail).

It is next to impossible to get a sense as to how widespread the use of privately made cameras by private landlords is in San Francisco and beyond, and there has been little done to monitor or regulate such use. We do know that landlords have been using surveillance cameras for decades, and that use of high tech systems and "digital doormen" entry systems has proliferated in recent years, which we detail throughout this report. We also know that there is precedence for regulating private use of technology in tenant housing, as recent battles against Airbnb and tenant screening systems in San Francisco and beyond have made clear over the last decades.

We go over policies and regulations related to surveillance cameras more extensively in Chapter 6, and we study the implications, geographies, and landlord tech companies related to new privately deployed surveillance technologies and systems in Chapters 2 and 3. In Chapter 4 and 5 we explore harms and battles related to Airbnb and tenant screening. Here, we conclude this chapter by detailing what it is like to live with landlord imposed cameras in privately owned housing. We offer several tenant experiences of having both neighbors and landlords install cameras that can (and sometimes have) led to eviction.

Roger

Roger Marenco grew up on Shotwell Street in the Mission and was interviewed for the 2001 film Boom: The Sound of Eviction, directed by Francine Cavanaugh, Mark Liiv, and Adam Wood.[54] The film is a testimony to the gentrifying impacts of the late 1990s and early 2000s Dot Com Boom, in which neighborhoods such as the Mission became decimated by tech capital and corollary evictions. In the film, Roger describes how his new neighbor installed a camera to spy upon him and his family, leading to his family, including 11 children, receiving a nuisance eviction notice.

"She came in here with anger, and with sort of an attitude towards the entire community. She put this huge fence right here. . . If you look up there now she has cameras up there looking at us right now as we speak. . . She went to our landlord that we were kids being a nuisance, like we were making too much noise, there was too much garbage, we were too loud and stuff like that. So our landlord thought that he could step in real quick and evict us. He gave us an eviction notice. It made me feel bad because you know, nobody deserved this. Nobody in the family deserved this. We've been living here the past ten years. It's not right for one person to come in with a whole bunch of money and think that they can screw up an entire neighborhood. My little sister's nine and my little cousin's ten - they knew what was going down. They knew what eviction was. They knew what was going to happen if we did get evicted. As the oldest of my siblings, I decided I was going to take charge and I wasn't going to let nobody push my family around. I mean if it was just me

being here by myself, I wouldn't care, you know, because I can just go with one of my friends, or one of my relatives. But I mean, where's the family going to go?"

Yet Roger, empowered by a mighty Mission District tenant movement, fought back. As he described at a demonstration against his eviction: "We're organizing the community, we're having a community protest against the landlord from this building right here, his name is Jim Korge, he works around the corner on 24th and Folsom Street. We're going to go boycott his store, tell him you know, we're not going to come here no more." Roger and his community presented his landlord with a tree decorated in notes saying, "Do not uproot us," alongside pictures of the eleven kids there that Korge evicted. This, alongside other Mission-based anti-eviction organizing, proved effective. Four months later, Roger and his family had defeated the eviction and gained the right to continue to live in their home.

While this victory story speaks to the power of tenant organizing, it also offers insight as to the relationship between surveillance and gentrification. Years later, in 2014, Alex Nieto was murdered by four Mission District police officers after a handful of gentrifiers new to the neighborhood reported him to the police for shadow boxing on his work break on Bernal Hill.[55] As we explore later in this report, today "digital doormen" cameras as well as platforms such as Amazon Ring cameras, Nextdoor, and more help automate these snitching processes–which can both lead to policing and evictions.

In what follows here we highlight a couple other tenant experiences of having cameras installed by their landlords in their homes without their consent. The following examples trace anxieties and eviction possibilities instantiated by this process.

J

Here we outline the story of J, who describes what it is like to have seven cameras set up by her landlord in her Mission District home. The following is based upon a press conference that Landlord Tech Watch held in 2020, in which she presented a video walkthrough of the cameras in her home. We also provide an illustration of her experience here to help map out what it is like to have numerous cameras installed by one's landlord in one's home:

> "After years of trying to evict me or get me to move out, the landlord installed seven — I thought it was six, but just yesterday I discovered another one — so seven known surveillance cameras in and around the building. So when the landlord installed the cameras, he didn't ask for my consent to install them and nor did he tell me how the data was going to be used."

> "This is a very secure building, there were no break-ins or burglaries which precipitated the landlord installing the cameras. It's an upscale neighborhood. There

are multi-million dollar homes on this street. And in the last nine years, maybe I've seen one police car on the street. But despite the landlord's claims, the motivation for the cameras is to capture something on the camera that he can use to evict me. These surveillance cameras - this is the latest in landlord eviction technology, it's designed to collect data and information to evict."

"The installation and the cameras really has made my home uninhabitable. Oh, it's triggered a PTSD reaction and is subjecting me to harmful electromagnetic fields."

"On Wednesday, I will be facing off with my landlord in an arbitration hearing and his attorney has claimed up until now that the cameras were installed for my security - but my biggest threat of security has been my landlord."

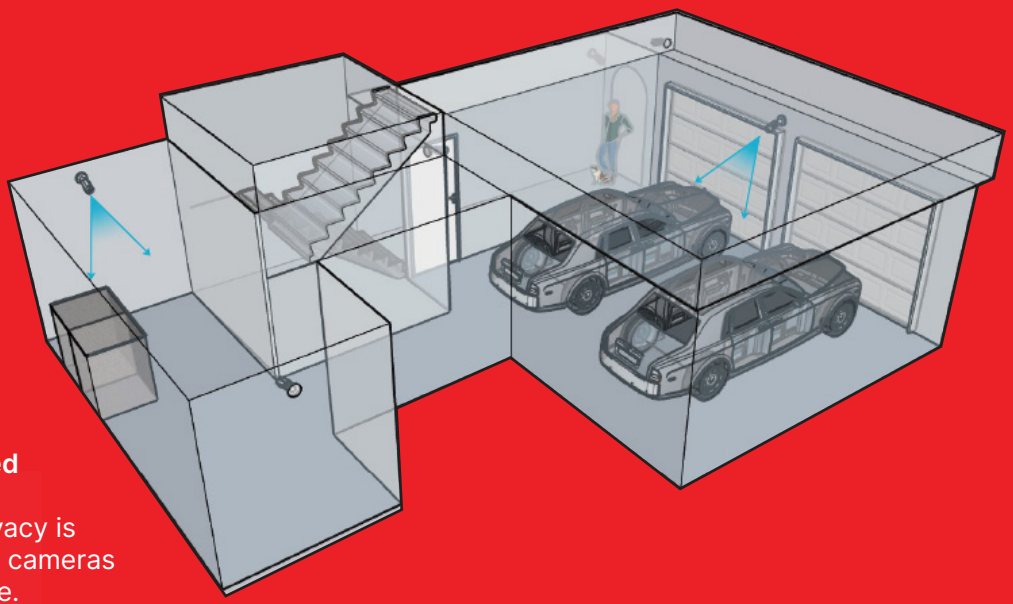


Figure 1.
A diagram of cameras installed in J's house.
Areas where privacy is compromised by cameras are shown in blue.

Veritas

Veritas Investments, Inc., owned by Yat-Pang Au, is currently San Francisco's largest landlord. The company controls hundreds of shell companies and multi-unit properties, many managed by GreenTree Property Management. Through the RentSFNow website, Veritas markets furnished apartments to transitory renters, thus evading the rent stabilization associated with long-term tenants. In 2020, 106 renters in San Francisco sued Veritas for harassment through construction and other tactics.[56] Hundreds of Veritas tenants in SF, Alameda, Oakland, and Los Angeles have joined the Veritas Tenants Association (VTA), the statewide union of renters living in Veritas buildings. In late 2021,

VTA members in SF engaged in a five-month debt strike to win commitments from Veritas on rent and shadow-debt relief. While Veritas's abusive practices are in and enough to organize against, tenants are increasingly also subjected to new surveillance tactics.

During the pandemic, Veritas began using an online virtual rent-payment system, Yardi, mandating tenants interact with their "landlord" digitally. This made things harder for tenants who prefer to pay with paper checks or who are not able or comfortable using digital payment platforms. Veritas has also installed "digital doorman" cameras made by the NYC-based Carson company (which we investigate further in Chapter 2). Tenants have recently speculated that Veritas will likely try to "pass on" the costs of installing Carson to tenants, who were never given a say about having to use this new technology.

Veritas buildings are also replete with cameras generally made by AEC alarms, which is run by Yat-Pang Au's brother. Prior, it had been run by Yat-Pang Au himself. These systems are generally composed of a network of security cameras with a bank of monitors in the manager's unit. Tenants are unable to access this footage, and are left scared about how data collected about them might be used. Even when tenants have filed a police report to get access to the footage, they haven't successfully been able to obtain footage. While some tenants want the cameras because there is some package theft, most don't want the cameras there at all. Many of the cameras allegedly don't even work, tenants have reported.

Veritas has attempted to evict tenants for lease violations based upon camera footage. Several years ago, they hired a private investigator to assess if certain tenants still lived in their units or if they had left and were illegally subletting them out. While no tenants were caught for this, the culture of surveillance creates an ongoing state of paranoia amongst many tenants.

Veritas is far from the only corporate landlord resorting to these surveillance tactics. Companies such as Mosser, Trinity, and Ballast use similar platforms and tactics to augment their corporate tactics of landlordism.

Tenant Testimonies

Below we include quotes from San Francisco tenants who have reported their experiences of cameras in their homes through our Landlord Tech Watch survey.[57] Here we include a few anonymized highlights in order to give a better sense of how increased surveillance impacts lives and communities.

These examples illustrate how commonplace yet intrusive surveillance cameras are when installed in one's home. Some also illustrate that despite the supposed alibi of increased security, tenants report feeling less safe due to surveillance. Other tenants report that the increased surveillance doesn't even work.

It (the camera) is targeted at me. Landlord tried to evict me, but he had no evidence, because there was none, so he installed cameras in February to catch me doing something evictable. Monitor is in the agent's apartment just below mine, in a 2 apartment building. I live alone.

The LL also installed surveillance cams about a few weeks after my taking possession of the apt.; he never once did he mention, announce, and/or propose the installation of these cameras; they just appeared suddenly. This instigated me to place cams atop my apt door, as there are NO security cams in my hallway.

We have had intermittent issues with our landlord over the course of our tenancy (accusations of us smoking, monitoring our comings-and-goings with a security camera)... she has been accusing us of various acts which we did not commit almost on a daily basis and has threatened to go to the SF rent board several times.

I noticed that the landlord surreptitiously installed two hidden cameras in the garage, one facing the laundry area and the other facing the entrance hall to the garage, which is the only way for all tenants to get in and out. The landlord has his own entrance on the second floor, and he usually doesn't need to pass by downstairs. The landlord installed the above two cameras without the consent of the tenants downstairs.

There is a speaker in the kitchen and a camera in the bedroom.

Landlord just installed a Google Nest camera through Dish TV because Dish TV scared my elderly landlord into thinking dangerous 'looters' will be destroying the property. We've never had any problems, and yet still the landlord got scared. Now there is a camera outside of my bedroom window.

We continue to have break-ins despite the cameras. True change would involve having keyless locks that can't be picked.

2
DIGITAL DOORMEN

The subset of landlord tech known as “digital doorman” refers to a virtual doorman service that remotely controls building access, provides property surveillance, and manages visitors and deliveries for apartment complexes. These services are advertised to facilitate a seamless user and managerial experience, with key features of digital doormen tech including: smartphone building and unit entry in place of tangible keys, video calling for guest access, door release logs with time stamped photos, and voice controls–– consolidating building access and control onto a single mobile app.

In this chapter, we look at how digital doormen increase the power of landlords while disempowering tenants and contributing to housing injustice. As property surveillance tech companies boast results highlighting profit increases for landlords as well as increased security, the demand for digital doormen has spread from coast to coast. The adoption of digital doorman services in renters' homes in San Francisco threatens to exacerbate existing contexts of housing precarity by violating tenant privacy and enabling unjust evictions.

Digital doorman companies market themselves primarily as security providers, but have found additional success in their ability to cut spending costs for landlords through automation. The services they provide are also attractive to renters who value the digitized access model as an amenity. However, there is a stark difference in how this tech is employed on the basis of rental demographics. Higher paying tenants are marketed the safety and luxury benefits of a digital doorman, while affordable housing complexes and lower paying tenants are often not made aware of these changes to quietly increase landlord surveillance capacities. In making this transition, landlords are able to increase their surveillance capacity even further by remotely monitoring the behavior of their tenants. As the landlord-tenant relationship becomes increasingly digitized and obscured, this creates obstacles for tenants wishing to file complaints, organize against their landlord, or protect their general privacy.

Landlord-tenant dynamics have shifted drastically in the wake of corporate landlordism. The 2008 stock market and housing crash made available to large investment firms a surplus of cheap, foreclosed upon single-family homes to build a new rental market. Today, tenants often do not know who their landlord is, given that the Wall Street and corporate investment company landlords increasingly hide behind shell companies.[58] As such, tenants are often left confused as to how to hold these entities accountable through reports, complaints, or organizing. This shroud of uncertainty is accelerated by digital property management apps such as Buildium or AppFolio, commonly used by institutional landlords to handle rent payment, work orders, maintenance reports, while collecting atypical "convenience fees" that are nearly impossible to contest, as well as collecting rent tracking and tenant tracking data on their residents.[59] While other scholarship has investigated the trend of increasing virtual property management platforms and what some call platform real estate,[60] here we look at the rise of doormen, which often integrate with virtual property management applications and services.

In what follows, first we examine the trend of increased corporate landlordism from 2008 into the pandemic. Next we trace findings on digital doormen and alarm companies in San Francisco. Lastly, we profile select companies that we have found to be widespread in San Francisco.

Corporate Landlordism

Corporate landlords have more resources and tenant information at their disposal than ever before, driving their focus to profit maximizing rental price increases––typically at the expense of tenants, indirectly by cutting property management costs, or directly through evictions, as shown through a study in Atlanta that found that corporate landlords were 8% more likely than small landlords to file eviction notices.[61] This pattern of eviction and housing injustice disproportionately impacts BIPOC communities as home ownership rates are the primary driver of wealth accumulation, and therefore the racial wealth gap in the United States. Because of the gap in racial demographics and home ownership, tenant abuses faced at the hands of corporate landlords is one that reproduces racism. According to congressional subcommittee data, corporate landlords are purchasing homes in neighborhoods where the percentage of Black residents is over three times their level of representation in the US,[62] profiting off of racist, segregationist housing practices that historically devalue homes in Black neighborhoods.

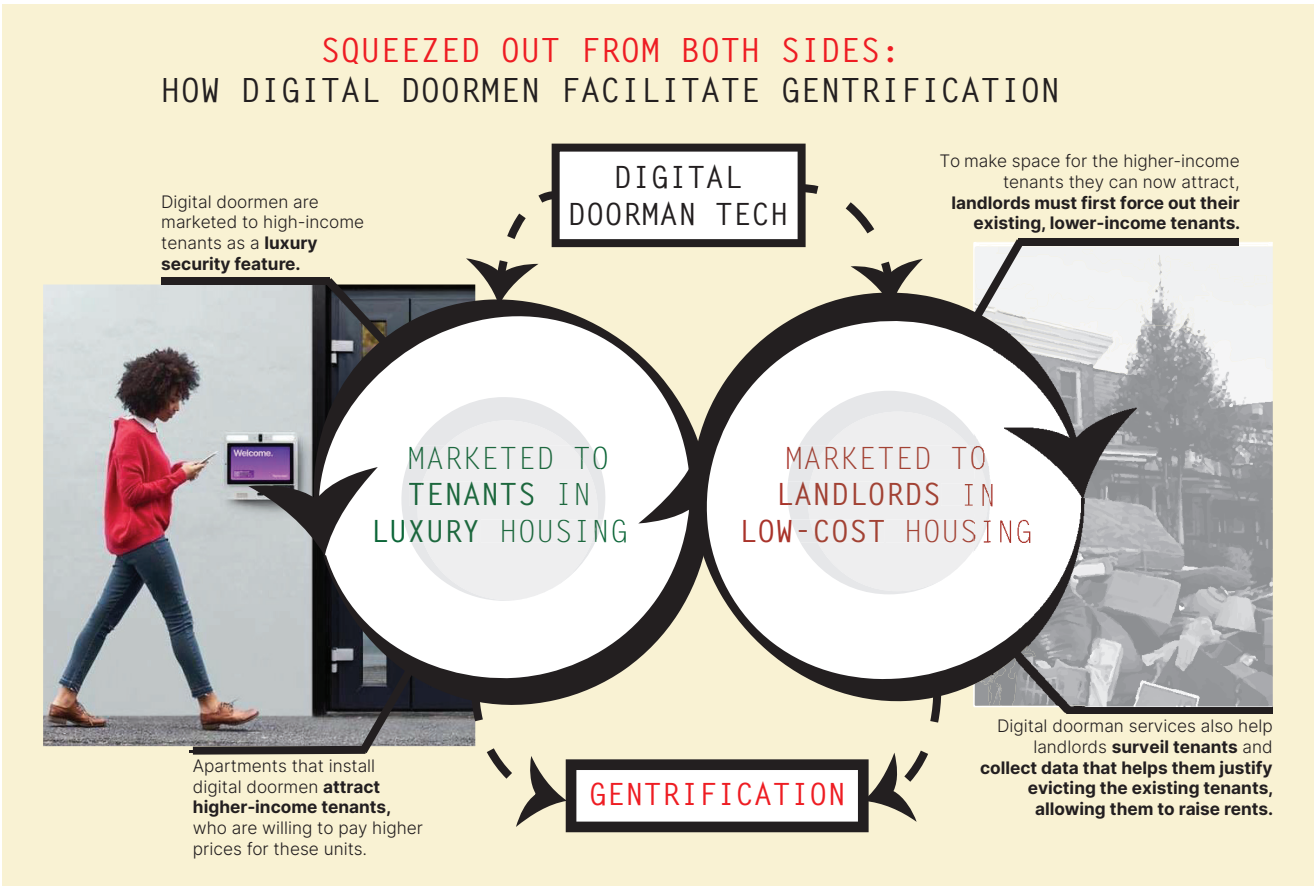
These predatory trends have continued to capitalize on pandemic-related financial vulnerabilities as well, evicting tenants at three times the previously recorded public data despite Covid-19 eviction moratoriums. Corporate landlord tenants additionally faced rent increases during the pandemic, contextualized by a record-setting quarter for investment firms with the purchase of over 90,000 U.S. homes.[63]

As corporate landlords continue to increase their scale and scope across the country, their abusive practices are made possible in part by the landlord tech at their disposal. Property management apps have been used to create a wall of bureaucracy preventing landlord-tenant communication, and digital doorman technology yields a high harm potential for tenants to be placed in even more surveilled environments.

In the context of the housing crisis and continued gentrification occurring in San Francisco and the Bay Area, the proliferation of digital doormen must be analyzed in terms of its harm potential for tenants. Marketing research from the popular digital doorman company ButterflyMX shows that luxury-based amenities were preferred among higher-paying tenants over convenience-based amenities such as parking lots.[64] As digital doorman technologies increase in popularity as a luxury good, landlords can utilize this tech to quickly increase rent prices and catalyze gentrification by catering to a wealthier demographic. Having laid the groundwork for gentrification, digital doormen then also provide landlords with the tenant data necessary to evict current residents–often serving as a workaround for eviction moratoriums or protected housing.

SF Alarm Company Data Findings

Of the home security systems companies registered in San Francisco and the Bay Area, the most popular companies share common threads in their advertising techniques, products, and AI analytics that have the potential for misuse if landlords install them as digital doormen. Property surveillance products are advertised to provide security and



peace of mind to both tenants and landlords, but, more specifically to San Francisco and the integration of tech and lifestyle products, they are pushed as a necessity in the realm of smart homes. The ability to stream security footage on your phone, monitor package drop off, as well as replace keys with digital locks and codes, all work to streamline the residential experience while simultaneously expanding the data available to landlords or tech companies at the expense of individual privacy.

The smart home market is only projected to grow in the coming years. It is currently worth $31.45 billion in the US, with a projection of $52.19 billion by 2027.[65] Within the smart home market, the security and surveillance segment is the highest earner, making up 31 percent of the total revenue.[66] During the COVID-19 pandemic, demand increased for smart tech products to curb the spread of the virus, such as video doorbells for homes to reduce in-person contact, or AI mask-detection cameras for businesses following mask mandates.[67] As people became acclimated to spending more time at home, consumers shifted their disposable spending priorities to invest in the security, comfort, and convenience of their homes through tech. From 2020 to 2021, home monitoring and security devices increased their growth by 13.5 percent globally, the US being the top consumer of smart home shipments with a quarter-over-quarter market growth of 9.5 percent, marking an uptick in smart home technology demand that was distinctly pandemic driven.[68]

The potential consequences of smart security technology installation in homes and

surrounding the expansion of these new technological solutions in order to immediately mitigate the effects of the COVID-19 crisis.[69] However, now that these technological infrastructures exist, personal data is susceptible to exploitation as legislation is still catching up to course correct the privacy violations occurring at the hands of tech giants.

In recent years, traditional 24/7 security footage monitoring services in San Francisco and the Bay Area have been competing with automated data analytics offered through visual AI tactics. Many smart products have their own version of this AI running already, but its accessibility has expanded to meet the needs of homeowners with dated, existing security hardware as well. Third-party companies such as Sentry AI offer their software to individuals or companies looking to bolster their security by organizing their camera footage. Sentry AI advertises the ability to detect packages, people, and cars, as well as the vague category of "suspicious activity."[70] Despite the racist history of AI technology and facial recognition that scholars such as Ruha Benjamin, Joy Buolamwini, Wendy Chun, and Timnit Gebru have importantly critiqued,[71] these new companies do not address how their services could result in inaccurate, bias-driven conclusions and perpetuate racial and gender-based discrimination.[72] As AI detection becomes a more ubiquitous tool for home security, it poses a risk to communities through false reporting, increasing neighborhood paranoia, and normalizing the use of facial recognition technology in public spaces.

The scope and character of home security and surveillance has changed drastically within the last decade, even more so over the course of the pandemic. Obtaining surveillance technology for one's home has never been more accessible, and as security systems increase in demand through less overt channels–such as luxury amenities or integrated smart-home ecosystems–their presence normalizes the existence of intrusive technologies in homes and public spaces. When installed by residents, the primary consequence of increased home security tech is an expansion of the surveillance state, but when landlords utilize this technology to manage their properties, the consequences compound into tenant monitoring, privacy violations, and increased evictions.

SF Digital Doorman Company Profiles

Eufy

PRODUCTS security cameras, video doorbells, wall light camera, smart lock, integrated security
FUNCTION remote property access control, video security, fingerprint and facial recognition, motion detection, package detection
LOCATION parent company Anker Innovations is headquartered in Changsha, Hunan, China
FOUNDING DATE 2016

Eufy advertises their 4G LTE camera as a tool to "see more of your surroundings to better protect your property" and "filter up to 95% of false alarms with built-in AI."[73] Eufy's Video Doorbell 2K "intelligently detects body shape and face pattern" using a "sophisticated algorithm" to "ensure you are only alerted when a human, and not a stray cat, is at the door."[74]

Eufy infamously compromised the security of individuals detected by its cameras by uploading camera data to cloud storage rather than local storage.[75] While the compay claimed all data was stored locally with no cloud access, an investigation by security researcher Paul Moore revealed that the images and videos were uploaded to Eufy's servers leased through Amazon Web Services (AWS) and were accessible through an incognito server.[76] Thumbnails uploaded to the cloud server displayed facial recognition data associated with user ID numbers.

In May 2021, users were suddenly given nearly full access to other users' accounts and video feeds. Eufy later admitted the feeds were never encrypted, claiming they had begun fixing the issue by updating cameras to use WebRTC, which contains default encryption.[77]

SimplySafe

PRODUCTS smart home security system, indoor/outdoor camera, video doorbell, smart lock
FUNCTION allows remote monitoring from mobile app and video motion detection and interaction; recognition AI to differentiate between pets, cars, and people
LOCATION Boston, MA
FOUNDING DATE 2006

SimpliSafe's flagship product, SimpliCam, detects motion at a property and alerts the user, who can then decide whether to record video. Recordings stay in encrypted storage for 30 days:

> "SimpliCam was built with a stainless steel privacy shutter to give you complete control over your privacy. The privacy shutter only opens with your permission. It protects your video feed with the same level of encryption used by banks to protect their accounts."

> "Alarms that cry wolf? No thanks. We precision-engineered our Motion Sensor to detect the unique signature of humans. Not pets... when motion is detected it sounds the alarm."

A new beta feature will allow monitoring agents to talk to intruders if the motion alarm is set off.[78]

Lorex

PRODUCTS remote security system for home and business; indoor/outdoor camera, video doorbell, smart lock
FUNCTION remote property access and control with motion detection, facial recognition, and 2-way communication
LOCATION founded in Canada; currently owned by Dahua, headquartered in China
FOUNDING DATE 1991

Lorex's proprietary smart motion detection software includes person and vehicle detection, and a facial recognition feature that notifies the user through the mobile app. Lorex touts their cameras' "stunning 4K clarity" and "vivid Color Night Vision."[79] Addition crime deterrence features include warning lights, sirens, and two-way communication.

Lorex's online privacy policy contains disclaimers about their cloud recording practices:

> "We do NOT have access to Video Data. Your Video Data is encryped, stored locally in your device and inaccessible to us. Neither we nor our service providers have direct access to your Video Data unless you disclose it to us with your consent for the limited purpose of prividing support services to you in connection with Lorex Solutions ... References to "cloud-enabled" Lorex solutions refers to the tranmission of video data from your recording device to other devices."[80]

Essentially, it is at the user's (landlord's) discretion whether to provide Lorex with video data access and what should be done with any findings contained in video data. Recordings and thumbnail images are encrypted and stored on the cloud for up to 7 days before being permanently deleted.

Doorbird

PRODUCTS video door stations, access control systems, cloud recording subscription, individualized security solutions
FUNCTION video doorman; visitor and package detection, mobile notification, property access control, cloud visitor history
LOCATION Berlin, Germany
FOUNDING DATE 2014

Doorbird's rapidly scaling video doorman now has over 100,000 users in over 160 countries:

> "Stranger in the night: With our IP video door station ... the home owner sees immediately who is in front of their gate. Individual PIN codes can be assigned via the DoorBird app, allowing family members keyless access."[81]

Doorbird's Open API allows for integrations with third party user solutions through LAN-based API access, and with cloud API for integration partners.

Virtual Doorman

PRODUCTS Virtual Doorman (building system integrating surveillance and access control), Virtual Guards (corporate security solutions)
FUNCTION virtual concierge, building security (video surveillance, intercom, remote access control), building management platform
LOCATION New York, NY

Virtual Doorman digitizes building security, and in doing so sells property managers access to remotely captured video of their properties. While the company touts the ease of access for residents, visitors, or delivery personnel who can connect to a virtual doorman "within seconds of pressing the call button," in detailing the video storage implications of this technology they make it clear that the only privacy safeguards are at the discretion of landlords.[82]

> "All activity is recorded and can be retrieved and reviewed as needed ... [making] it easy for property managers to stay on top of what's going on in their buildings."[83]

Virtual Doorman offers several payment tiers for their services. Depenging on which tier a property manager purchases, they allow for different amounts of video investigation retrieval per month, from 30 minutes up to two hours, as well as varying levels of personalized service. It is unclear whether any encryption or other security measures exist to protect tenants' data.

Q5iD

PRODUCTS Know Your Employee (KYE), Business (Proven Identity Solution), and individual security (Guardian)
FUNCTION Cloud-based biometrics authentication, fraud prevention, liveness testing
LOCATION Hillsboro, Oregon
FOUNDING DATE 2018

Q5iD has tried to position itself as a revolution in biometric IDing by demystifying their encryption method and presenting it as non-threatening and secure:

> "KYE by Q5iD goes beyond traditional ID verification by providing the identity of the person, not just verifying the provided ID ... Face and palm biometrics are converted into a character string using a hashing algorithm and that algorithm cannot be reverse-engineered."[84]

Natix

PRODUCTS virtual doorman, parking spot monitor, crowd density detector, zone security supervision
FUNCTION combines AI processors to camera through installed software to track changes
LOCATION Meadow Vista, CA
FOUNDING DATE 2012

Natix provides AI-enhanced surveillance solutions for property managers and event venues, with a recent focus on COVID-19 compliance monitoring. Their proprietary digital doorman features include mask detection, maximum occupancy monitoring and entry control, and SMS communication to administrators in the event of violations.[85] For events, they offer crowd density features such as analyses and heat maps to show crowd position, movement, and behavior.

Natix's core technology is an event detection AI that allows from customizations. The deployed AI automatically trains and detects on side nodes, and combines with compatible camera hardware. Anonymity is offered as an add on in cases where human review is relevant.

While Natix does not advertise its crowd density features and other AI enhancements as relevant to residential landlords, it is not hard to imagine how these features could be used in residential buildings in combination with cameras to surveil potential organizing efforts and collect evidence of unauthorized gatherings to use against tenants in eviction proceedings.

Carson

PRODUCTS virtual doorman
FUNCTION digital doorman and app-based property management platforms
LOCATION Headquartered in New York City
FOUNDING DATE 2017

Carson was started by a group of property management software and hardware industry executives seeking to provide a one-stop "full service lifestyle to unstaffed buildings, at an affordable price."[86] To streamline its services, Carson has partnered with Comelit, an intercom provider, and SMARTAir, an electronic key provider for multifamily properties. Carson is primarily marketed to smaller buildings, offering an integrated property management experience similar to those larger buildings have, but tailored to the needs of a smaller community. During COVID-19, Carson has also started promoting its products as necessary to prevent package theft.

As of 2019, Carson software was in use in at least 300 buildings.[87] Based on Instagram posts and tagged locations, Carson has been deployed in multiple cities around the world, including NYC, SF, and London.

Carson founder Guy Blachman previously founded the property management startup ActiveBuilding/MyBuilding, which was acquired by RealPage in 2013.[88]

Latch

PRODUCTS integrated building access system
FUNCTION Keyless entry, guest management, and package deliveries
LOCATION Headquartered in New York City
FOUNDING DATE 2014

Latch is a major player in the digital doorman industry. Rather than speaking directly to landlords in its marketing materials, Latch promotes itself as a service for residents, describing its product as:

"A full building access system that allows you to leave your keys behind and unlock doors with a smartphone ... additionally, you can easily share access with your friends, family, and services like cleaning by sending them Doorcodes via the Latch App. The Latch Lens also takes pictures of your guests to provide a history of who entered your space and when."[89]

No systems are present to confirm that cleaning staff and other service providers entering a user's home have consented to be photographed.

Latch has a growing presence nationwide, including at least 1,000 buildings in New York alone.[90] According to their website, "today, 1 in 10 new apartments in the US are being built with Latch." Through a partnership with UPS, in 2019 Latch expanded their in-home delivery program to 10 new US cities.[91] They now work with several big names in the real estate industry, including Tishman Speyer, Related Properties, and Avalon Communities.[92]

ButterflyMX

PRODUCTS smart video intercom products
FUNCTION integrated video intercom system that pairs with any smartphone
LOCATION Headquartered in New York City
FOUNDING DATE 2014

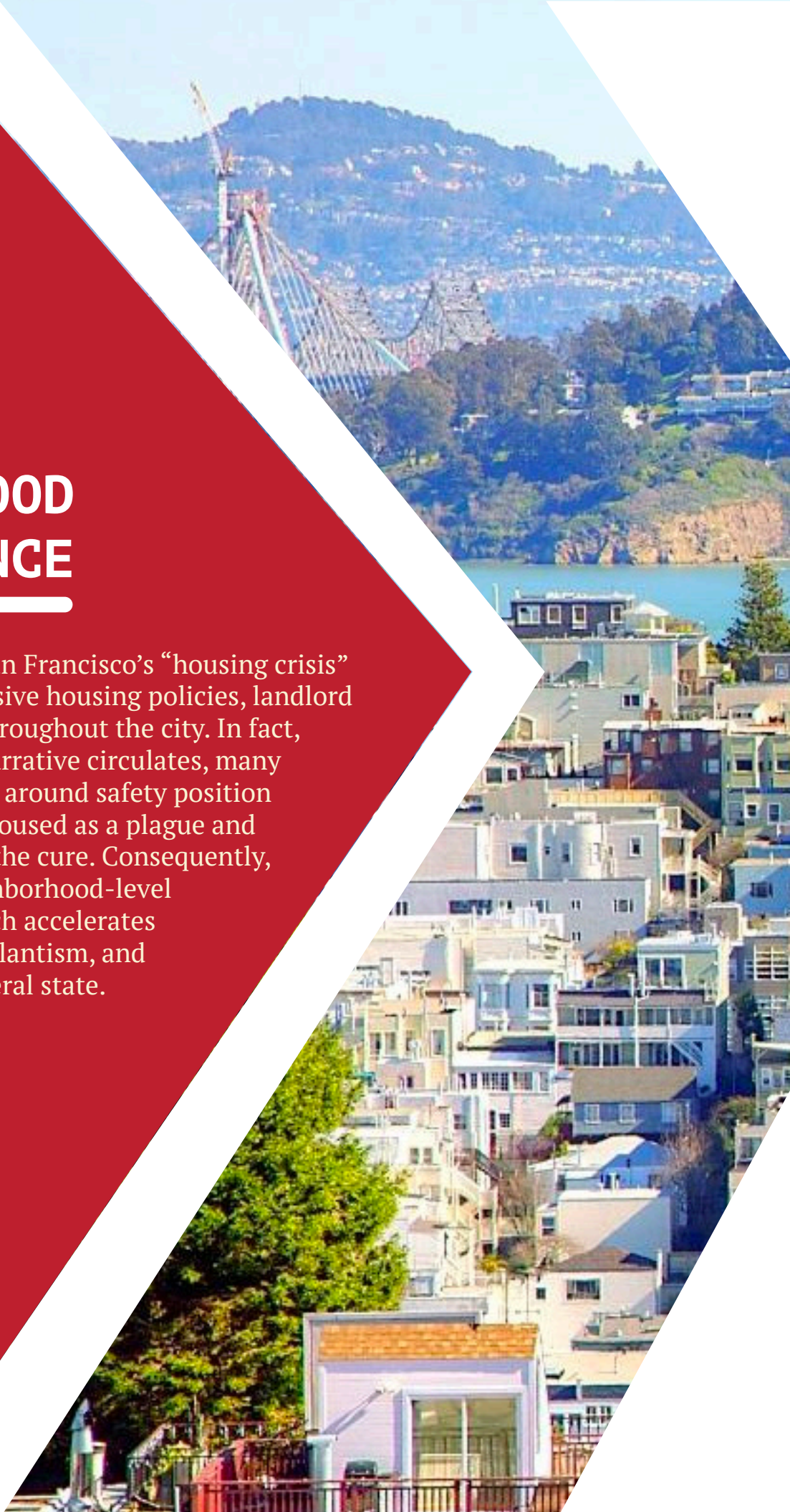
ButterflyMX "transforms any smartphone into a mobile video intercom system": once the company has installed an intercom, it allows residents to take calls from the intercom as video calls on their phones. This allows residents to "view the visitor before granting access to the building."[93] ButterflyMX's system also provides for virtual keys, messagin options, and digital timestamps, and costs roughly $5000-7000 to install depending on specifications.[94]

In 2020, ButterflyMX released a COVI-19 renter trends report in which they proposed that clients have recently shifted their priorities from convenience-based amenities to safety-based features, especially in multi-family housing.[95] Among other proposals, the report promoted virtual keys and self-guided tours (monitored by video cameras) as solutions to apartment tours during COVID-19.[96] In their vision of the future, new security threats and the need for social distancing-ready management infrastructure will necessitate the expansion of remote surveillance tech.

ButterflyMX serves over 5,000 properties worldwide, including multifamily, commercial, student housing, and gated communities. They have a presence in numerous big names in the real estate industry, including Jamestown Properties and The Chelsea Apartments in NYC and Avalon Communities in San Francisco.[97]

3
NEIGHBORHOOD SURVEILLANCE

As the media fixates on San Francisco's "housing crisis" and the city enacts regressive housing policies, landlord technology proliferates throughout the city. In fact, as this abstracted crisis narrative circulates, many community conversations around safety position people who are living unhoused as a plague and increased surveillance as the cure. Consequently, a complex system of neighborhood-level surveillance emerges which accelerates policing, extrajudicial vigilantism, and the expansion of the carceral state.



From private home cameras to online platforms such as Nextdoor, technology on this scale is redefining the housing landscape in San Francisco and beyond. Landlords are not always the primary culprits behind this form of tech- deployment. However, landlords catalyze and then capitalize on the circumstances of this technology's use. So, the term "neighborhood" here involves a vast array of actors from homeowners to the unhoused to (corporate) landlords to other large corporations.

Surveillance in everyday spaces marks technology's role in fundamentally shifting urban systems and the entrance of large transnational corporations into them. Thus, deeply intimate community spaces become sites for capitalist extraction through gentrification. In turn, they whiten and are rendered inaccessible to residents already targeted by structural housing inequalities.

We have seen an uptick in police use of residential cameras throughout the pandemic. In 2020, for instance, the San Francisco District Attorney created a Google form allowing San Franciscans to register residential and business cameras. Users can indicate if cameras are infrared, high definition, or standard definition, where camera footage is stored, where the camera looks (ie. garages, streets, doorsteps), and more–all "to deter crime and promote public safety through collaboration between the San Francisco District Attorney's Office and the communities we serve."[98] This camera data can then be used in subpoenas.

In 2022, the San Francisco Board of Supervisors passed an ordinance allowing San Francisco Police Department (SFPD) the ability to access private security cameras, including those erected by property owners on their own property. The ordinance inaugurates a 15-month pilot program, which would allow the police the ability to "temporarily live monitor activity during exigent circumstances, significant events with public safety concerns, and investigations relating to active misdemeanor and felony violations" and to "gather and review historical video footage for the purposes of conducting a criminal investigation."[99] Certain camera systems such as Amazon Ring and Google Nest have also seen increased use during this time, as we detail below.

Home "Security" Systems

"Non-stop peace of mind" awaits future Ring users, suggests Amazon on the surveillance system's website.[100] Packaged as a seemingly benign doorbell, Ring systems have become fixtures in many neighborhoods around the US. Importantly, they represent one of the most prominent forms of neighborhood-level surveillance: the home surveillance system. This can lead to increased forms of harm for those captured through Ring cameras. As the American Friends Service Committee aptly summarizes, "Ring's policies and law enforcement relationships jeopardize privacy, lack regulation, rely on fear-mongering, and enable over-policing, increased surveillance, and racial profiling, in what the Electronic Frontier Foundation calls a "digital porch-to-police pipeline."[101]

While many are familiar with the doorbell, Ring has become an umbrella for an array of surveillance devices. These include indoor and outdoor cameras, "smart" lighting, locks, and comprehensive property "security" systems. Each has multiple models with varying degrees of sophistication and can be controlled remotely from a user's phone. Diving into the features of these systems raises many concerns. Even the most basic doorbell, for example, is capable of "person alerts," a type of motion detection.[102] Another product, home security systems connected to cameras, includes a siren function. The sound can surpass 100 decibels – comparable to a jackhammer and some car horns – loud enough to cause hearing loss. In San Francisco, this function violates section 3704(a) of the Police Code which outlaws alarms that mimic the sounds of emergency services.[103]

Another notable Ring feature is the accompanying Neighbors app. The platform allows users to share geotagged footage from their systems that, most often, is of nondescript individuals whom users accused of stealing packages or vandalizing their property. Yet, it is not just users' neighbors who are able to access this footage, but police as well. In fact, Ring offers a designated Law Enforcement portal that, according to Amazon, "allows police departments to request, obtain, view, and download Ring footage without a warrant and to store that footage indefinitely."[104]

The number of US police departments that use Rings' Neighbors Portal surpassed 2000 during the pandemic.[105] Prior to 2019, however, only 60 police departments used Ring.[106] As of 2022, San Francisco does not currently have an agreement with Ring,[107] though there have been recorded abuses of the SFPD obtaining Ring footage–including footage targeting Black Lives Matters protestors.[108] As one tenant reported in our own survey of a Ring camera installed in Potrero Hill, "A Latino man was mistaken for someone else and arrested - this is not okay."

Amazon has in recent years been awarded patents indicating a plan to introduce biometric capabilities. These could range from facial recognition to odor and skin texture recognition, as the patent suggests.[109] Yet, this intrusive level of surveillance would go further. With this technology, doorbells would be capable of scanning surrounding areas to identify "suspicious" individuals based on biological markers like gait or voice. Moreover, the "Neighborhood Alert Mode" outlined in one patent would invite users to share data related to someone they deem suspicious with other users. Consequently, local Ring systems would constantly be scanning for the suspicious person. While this is not yet being deployed in San Francisco as far as we know, it could be in the future.

Yet, the concerns associated with Ring extend beyond its functions. Its relationship to law enforcement is of particular concern. Amazon purchased Ring in 2016; prior to this acquisition, the company boasted its neighborhood surveillance capacities.[110] Ring is also known to host annual parties at police conferences and conduct extensive training for officers on how to access Ring data. This training is often performed in exchange for departments advertising the systems. For instance, Lakeland, Florida's police department received free devices for distribution to residents.[111] Cities often pay roughly $100,000 to Ring to subsidize the sale of its systems,[112] offering promo codes and other offers to residents. Ring and Amazon have also helped police departments establish package theft sting operations. This involves using "dummy Amazon packages (using tape and

boxes provided by Amazon) and putting these packages on doorsteps equipped with doorbell cameras."[113] Ultimately, all of these actions are taken with the presumption that Ring systems will prevent crime. An MIT study, however, found fault in the evidence supporting this claim.[114]

The use of Ring is particularly salient in San Francisco and has become commonplace. While the police department has yet to partner with Amazon, any barrier between law enforcement and Ring footage is slowly chipping away in the city. Yet it is not only law enforcement to blame. Neighborhood and complaint-oriented policing also play a role, particularly with increased accusations of "porch pirates."[115] An article in The Atlantic for instance describes how Potrero Hill residents conducted a witch hunt to imprison an unhoused Black woman who had been evicted from the neighborhood she once called home due to gentrification.[116] Amazon Ring systems played a central role in this: they empowered property owners to capture photos reminiscent of "wanted" posters used against the individual. Importantly, Ring is only one of many products functioning in this capacity. As the Electronic Frontier Foundation put it, "once infrastructure exists, there will always be temptation for police to use it for less urgent situations."[117]

In addition to Ring, other home surveillance systems like Google Nest. Google Nest, originally built as Nest Labs in 2010 by former Apple employees before being absorbed into Google in 2018, includes a line of smart home products including smart security systems, speakers, displays, thermostats, smoke detectors, routers, and locks. During the Covid-19 pandemic and the Movement for Black Lives that sprung up after the murder of George Floyd, Google Nest had forged a deal with Dish TV, which actively recruited property owners and landlords to install Nest cameras to protect property from the "looters" now allegedly roaming San Francisco's streets.[118] This speaks to the crisis capitalist logics undergirding landlord tech deployment.[119]

Another notable home surveillance system is Vivint, which according to documents from the San Francisco Tax Collector's Office confirm its operation in San Francisco. Blackstone, an investment firm behind landlord tech company Invitation Homes, owns Vivint in part. Following the 2008 subprime crisis, Invitation Homes purchased thousands of foreclosed single-family homes. These large portfolios, often concentrated in clusters, gave corporate landlords like Invitation Homes the capacity to control markets and rent gouge.[120] Blackstone's merger with Vivint in 2012 marks their expansion into the realm of neighborhood surveillance. It demonstrates their vested interest in neighborhood "change" and is symptomatic of the relationship between large corporate landlords and neighborhood surveillance. In the past, Vivint has partnered with Airbnb to systematize the surveillance of units listed on the platform.[121] This relationship emphasizes the mutually reinforcing impacts of different forms of landlord tech and the extent of neighborhood change.

Platform Tech: Nextdoor, Citizen

While perhaps less self-evident as a form of landlord tech, online platforms like Nextdoor also engender gentrification. Such platform tech emboldens neighborhood vigilantism,

homogenization, and policing. Nextdoor, intended as a digital space to build community, includes several functions: product reselling, sharing local news, publicizing events, advertizing lost pets, among others. One of the most significant and active features is the platform's "crime and safety" forum that echoes neighborhood watch programs. Purenne and Palierse describe this as "citizen-based surveillance" or "participatory surveillance" where communities collude with police as the result of both self-initiated grassroots and top-down government-encouraged efforts.[122] Rahim Kurwa importantly explores how the platform ultimately reifies the carceral state and entraps people in regimes of surveillance.[123]

For instance, neighbors often complain and warn one another about recent events, including property theft. These posts (i.e., Figure 1) typically include nondescript media and antagonistic messages calling for action. They also regularly characterize San Francisco as generically "unsafe." Such a framing has only grown throughout the pandemic with pro-policing and pro-development propaganda being spun to describe San Francisco as a "failed city" due to increased houselessness and putatively "dangerous" unhoused residents.[124]

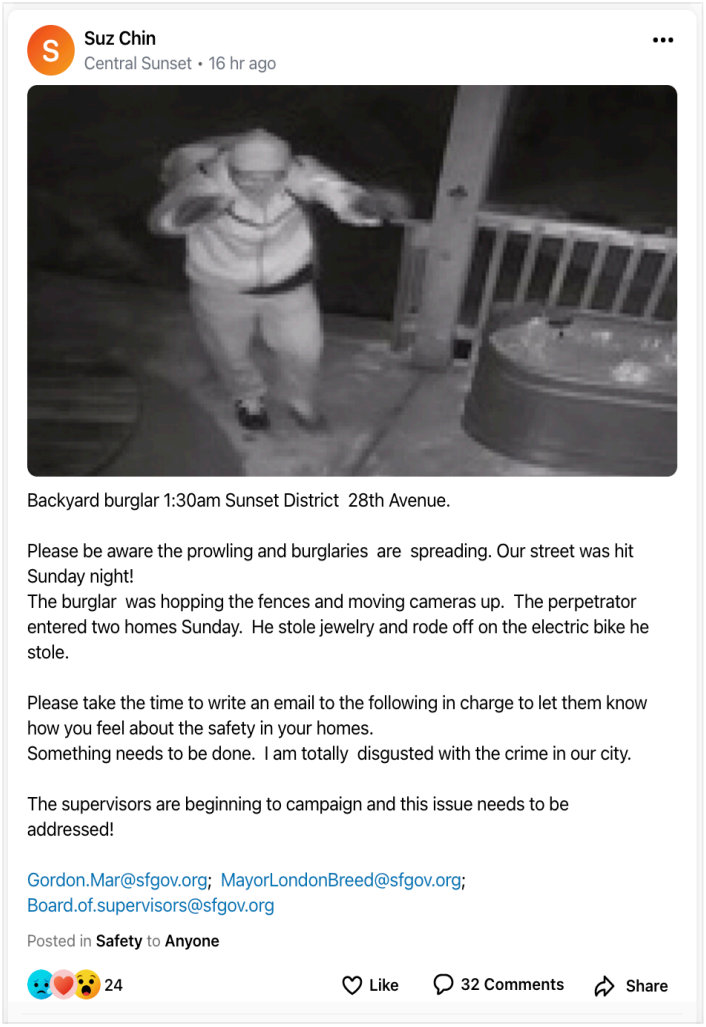


Figure 1. Source: Nextdoor.

As the Anti-Eviction Mapping Project found through survey data on its Landlord Tech Watch platform, many people on Nextdoor use the app to report on unhoused people. Nextdoor also serves as an echo chamber for racist rhetoric associating Blackness with violence. These sentiments often manifest in outing "suspicious" Black men captured on home surveillance footage. Since the app outsources moderation to individual volunteers,[125] racism often goes entirely unregulated. Neighbors usually respond with sympathy and affirm anti-homeless and racist comments. They also include sweeping statements about the contemporary *character* of San Francisco indicating the reality of platform technology's functions: it privileges and fortifies the position of those who are wealthy and housed against the unsafe *other*.

The presence of the police on Nextdoor is cause for concern. In 2016, Nextdoor added a function to allow users to directly share posts with police,[126] and it has regularly answered subpoena calls from police departments.[127] In San Francisco, the Police Department regularly posts neighborhood-wide news, polls, and updates that position it as a force for good. The SFPD often positions itself as a local hero on the platform, for instance as displayed in Figure 2 on a post written almost like a movie script, in which the agency boasts of taking "another gun off the street." The rhetoric of the post follows the following logic: 1) this gun is symptomatic of a larger issue plaguing the city; 2) the police are the one force effectively addressing this threat; and 3) the elimination of guns from suspicious individuals is the solution. In a country with sparse gun laws and in a city plagued by homicides committed by law enforcement, other faults are at play. [128]In posts like this one, more often than not, the comments are positive, affirming the police's "service" with a positive reaction (i.e., the love or happy face emoji). Platforms like Nextdoor thus normalize neighborhood surveillance and the increased presence of law enforcement in community spaces.

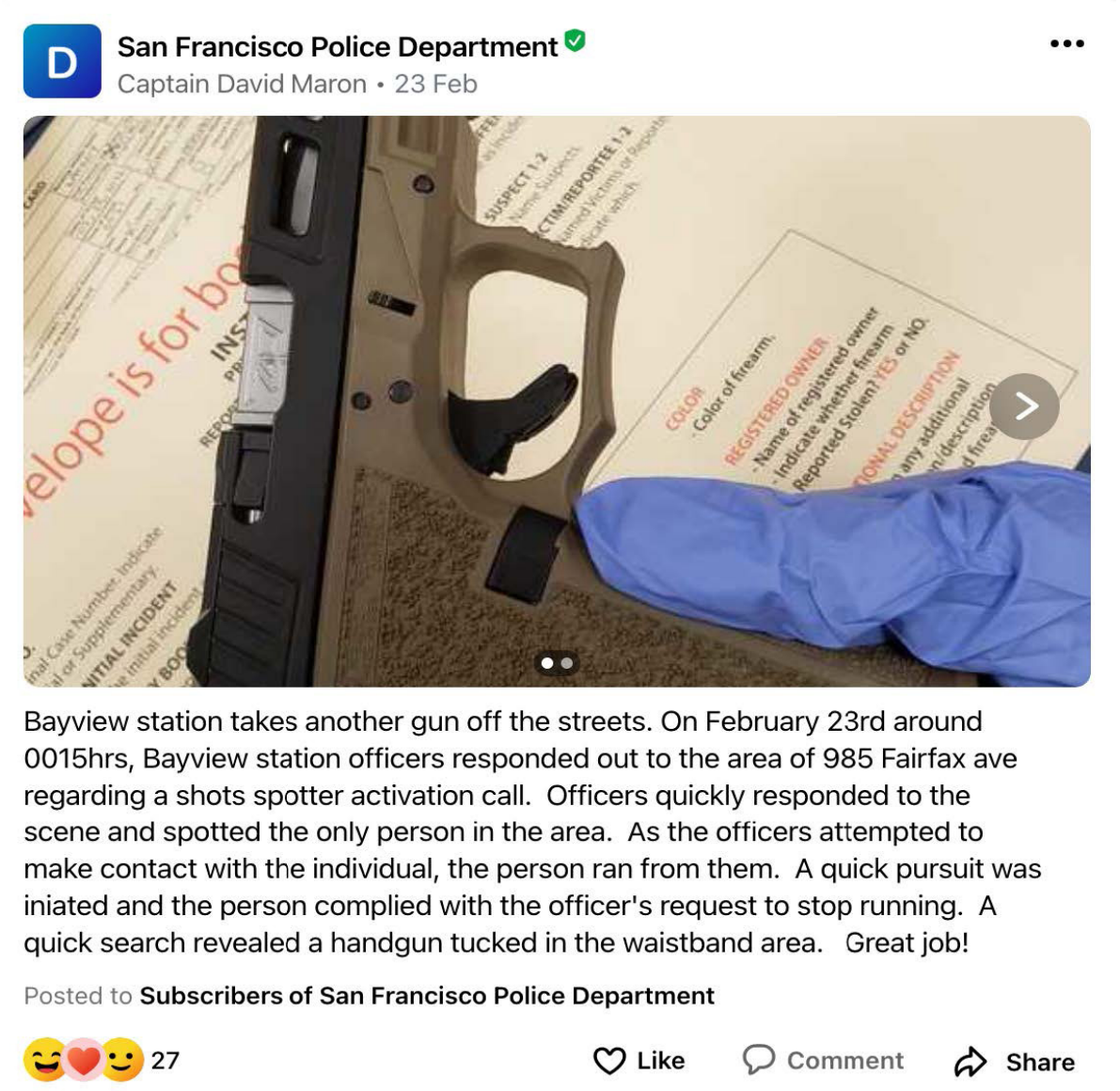


Figure 2. Source: Nextdoor.

Nextdoor is not unique. The crime and neighborhood watch app, Citizen, similarly emboldens extrajudicial vigilantism and the expansion of the carceral state into neighborhoods. In fact, the app was once called Vigilante.[129] Operating in around 50 US cities including San Francisco, Citizen employees monitor police scanner audio, send that data to the app, and bombard users with notifications of nearby "criminal" activity. Users can also report incidents, submit content and interact with others. Citizen's "around you" also facilitates direct involvement with local policing. In early 2021, Citizen capitalized on a wildfire, labeling it arson, to promote its product. The company announced a $10,000 reward–which was later raised to $30,000–for the individual who found the supposed-culprit, ideally live on the app. The vitriolic posts of the ensuant witch hunt provoked a mob of racist digital vigilantes to target an innocent Black man. This manhunt, while extreme, underlines the danger of apps like Nextdoor or Citizen: they incentivize racialized surveillance since it drives user engagement and retention.

Unsurprisingly, Citizen has forged relationships with private security services. In Los Angeles, for example, a Citizen vehicle was discovered to be part of a pilot program with the well-known security firm Securitas.[130] For a price, users would have direct access to these security services. Because the app disproportionately targets unhoused folks and people of color, the company has thus monetized racially-motivated paranoia. While it does moderate discussion, unlike Nextdoor, overt racism shapes how individuals engage with one another. The implications of such tech for neighborhood policing are perhaps best encapsulated by a comment from Citizen CEO Andrew Frame: "This is tech closing in on you. Good luck buddy." Thus, like Nextdoor, Citizen emboldens individuals to essentially become a branch of law enforcement.

The use of this witch hunt-like neighborhood surveillance technology is not uncommon in San Francisco. For instance, Lauren Smiley details the hunt for a "porch pirate" in the Potrero Hill neighborhood.[131] Ganave Fairley was first caught taking packages in 2016 by a homeowner's surveillance camera. The residents, once several of them identified her, took to Nextdoor to chase her down. One neighbor posted wanted photos of her, while another actively began to organize community members to get her arrested, while others began harassing her. One even grabbed a box from Fairley that they suspected she had stolen. For individuals like Fairley who have prior offenses, minor actions like this can spell larger jail stints.

4
AIRBNB AND PLATFORM TECH

While a variety of short-term rental (STR) platforms exist in the Bay Area, here we follow Airbnb's influence on cities and the regulations enacted to reduce harms propagated by the tech giant.

As the story goes, the idea for Airbnb (formerly Airbed and Breakfast) sparked in 2007 when two of the three founders, Brian Chesky and Joe Gebbia, invited strangers to stay at their apartment on air mattresses during a design conference. The two had been brainstorming ideas to make money to pay their expensive San Francisco rent when they landed on an idea to offer a bed-and-breakfast-esque experience amidst costly or unavailable traditional hotel rooms in the city. Jump forward a decade and a half, and all three founders are now billionaires heading a ballooning global platform. Although their start-up idea was entrepreneurial, the company has had a significant negative impact, with many displaced people and increased housing costs since its inception. It's rather ironic that the company was started as a way to make rent, while millions today struggle as a direct and indirect result of their solution: Airbnb.

In this report, we consider the Airbnb platform as a form of landlord tech because landlords use it to fill living spaces (i.e., houses and apartments) for short periods at the expense of long-term tenants.[132] In this section, we examine efforts to regulate Airbnb and propose that studying such regulation could serve as a valuable framework for conceptualizing the regulation of landlord technology more broadly.

Along with Uber, Lyft, and TaskRabbit, Airbnb helped pave the way for the so-called "sharing economy," in which goods or services owned by others are shared for a price. The Saïd Business School at Oxford University defines the sharing economy part of the proptech (what we describe as landlord tech) boom, which they also attribute to fintech, smart home devices, and venture capital. They define the sharing economy as "distributed ownership of a resource [which] enables individuals to split the use of things like cars, houses and other spaces, or to hire personal and real property assets to other intending users," but definitions of this abstract phenomenon are varied.[133] In the case of Airbnb, the sharing economy's poster child, households can participate in this peer-to-peer model by capitalizing on "underutilized space."[134] However, neglecting to acknowledge the commercial landlords who act as "Hosts" or those who manage multiple listings overlooks the significant capital supporting the platform's usage.

Short-term rental platforms incentivize the displacement of renters on a large scale because higher revenue is possible in a shorter period of time than rent (profitability). Additionally, short-term rental platforms, like Airbnb, are prolific in part due to their scalability, availability of private spaces (supply), and of people looking for places to rent (demand).[135] The accessibility of Airbnb via an app increases its potential for integration on a global scale. That being said, its digital nature also makes it more difficult to regulate and enforce. Even so, there have been multiple efforts to curb its abuse, as we map out here.

Airbnb in San Francisco

Airbnb began as a short-term rental service, defined by the San Francisco Board of Supervisors as "rentals of housing units or rooms for less than 30 days."[136] Airbnb's service allows "Hosts" to rent out rooms in their homes to guests. Since its launch in San Francisco in 2008, Airbnb has grown into a multi-service company offering entire apartment and house rentals, "trips," and even in-app restaurant reservations.[137] Airbnb has a vast global footprint, operating on every continent and in numerous cities worldwide.

Even in the aftermath and uncertainty invoked by the COVID-19 pandemic–a particular challenge for the tourism sector–Airbnb's net worth reached around $113 billion as of 2021, a more than fifty percent increase since 2020 alone.[138] While this figure is staggering and debatably inflated, it nevertheless represents investors' zeal for tech and their ability to tolerate loss.[139] As of 2022, the company boasts 7 million listings (660,000 of which are in the US) and 2.9 million hosts, globally.[140]

Airbnb seems to place a heavy emphasis on living in the places where their guests travel. An authentic experience is a big selling point and one of the key characteristics that the brand uses to differentiate itself from other traditional hotel/bed-and-breakfast stays. Particularly in its early years, the company aimed to normalize staying in lesser-known, non-touristy locations with strangers. In April 2016, Airbnb launched its "Live There" campaign with the slogan, "don't just go there, live there, even if just for a night."[141] But what happens when a guest's authentic experience results in less housing for local residents? What happens when an unregulated or underregulated company's profit depends on property and the displacement of people? What happens when touristic fantasies and far-off imaginations entangle with tech and collide with real life?

As a Silicon Valley "unicorn" company–a privately owned startup valued at over $1 billion–and disruptor of the tourism industry, Airbnb's reach is unprecedented. The motivation to experience space and place authentically might originate as a rebellion against traditionally curated tourist paths: guided, safe, insular, and safe. Yet, the form of travel that Airbnb offers is not revolutionary; it is commercialized and popularized. With Airbnb's growth, those "authentic" experiences have become less available, giving way to increasing prices and Instagrammable locations have usurped "living there." Because living in a place–calling it home–means participation in a rooted community through difficulty and celebration.

Sharing economy platforms sell the image of freedom and mobility through self-employment and passive income. Yet, these benefits are only available to a lucky few with excess space to host guests. In fact, much of the profit that Airbnb benefits from is garnered by corporate landlords operating stealthily within the platform, who own and rent numerous properties. In pursuit of higher and more rapid returns than a building full of tenants would allow, such landlords have turned to Airbnb or similar platforms that offer STRs. According to Airbnb's own count, there are more than twice as many listings as there are hosts globally.[142] Further, some renters' leases restrict them from legally subletting their units or houses, reducing the pool of potential "Hosts" who can legally reap profit from the platform to property owners.[143] In a study of Airbnb listings

in Reykjavik, it was found that peer-to-peer accommodation opportunities are afforded disproportionately to middle- and high-income earning households, where excess space is more widely available.[144] As a result, living spaces have become increasingly inaccessible to lower-income earning households – something that there has been ample evidence of in San Francisco as well. Entire neighborhoods, such as North Beach, have become lined with Airbnb accommodations, vacated by longtime residents. Many of these displacements across the city have been executed by serial evictors.

For instance, in 2015, when San Francisco was experiencing a surge in Airbnb conversions, the city filed a lawsuit against the serial evictor Trinity Properties for illegally converting rent-controlled units into short-term rentals. At the time, the company's strategy was to acquire apartments, hotels, and motels, and then operate the buildings with in-house property management and forcing considerable capital improvement costs onto tenants. More recently, Landmark Realty has entered the STR market, with 144 short-term rentals currently listed on Airbnb as of August 2021.

Meanwhile, Fergus O'Sullivan, President at FOS COMPANY and a serial evictor, manages several limited liability companies (LLCs) and is notorious for using various tools to displace tenants, including Ellis Act evictions, Owner-Move-In (OMI) evictions, eviction through construction, buyout evictions, and intimidation. At least one of the units he evicted tenants from and obtained via an OMI eviction is listed on Airbnb by O'Sullivan, and he has also offered many of his properties as STRs at other times. After buyouts and evictions, units are sometimes turned into "tech dorms"--or temporary housing for those moving to the region to work in tech.[145]

Similarly, Danny Haber and Alon Gutman have been behind a wave of displacement in both San Francisco and Oakland, most notoriously by exploiting former single residency occupancy (SRO) housing to turn units into tech dorms, and by profiting from fires to flip buildings.[146] In San Francisco, they purchased an SRO in the SoMA neighborhood and rebranded it as "The Negev," a tech dorm for "communal" living. Initially using Airbnb, and later launching their own website, they took living spaces from some of the poorest SRO residents. Following their involvement in multiple lawsuits in San Francisco, Haber and his associates shifted their focus to Oakland, which has fewer protections for SRO tenants.[147] They have continued to displace numerous tenants on both sides of the Bay since.

Regulating Airbnb in San Francisco

In 2016, a letter from Sens. Elizabeth Warren, Dianne Feinstein, and Brian Schatz to the Federal Trade Commission (FTC) underlined concerns shared by many cities regarding STRs.[148] Citing a report provided by the New York Attorney General, the senators urged the FTC to "study and quantify" how STRs on platforms such as Airbnb, Flipkey, VRBO, and HomeAway are "exacerbating housing shortages and driving up the cost of housing," as well as racial discrimination on these platforms,[149] inconsistent tax collection on properties, and the low proportion of commercial users (6%) owning multiple properties

to individual users owning fewer than three listings, and where commercial users rake in the majority of profits (37%).[150]

But when communities have gathered in solidarity against the displacement of their community members by Airbnb, the company, which presents an ethos of "belonging" and "community," turns its face toward profit over people.[151] In some instances, Airbnb has actively campaigned against policies intended to regulate the platform (i.e., Proposition F in San Francisco, which sought to restrict Airbnb abuse).[152] Even when cities have stated concerns or enacted legislation as a result of housing shortages spurred by increasing Airbnb listings, the company has deferred responsibility, claiming that "as an Internet platform, it is not responsible for the listings on its website."[153]

San Francisco put the "Airbnb Initiative" on the ballot

In 2015, Proposition F, or the "Airbnb Initiative," was introduced on ballots by Share Better SF, headed by Doug Engmann (ironically, a landlord), and garnered over 6,000 more signatures than were necessary to be included on the ballot.[154] The Airbnb Initiative was intended to accomplish three primary aims: to limit private STRs to 75 nights per year, to ensure that those STRs were abiding by city code and hotel taxes, and to allow the city to enforce such provisions of the proposition, as well as "authorize private action lawsuits by interested parties."[155] According to SFGate, the controversy surrounding the Airbnb Initiative was "centered on whether vacation rentals divert scarce housing to lucrative illegal year-round hotels, as its backers claimed, or helped middle-class people make ends meet, as Airbnb and other opponents of the measure said."[156]

While the Airbnb Initiative was voted down in 2015, it received over 44% "yes" votes–a high level of support for a proposition that was the first of its kind.[157] Additionally, its proponents provided a lesson in direct action and some argue those movements inspired tangible change in the long term. Key takeaways from the Prop F campaign were:

1. ***Residents don't have to wait for governments to propose initiatives.***
   In the state of California, citizens can follow a process to put an initiative in front of voters to change legislation or amend a state constitution. While the process varies from state to state, citizens have similar opportunities to propose both direct (straight onto the ballot) and/or indirect (goes to the state legislature for approval) statute initiatives in all US states, except FL, IL, MD, MS, and NM.[158] In the case of the Airbnb Initiative, residents voted on a direct statute initiative to regulate short-term rentals.[159]

2. ***Direct action grabs attention and activates voters.***
   There are a variety of approaches to prevent or combat homelessness and displacement, but few attract media coverage like direct action. And with the availability of recording devices, such as smartphones, it's easier than ever to broadcast protest movements.

In a widely covered 2015 protest organized by the Heart of the City Collective, organizers filled an atrium of the Airbnb headquarters in San Francisco for ninety minutes, replete with a brass band, drummers, and helium balloons tied to red, house-shaped signs parodying Airbnb's campaign against Prop F. Signs read, "Evictions. Love, Airbnb" and "Homelessness. Love, Airbnb." The protest took place the day before local elections were held to activate voters.

3. ***A little $ goes a long way.***
Leading up to the vote, Airbnb shelled out nearly $8.5 million of the $9 million+ donated to oppose the Airbnb Initiative.[160] In contrast, those supporting the initiative donated a total of $1.1 million.[161] So even though the initiative only received 44% of the vote, the proponents' campaign received a fraction of the financial backing than the opponents'. This demonstrates that residents have a fighting chance against predatory corporations even if they don't have the same financial resources.

Ongoing Struggles

In 2015, San Francisco passed Ordinance 130-15 permitting STRs within the city, albeit with several restrictions. Among other requirements, hosts of all existing (and previously illegal) STRs were required to register with the San Francisco Treasurer and Tax Collector.[162] However, over 76% of unique Airbnb hosts in San Francisco continued to operate illegally without registration.[163] As Airbnb continued to profit off of the service fees from bookings at illegal listings, the City and County of San Francisco turned up the heat on the company by fining Airbnb for each active Host operating without registration. The $1 million in fines against Airbnb–the company's net worth was valued at $30 billion at the time–were for 483 violations.[164] San Francisco's counter to Airbnb's lack of regulation regarding its hosts and their listings was not the first against the rental platform. Several cities around the world had brought similar fines against Airbnb in an effort to enforce city codes, business registrations, taxes, proof of insurance requirements, etc. Airbnb responded to such fines with a lawsuit against its birth city.[165]

In 2017, Airbnb and the City of San Francisco reached a settlement in which the platform agreed to create a registration system requiring hosts to register prior to posting their listing and to send this information to San Francisco's Office of Short-Term Rentals (OSTR) to be checked against their own records.[166] While the settlement took six months to go into effect–giving hosts plenty of time to register–in January of 2018 Airbnb listings in San Francisco dropped by nearly 50% as thousands of hosts failed to register.

Recently, another type of rental, Intermediate Length Occupancy (ILO) dwelling units have been designated by the San Francisco Planning Department. While these are similar to short-term rentals, they differ in length, and are often used for medium-term corporate rentals. Code specifies that ILOs are, "offered for occupancy by a natural person for an initial stay, whether through lease, subscription, license, or otherwise, for a duration of greater than 30 consecutive days but less than one year."[167] This form of dwelling space

and renting pattern is hardly new, but with the evolution of lodging tech platforms and landlordism trending away from long-term leases, policy regarding ILOs has become necessary. Policy, put forth by the Board of Supervisors in June of 2020, specifically caps the total number of ILOs within the City limits at 1,000 (down from some 2,700) with several limitations on permissible building type, as well as a registration requirement. Additionally, ILOs are distinguished as non-residential housing and often are used as corporate rentals, in contrast with STRs typically used for holidays.[168] The ordinance went into effect in June of 2022 and is certainly a step toward making long-term housing units available to residents. However, the ordinance operates on a complaint basis and funds no entity for direct enforcement.[169] As People Power Media puts it, "Planning must devise a regulatory system that ensures strict compliance with the new legislation, and updates the legislation to regulate new non-residential uses as they appear on the scene."[170]

Global Regulations

The "Airbnb effect," while complex, describes the negative impacts of Airbnb's presence (and the presence of similar platforms) in cities. From increased rent prices, shortage of rental units, and increased property values, many blame the "Airbnb effect" for the lack of housing opportunities, particularly in urban areas.[171] Globally, cities have grappled over how to regulate STRs, as well as combat the "Airbnb effect".[172] In particular, Amsterdam, Barcelona, New York City, and Berlin have imposed restrictions or conditional bans on STRs. Here we trace the paths of regulation and organization against the gentrifying impacts of Airbnb.

In Amsterdam, where residents annually experience an average of over four times their population in foreign tourists, the city council attempted to ban STRs in some residential areas due to concerns regarding "excessive tourism and disruptive guests".[173] However, the court blocked this effort in 2021. Fortunately, the city council successfully passed limits on the number of nights a unit may be rented per year, restrictions on the number of guests who may stay in a unit, and permit requirements for Hosts.[174] New York, Paris, and San Francisco have followed a similar approach.

Barcelona took a different approach to STRs. The city, led by Mayor Ada Colau (former anti-eviction activist), enacted a series of restrictions on STRs, including a freeze on licenses for entire-apartment tourist rentals, regulation of tourist shops in particular neighborhoods, as well as tightening sanctions on illegal listings.[175] Further, Barcelona's City Hall has dedicated inspectors of Airbnb listings who have discovered that many Hosts are actually real estate speculators, unlike the image conjured by Airbnb of Hosts using their listings to supplement income. Historically, Airbnb has repositioned "local families" as the victims of government regulation in an attempt to humanize itself.

HOW ARE GLOBAL CITIES REGULATING STRS?

	Permit requirements	Outlawing STRs under some conditions	Limiting rental periods	Rental tax
AMSTERDAM			■	■
BERLIN	■	■		
BARCELONA	■			
PARIS	■		■	
SAN FRANCISCO	■		■	■
LOS ANGELES	■			
NEW YORK CITY		■	■	

In addition to local short-term rental restrictions, organizations like the European Union (EU) have sought to restrict digital platforms across member states. For example, the European Commission, being the executive branch of the EU, proposed the Digital Services Act and the Digital Markets Act in December 2020.[176] Both were approved in the spring of 2022. The joint acts are intended to "evolve European legislation" to meet changes in the digital world in order to preserve the rights of EU citizens.[177] As the European Commission states,

> "A core concern is the trade and exchange of illegal goods, services, and content online. Online services are also being misused by manipulative algorithmic systems to amplify the spread of misinformation, and for other harmful purposes."[178]

These policies are relevant to sharing platforms because as a gatekeeper platform–defined by the European Commission as a "digital platform with a systemic role in the internal market that function[s] as [a] bottleneck between businesses and consumers for important digital services"[179]–Airbnb's blitzscaling method has empowered them to act as private rule-makers and has reduced choices for tourism and tenant consumers by gobbling up competition.

However, some European cities already view the acts as too lax. Since the approval of the two acts, sixteen cities within the EU have submitted amendments to the Digital Services Act, with particular attention to tightening regulation against lodging platforms.[180] These amendments underscore enforcement difficulties unique to digital platforms and request clarity for authorities' roles and timelines.[181]

City Portal and Airbnb Data

In September 2020, facing numerous pressures from city governments, Airbnb launched City Portal, a partnership tool pitched as a technological fix to quell government skepticism and concerns regarding Airbnb's impact on and presence in neighborhoods.[182] City Portal is intended to enable local governments and tourism bureaus to access elements of the platform's data, such as listing registrations and marketing insights.[183] Whereas Airbnb's City Portal is popular with its partnered tourist organizations as a marketing tool, some of the key complaints from local governments regarding STRs received only a partial solution. While some cities laud the new tool as a step forward and have encouraged other platforms to take similar steps to cooperate, it does not provide the open access to data that others would like to see available. Speaking about City Portal, David Proserpio, a digital travel platform researcher, stated, "...when it comes to data-sharing there is still a lot to do, and so far only a few cities were able to obtain detailed data from Airbnb."[184]

The lack of Airbnb data has led to projects such as data activist Murray Cox's Inside Airbnb, which opens up Airbnb data and analysis to the public. As their website states, they are "a mission-driven project that provides data and advocacy about Airbnb's impact on residential communities. We work towards a vision where data and information empower communities to understand, decide and control the role of renting residential homes to tourists."[185] Cox created the site in 2015 enraged by Airbnb's role in gentrification. [186]Similarly, Tom Slee's Airbnb Data began opening up Airbnb data and code as early as 2013.

Airbnb Surveillance Technologies

In addition to the platform's role in housing instability and tenant displacement, it has integrated various forms of surveillance tech in order to placate hosts' security concerns. Though further regulations on STRs are still needed–even in cities with the most successful restrictions–additional surveillance technologies are not the solution to displacement by STR platforms' presence, such as Airbnb. Interestingly, GateGuard, a building access landlord tech company implemented in NYC to track and log visitors to a property with an option to incorporate facial recognition, was first conceptualized by Ari Teman who felt that his apartment had been ransacked by Airbnb partiers when he rented his unit out. In response, he developed GateGuard to allow landlords to detect illegal sublet activity to evict or fine tenants who Airbnb illegally.[187] Another popular landlord tech company, Granicus (formerly Host Compliance), partners with over 5,500 government organizations to ensure STR Hosts comply with city regulations. Granicus' pitch to cities is that they will see higher tax revenue from STRs that meet compliance requirements."

As of August 2022, Airbnb has been piloting an "anti-party" technology two years after the platform banned house parties, or gatherings of more than sixteen people at any listing.[188] The technology is being trialed in Australia, and soon to be implemented in the US and Canada.[189] It appears to operate preemptively by preventing guests from booking a

listing that an algorithm presumes will be used as a party site based upon several factors. As we do not have information on how these anti-party predictive algorithms function, we cannot assess whether or not they are impartial.

5
TENANT SCREENING

Landlord tech squeezes tenants out of the housing market from multiple directions, especially in rapidly gentrifying markets such as the Bay Area. In the previous sections, we overview a range of property surveillance systems that help landlords bypass eviction moratoriums and displace existing tenants in favor of higher-paying ones. For tenants forced out of housing by these systems, the exploitation does not stop there: often, their illegitimate evictions become a data point to be used against them in their attempts to secure housing going forward.

In this section, we examine the technologies landlords use to collect and share data about tenants – including eviction records – with one another. Today, an estimated 90 percent of landlords use tenant screening services to make leasing decisions.[190] These services work in tandem with surveillance technologies and other tools of eviction to make tenants more vulnerable, allowing landlords to bypass housing discrimination laws and intimidate would-be organizers.

Screening Systems and Effects

A "tenant screening service" is a third-party agency that collects data on prospective tenants and sells this data to landlords.[191] Landlords may receive either an itemized report of compiled tenant information, or, as is more common today, a composite tenant "score" (either binary or numeric).[192] By receiving only a composite score, landlords can leave it up to the algorithm to decide which tenants to accept, and thus avoid liability for discrimination.[193] The data used by tenant screening companies is most often sourced from public records such as criminal records, eviction records, and credit reports. For instance, U.D. Registry, the first major "tenant screening bureau" (TSB) in the U.S., which emerged in California in the 1970s, initially based its reports solely on eviction notices.[194]Data can also, however, be sourced from other landlords and other private sources. In the 1980s, TSBs began moving beyond public data and incorporating investigative tactics such as interviews with previous landlords into their tenant reports.[195] These practices persist today, often in more comprehensive and mechanized form. During the COVID-19 economic shutdown of April 2020, for instance, tenant screening company Naborly asked landlords to report whether their tenants were late to pay rent, promising to incorporate this information into their tenant database.[196] This rent "delinquency" data, which was not public record, was then sold to prospective landlords without the affected tenants' knowledge or consent.[197]

The spread of algorithmic tenant screening poses urgent questions about the legal frameworks in place to combat housing discrimination. In the 2015 case Texas Department of Housing and Community Affairs v. Inclusive Communities Project, the Supreme Court ruled that housing discrimination suits based on "disparate impact" claims had legal standing under the Fair Housing Act.[198] This case marked a watershed moment in housing discrimination law: before, courts could only hear housing discrimination cases if the plaintiffs could produce evidence of "discriminatory intent." However, lower courts have produced conflicting opinions on whether the "disparate impact" standard can be applied to tenant screening algorithms.[199]

Because the public data typically found in tenant screening reports, such as eviction records, criminal records, and credit scores, are "race-neutral" on their face, landlords who use screening services that rely on this data cannot be held liable for "discriminatory intent." Yet these records are produced in an institutional environment with a long and ongoing history of racist and discriminatory practices– including but not limited to racialized policing and resulting disparities in arrests, discriminatory housing laws such as exclusionary zoning and redlining, and discrimination in credit access. In practice,

eviction filings disproportionately target low-income tenants, people of color, and women.[200] With landlord interviews or reviews emerging as a factor in some companies' tenant scores, individual racial biases among landlords may also factor into leasing decisions– an ironic outcome of a process advertised as a way to eliminate landlords' personal biases and subjectivity. The presence of subjective landlord reports in tenant screening algorithms lays bare the twisted logics by which these services allow landlords to evade liability. Landlords can be held liable for discrimination based on disparate impact if they make their own leasing decisions without the help of an algorithm, but in theory may be home free if they base their decision on a subjective review by the prospective tenant's previous landlord filtered through an algorithm.

As rents in the Bay Area and elsewhere skyrocket and housing access becomes increasingly tenuous, TSBs contribute to a multi-frontal assault on tenants' security and ability to contest the status quo. Behavioral experiments have demonstrated that when presented with a typical tenant screening report, landlords avoid renting to tenants with prior eviction records regardless of the outcome of the eviction case.[201] If adopted by all landlords, automated tenant screening could thus exclude all tenants with eviction records – even those who were never evicted – from all standard rental housing, relegating them to informal, substandard, and/or discriminatorily overpriced housing. This process of coordinated exclusion of tenants by landlords and TSBs has been referred to as "blocklisting"[202] by housing scholars and organizers. Given racial and gendered disparities in evictions, blocklisting constitutes housing discrimination in all but name. The Tech Equity Collaborative has laid out the chilling effects of coordinated exclusion:

> "[Exclusion from housing based on criminal and eviction records] creates a secondary market of so-called "second-chance" landlords, who will rent to people with unfavorable background checks and use them as grounds to charge extortionist rates for things like security deposits, strapping a vulnerable population with even greater debt."[203]

At the same time, the prospect of exclusion from the rental housing market may also discourage tenants from challenging exploitative landlords. While retaliatory evictions are illegal in many jurisdictions, such laws only prevent landlords from winning eviction suits, not from filing them. As such, landlords can and do use the threat of filing an unwinnable eviction suit as an intimidation tactic. This dynamic has been observed by organizers in New York and elsewhere[204] and acknowledged by landlords themselves, who describe tenants at risk of eviction as "less antagonistic, less likely to report maintenance issues, and even willing to help with home repairs."[205] In New York City in the 2000s, the ratio of eviction filings to evictions was 10:1, indicating that the majority of eviction suits were filed to intimidate and harass tenants.[206] While evictions can already be economically devastating for tenants, the threat of eviction will only further dissuade organizing against landlords as tenant data sharing among landlords becomes more ubiquitous and past eviction filings become a bigger barrier to future access to rental housing.

CoreLogic and the Logics of Automated Screening

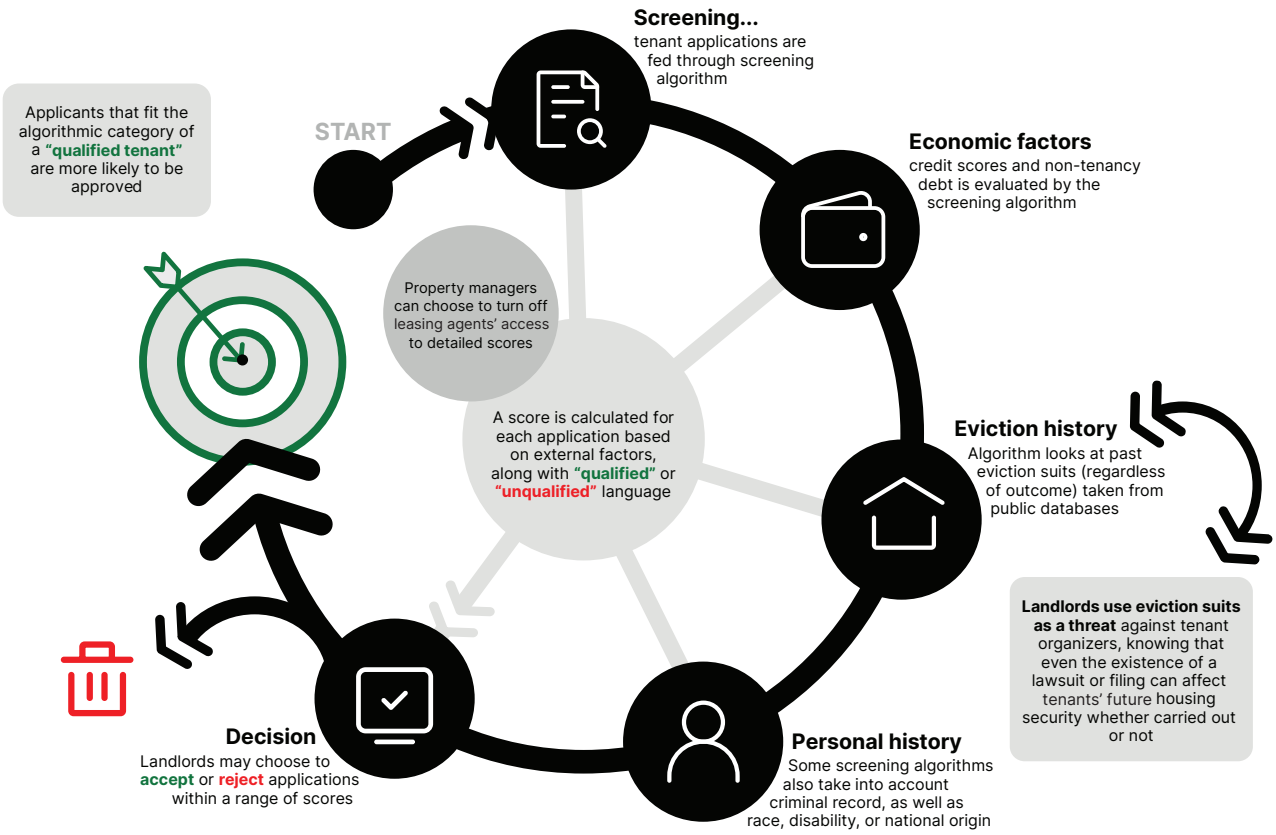
Irvine-based consumer information and business intelligence company CoreLogic has been at the center of recent legal controversy in tenant screening. CoreLogic's proprietary tenant screening software, Registry CrimSAFE, has been the subject of numerous lawsuits including Arroyo v. CoreLogic, Connecticut Fair Housing Center et al. v. CoreLogic Rental Property Solutions, LLC, and Marco A. Fernandez v. CoreLogic Credco, LLC, among others.

Like many TSBs, CoreLogic explicitly positioned CrimSAFE as a middleman for discrimination. A property manager who partners with CrimSAFE does not receive an itemized report on a prospective tenant's criminal record. Instead, the software inputs criminal records and other information pulled from an undisclosed range of sources and simply outputs whether an applicant has "disqualifying records."[207] Landlords then decide whether to accept or reject an applicant based only on whether they are flagged. While CoreLogic contends that "it is up to the landlord" to make final leasing decisions, this claim is far-fetched given the only information landlords receive is whether an applicant has an unspecified criminal disqualification.[208]

While TSBs today publicly market themselves as "filtering tools," language in CrimSAFE marketing materials through the 2010s reveals that CrimSAFE's "black-box" approach was designed as a means for landlords to evade liability for discrimination. CrimSAFE's 2005 patent application describes the software as a product that "relieves staff of the burden of interpreting criminal records."[209] This language was mirrored in pamphlets marketed to landlords throughout the 2010s, and, until 2020, appeared on CoreLogic's website. [210]

Of note, CoreLogic also marketed an alternative software, called Registry CrimCHECK, which allowed property managers to view detailed criminal records rather than just a binary flag for criminal disqualification. In fact, CoreLogic marketed the ability for property managers to turn off leasing agents' access to detailed criminal reports as a key feature of CrimSAFE.[211] Any property manager using CrimSAFE was thus making a conscious decision to avoid any possible liability that could result from viewing actual criminal records. Making this trend all the more disturbing was the omnipresence in CrimSAFE marketing materials of the claim that CrimSAFE (as opposed to CrimCHECK) "optimizes Fair Housing [Act] compliance."[212]

A CoreLogic training video for sales and account managers from 2016 reveals that the use of arrest rather than conviction data in the CrimSAFE screening algorithm was a deliberate choice. CoreLogic sales trainers explained that criminal data can be taken from the Administrative Office of the Courts (AOC) or the Department of Corrections (DOC), but that AOC data is preferred for its comprehensiveness as DOC data "generally only covers cases that resulted in the defendant entering the correctional system."[213] In other words, AOC data covers all types of cases that go to court, whereas DOC only covers cases that actually result in incarceration or probation. CoreLogic justified their preference for AOC data by noting that some criminal convictions might only result in a fine and thus not be reflected in DOC data.[214]



The disturbing opacity of the CrimSAFE algorithm came to light in the case Arroyo v. CoreLogic, in which a property manager using CrimSAFE denied Connecticut tenant Carmen Arroyo's disabled adult son, Mikhail, the right to live with her based on undisclosed "disqualifying criminal records." After suffering a coma and severe injuries in a freak accident, Mikhail could not care for himself. Mikhail was no criminal: he had a single dismissed shoplifting charge, and, further, he was newly paralyzed and obviously could pose no threat to public safety. Unfortunately, when Carmen appealed this obvious oversight to the property manager, she discovered that the property manager had no actual knowledge of Mikhail's criminal history.[215] He had simply been flagged as "disqualified" by CrimSAFE's algorithm. CoreLogic subsequently refused to provide an itemized criminal report to either the Arroyos or the property manager, and with no clarifying details available, Carmen's appeal was denied. Unable to live on his own due to his disability, Mikhail remained in a nursing home.[216]

Arroyo illustrates several layers of the discriminatory potential of tenant screening algorithms. For one, Mikhail was flagged based on a dismissed shoplifting charge; he had no actual record of criminal activity. Racist stereotyping by store employees notoriously plays a role in many shoplifting arrests, a pattern that data reveals to be systemic: despite

evidence that race has no correlation with who actually shoplifts,[217] Black people are arrested for stealing at a rate nearly 3 times their proportion of the population.[218] Ironically, a technology designed to eliminate racial bias on the basis of individual leasing agents thus delegates decisions to the individual racial biases of Walgreens security guards and countless other individuals implicated in the creation of arbitrary arrest data.

As of 2021, CoreLogic has divested from CrimSAFE, declaring themselves "out of the tenant screening business."[219] Yet similar companies and similar algorithms continue to systematically and wrongly exclude tenants from housing in California and elsewhere.

Policy and Organizing Implications

In cities like San Francisco, where people of color are disproportionately likely to be tenants due to decades of discriminatory housing practices such as redlining and racial covenants, the reproduction of racial discrimination through tenant screening is yet another way in which the deck is stacked against people of color in acquiring quality housing and building wealth.[220] The ways in which screening technologies perpetuate inequalities are all the more disturbing in light of the fact that property managers deliberately allow them to do so, restricting their own access to information that could help clarify screening results, simply to "save time" and shield themselves from liability for housing discrimination.

As TSBs proliferate and contribute to tenants' vulnerability, cracks are showing in the popular techno-capitalist narratives in which "open data" is always construed as a universal good. Data is power, and who benefits from it depends on who is able to access and use it. Several of the writers of this report have relied on eviction records and other public data sources to build tools for tenant organizing. Tenant organizers, nonprofits, and housing policy researchers all use housing court records to track eviction trends, identify particularly eviction-happy landlords, and formulate anti-eviction policies.[221] At the same time, however, landlords are using the same records to coordinate to increase profits and increase many tenants' vulnerability to exploitation, often in a highly organized manner. These conflicting efforts give rise to questions about the appropriate levels of privacy controls for "public" housing data.

Many pro-tenant organizations have recommended sealing and expunging housing court records in order to limit TSBs' ability to "blocklist" tenants.[222] States such as California, Oregon, Minnesota, Nevada, and New York have passed a range of anti-blocklist legislation.[223] In New York, a blocklist ban embedded in the Housing Security and Tenant Protection Act (HSTPA) bans the use of eviction data by TSBs in the state, although this does not prevent retaliatory evictions that occur in New York from being used against tenants by landlords in other states.[224] In California, eviction filings are "masked" and are not publicly available unless the landlord prevails in court.[225] In Minnesota, Nevada, and Oregon, housing court records are "effectively expunged," either formally or through record sealing.[226] Several other states and cities introduced anti-blocklist laws during the COVID-19 eviction moratorium, some of which may become permanent.[227] In states

such laws, however, no federal legislation exists to prevent landlords from systematically weaponizing the blocklist.

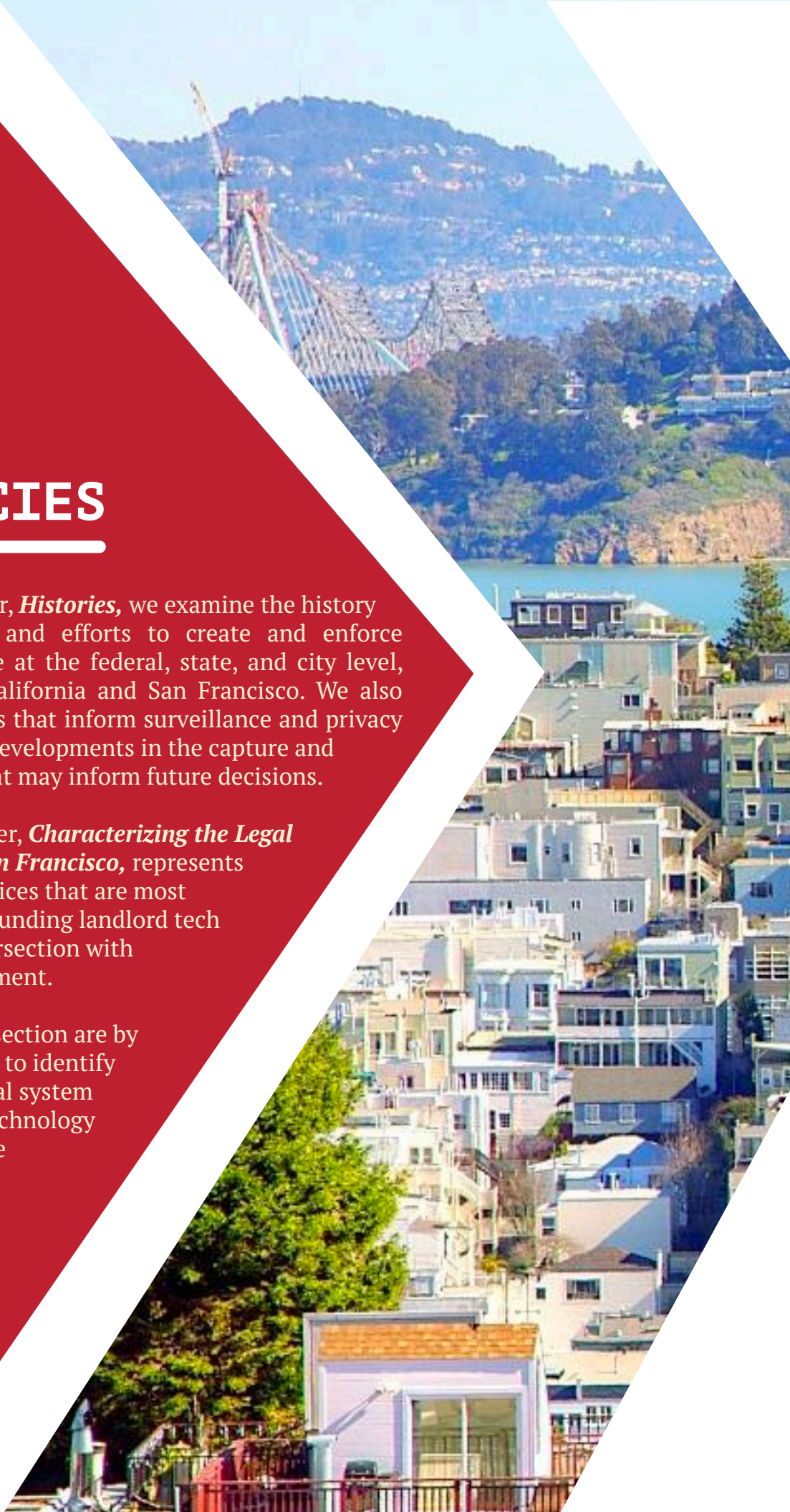
Tenant protections against TSBs in the Bay Area are sparse, but recent legislation gives cause for hope. In Alameda County, the Fair Chance Ordinance was passed in December 2022 prohibiting landlords and TSBs from using criminal background checks in tenant screening, a decision that was widely hailed as a way to combat criminal recidivism and houselessness.[228] In the wake of the Alameda County ordinance, California Sen. Aisha Wahab introduced a similar bill in the state Senate that would prohibit landlords from requiring would-be tenants to disclose their criminal history or authorize a criminal background check.[229] As of July 2023, Sen. Wahab's bill has not yet been brought to a Senate floor vote. In September 2022, California also passed a reusable tenant screening bill, Assembly Bill 2559, aimed at shifting the immediate financial costs of tenant screening away from tenants. The bill gives applicants the ability to buy their own screening reports and submit them to landlords themselves, allowing them to reuse the same reports for all applications rather than being charged for the landlord to run a report every time.[230] Unfortunately, landlords are not forced to accept reusable reports from tenants, and many landlords are likely to continue choosing to profit off of application fees rather than allow tenants to accept their own reports. Landlord association spokespersons have already expressed dismissive sentiments toward reusable tenant screening, often under the guise of concern about "fraudulent" reports.[231]

6
LANDLORD TECH POLICIES

In the first half of this chapter, ***Histories,*** we examine the history of surveillance technology and efforts to create and enforce regulations regarding its use at the federal, state, and city level, honing in particularly on California and San Francisco. We also compare and contrast models that inform surveillance and privacy policy and look toward new developments in the capture and use of tenant information that may inform future decisions.

The second half of this chapter, ***Characterizing the Legal Landscape for Tenants in San Francisco,*** represents a collection of laws and practices that are most applicable to the issues surrounding landlord tech in San Francisco and its intersection with ongoing patterns of displacement.

While the list of laws in this section are by no means exhaustive, we aim to identify major components of the legal system that interact with landlord technology and demonstrate the multiple dimensions and crossover in practice it creates.



HISTORIES

Histories of Surveillance in Housing

Video surveillance originates as far back as 1956, when it was deployed by police departments across the United States for the first time.[232] The 1960's saw the rise of CCTV cameras deployed both in the public sector by police, and in the private sector by businesses and private landlords.[233] In 1997, 13 cities had their own public surveillance programs, by 2016, 49 percent of local police departments in the United States reported using CCTV.[234]

The proliferation of the use of CCTV and video surveillance in private residential buildings has been highly normalized despite the ongoing concerns of housing advocates. Security cameras have become so common that an estimated 58 percent of New York City Housing Authority public housing developments have cameras, and comparably in San Francisco, surveillance networks both public and private have amassed 2,753 cameras–– predominantly clustered in tourist areas and lower income neighborhoods.[235] Landlord-tenant law, and therefore surveillance policies, vary state to state. but most jurisdictions view tenant surveillance as part of the common law duty of a landlord to provide security for their tenants. Under this duty, in some states, landlords can be held liable for failing to provide security when that failure resulted in injury to a tenant. As such, courts have long recognized that landlords have the right to install surveillance cameras, intercom systems, and other precursors to landlord tech on their properties to assure the safety and security of their tenants.[236]

In general, tenants have a reasonable expectation of privacy inside their dwellings, but landlords are free to surveil common areas on their properties, where the same rights don't exist.[237] In almost all states, security cameras are allowed so long as landlords notify tenants prior to installation and as long as cameras that are placed in common areas are visible so that tenants know they are being surveilled.[238] Outside of the landlord-tenant law context, some states have unlawful surveillance laws that criminalize invasive spying by anybody.[239] Surveillance by landlords also, in general, must comply with state and federal wiretapping laws, which generally prohibit audio recording of tenants.[240] Aside from these common-law protections, tenant surveillance is largely unregulated, which contributes to the furious proliferation of landlord tech and the expansion of the landlord tech sector.

The following review consists of a summary of the policy landscape in the main areas that intersect with landlord tech: biometric surveillance regulation, data privacy, and landlord-tenant law. After an overview, we discuss how existing policies and laws might be utilized in the fight against landlord tech and give recommendations for the tenant's rights movement going forward.

The use of surveillance in public housing has been encouraged by legislators and law enforcement officials with the aim of deterring crime. Functionally, this means that communities of color have largely borne the brunt of the use of residential surveillance

and have directly suffered the consequences.[241] Legislators have the most say in the use of technology in the housing context when it comes to publicly funded housing. Municipalities that have an interest in testing new forms of surveillance often do so at the expense of residents of publicly funded housing, as public-private partnerships that fuel public housing tend to leave these types of residences even further vulnerable to private technology investment with free license by the municipal government. But paradoxically, because governments have the most oversight over public housing, it also means that regulations of landlord technology exist almost exclusively in the public housing context.

Federal Regulation of Facial Recognition Tech

Technology has far outpaced regulation in the recent past, and as a result, regulations on its use and development is notoriously fraught. The same is true of the technology used by landlords. Because of the inherently local nature of housing, the use of landlord tech will invariably be most affected by state and local ordinances that govern the use of such technology. When it comes to housing, the federal government's ability to regulate the use of technology on physical properties only extends to buildings under its purview as a "landlord" – buildings that receive federal affordable funds—for example, those provided by Section 8 of the Housing Act of 1937 on behalf of low-income households. While federal legislation rarely addresses the use of tech in housing specifically, many legislative proposals address key components of landlord tech: facial recognition, automated decision making, algorithms, AI, and data privacy. Despite a flurry of bills introduced to deal with these issues, little has passed Congress. However, federal agencies have increased the pace at which they use their existing powers to regulate technology in this space, even in the absence of Congressional legislation.

Landlord tech, and biometric and AI-based technology in general, are largely unregulated at both the state and federal levels. Regulations around technology in the housing sector, specifically, remain lacking even as the industry continues to expand.[242] After the organizing campaign to prevent facial recognition systems from being deployed in the Atlantic Plaza Towers in New York gained national and international attention, lawmakers (informed by tenant organizers) introduced legislation in 2019, and again in 2021, but it has not advanced to become law. The No Biometric Barriers to Housing Act of 2019 was introduced by Senator Cory Booker and U.S. Representative Rashida Tlaib (and in 2021 by Reps Ayanna Pressley, Yvette Clarke, and Rashida Tlaib) as the first federal law that would regulate facial recognition in any context.[243] The legislation would have banned the use of multiple forms of biometric-based surveillance, including facial recognition but also any other form of biometric data collection and use including fingerprint/palmprint and retina/iris scanning.[244] Crucially, the bill also contains a mandatory reporting section, which would require public disclosure of the use of facial recognition or biometric recognition technology, though the law would only apply to housing funded by the U.S. Department of Housing and Urban Development (HUD). Furthermore, the bill contains no specific relief or cause of action, which would make enforcement difficult. There are also no specified forms of relief (such as the authorization of money damages). The reporting function is similarly weak: while the bill asks for retroactive information

installed forms of facial recognition, it does not include any requirements for reporting on the removal of those systems.

There have been several bills introduced for the regulation of facial recognition technology. The Facial Recognition and Biometric Technology Moratorium Act, which seeks to place a moratorium on the practice in general, was introduced in June of 2021 but has seen no further action.[245] Several other bills seeking to regulate the use of technology in the commercial context have been introduced, including the Ethical Use of Facial Recognition Act of 2020, the Facial Recognition Warrant Act of 2019, the FACE Protection Act of 2019, and the Commercial Facial Recognition Warrant Act of 2019, the FACE Protection Act of 2019, and the Commercial Facial Recognition Privacy Act of 2019. None of these bills specifically target the use of such technology in housing, and none have been passed into law. The Facial Recognition and Biometric Technology Moratorium Act does not specifically prohibit the use of facial recognition in housing, but it does prohibit the use of the technology by any federal government entity, and conditions federal funding for state entities on the enactment of their own moratoria.[246]

The pace of regulatory proposals picked up in 2021, accelerated especially by the Facebook Whistleblower hearings which occurred in the fall of that year. The focus of these hearings brought increased scrutiny to the use of algorithms by online platforms. More than 30 bills seeking to regulate the use of algorithms were put forth in 2021, although none came to pass. In May 2021, Senator Markey and Congresswoman Matsui introduced the Algorithmic Justice and Online Platform Transparency Act, which sought to create a commission to study the impact of discriminatory algorithms on the national economy and establish safety and effectiveness standards for the use of algorithmic processes. In early 2022, Senators Booker, Wyden, and Clarke introduced the Algorithmic Accountability Act of 2022. The Act seeks to direct the Federal Trade Commission to promulgate regulations for ADS and "augmented critical decision processes" that have material effects on a consumer, which would have clear applications in the landlord tech context.[247] The same Act had been proposed in 2019 but did not advance.

Prior to the Facebook whistleblower hearings, the only bills regulating the use of AI systems were those that addressed the markets for self-driving vehicles and automated decision systems in the aviation industry. Bills regulating other automated decision-making (ADS) systems have circulated on the Hill for years. H.R. 2644, The Reasonable Policies on Automated License Plate Readers Act, was introduced in 2012, and similarly never made it out of committee.[248] Congress's latest move in the AI regulatory space was to pass the defense budget with provisions establishing investigatory bodies for the regulation of AI in early 2021, including a White House AI Office and several other regulatory bodies across the federal government.[249] A slew of bills for regulating AI and Machine Learning (ML) in the social media context were introduced in late 2021, including the Filter Bubble Transparency Act, the Justice Against Malicious Algorithms Act, The Social Media DATA Act, and more. While several of these proposals don't have a direct application to landlord tech, the fact that Congress is paying attention to the use of algorithms and AI is a promising step, as AI is one of the building blocks of problematic surveillance tech.[250]

FEDERAL REGULATION OF AUTOMATED DECISION-MAKING

Reasonable Policies on Automated License Plate Readers Act

BILL #	DATE	COMMITTEES	SPONSOR	STATUS
H.R. 2644	08/02/2012	House Judiciary Committee	Rep. Michael E. Capuano	Introduced

Law enforcement agencies cannot use license plate readers unless agreements have been made to prevent storage of data for 30+ days, storage in national databases, or sharing information obtained with external agencies.

Reasonable Policies on Automated License Plate Readers Act

S.4400	08/03/2020	Senate Judiciary	Sen. Jeff Merkley	Introduced

Regulates "the collection, retention, disclosure, and destruction of biometric information."

Information Transparency and Personal Data Control Act

H.R.1816	03/11/2021	House Energy and Commerce	Rep. Suzan K. DelBene	Introduced

Requires the Federal Trade Commission (FTC) to "establish requirements for certain entities when they collect, transmit, store, process, use, or otherwise control sensitive personal information" (defined as non-public information relating to an identifiable individual).

Social Media Privacy and Consumer Rights Act

S.1667	05/18/2021	Senate Commerce, Science, and Transportation	Sen. Amy Klobuchar	Introduced

Requires "online platform operators to inform a user, prior to a user creating an account or otherwise using the platform, that the user's personal data produced during online behavior will be collected and used by the operator and third parties. The operator must provide a user the option to specify privacy preferences, and an operator may deny certain services or complete access to a user if the user's privacy elections create inoperability in the platform."

Social Media DATA Act

H.R.3451	05/20/2021	House Energy and Commerce	Rep. Lori Trahan	Introduced

Requires "consumer-facing websites and mobile applications with a large number of users to maintain advertisement libraries and make them available to academic researchers and the FTC."

Algorithmic Justice and Online Platform Transparency Act

H.R.3611	05/28/2021	House Energy and Commerce	Rep. Doris O. Matsui	Introduced

Prohibits "the discriminatory use of personal information by online platforms in any algorithmic process" and requires "transparency in the use of algorithmic processes."

Filter Bubble Transparency Act

S.2024	06/10/2021	Senate Commerce, Science, and Transportation	Sen. John Thune	Introduced

Requires "that internet platforms give users the option to engage with a platform without being manipulated by algorithms driven by user-specific data."

Justice Against Malicious Algorithms Act

H.R.5596	10/15/2021	House Energy and Commerce	Rep. Frank Pallone Jr.	Introduced

"Limits federal liability protection that applies to a provider of an interactive computer service for claims related to content provided by a third party if the provider makes personalized recommendations of online content that cause physical or emotional injury."

Justice Against Malicious Algorithms Act

H.R.6580	02/03/2022	House Energy and Commerce	Rep. Yvette D. Clarke	Introduced

Directs the FTC to "require impact assessments of automated decision systems and augmented critical decision processes."

2022 was expected to be a year of growth on the data privacy front, but regulation has not significantly accelerated as compared with previous years. Several bills were proposed in 2021, including the Social Media Privacy Protection and Consumer Rights Act and the Information Transparency and Personal Data Control Act, but neither has been advanced. Senators Bernie Sanders and Jeff Merkley also introduced S.4400, the National Biometric information Privacy Act in late 2020, which would create the first regulations on the general use, collection, storage, and retention of biometric data. To date, the U.S. still lacks a nation-wide data privacy law.

Pushback from industry, the difficulty of creating brand-new regulatory frameworks, and a lack of targeted focus have stalled the progress of new federal laws regulating tech. However, tenant rights advocates have found purchase in existing laws and by turning to agencies for agency-level regulation. The Fair Housing Act (FHA), which does touch private landlords by forbidding discrimination, and the Fair Credit Reporting Act (FCRA) and other consumer protection statutes have been used to challenge the use of landlord tech.[260] In a major win against tenant screening companies, the Connecticut Fair Housing Center's lawsuit against major tenant screening company CoreLogic over their biased algorithm survived a motion to dismiss in late 2020.[261] The Federal Trade Commission (FTC) has brought enforcement actions against screening companies under these statutes in the past, including an action against RealPage that resulted in a $3 million settlement for failing to meet accuracy requirements.[262] The Consumer Financial Protection Bureau (CFPB) has warned consumer reporting companies, including tenant screeners, that they may be violating the FCRA with careless background screening practices.[263] Authorized by the National Defense Authorization Act of 2021, the National Institute of Science of Technology (NIST) is at the forefront of regulating facial recognition by evaluating the accuracy of multiple FRS through the Face Recognition Vendor Tests.[264]

State and Local Regulation of Facial Recognition Tech

In lieu of national legislation, more and more states are passing comprehensive surveillance, tech, and data regulations. A number of localities have passed outright facial recognition bans and more cities have created oversight bodies for surveillance technologies.The majority of these ordinances focus on the use of these technologies by the state or local government, especially the police, and forbid their use or purchase in the policing context. Several of the ordinances are written broadly enough to include the use of these technologies in public housing as well. In cities and states that have their own affordable housing programs with oversight bodies that fall under the purview of these regulatory ordinances, the use of the technologies can be regulated without housing-specific legislation. Increasingly, state and local rules have begun banning or regulating the use of these technologies in the private and commercial context, as well.

State Regulations

Landlord tech that tracks and surveils tenants can fall under the purview of regulations

on data privacy and usage. Three states – California, Virginia, and Colorado – have comprehensive data protection laws on the books, which are modeled after data privacy laws such as the GDPR–for example, the California Consumer Privacy Act which we will introduce later in the chapter.[265] Additionally, Illinois, Texas, and Washington have biometric data privacy protection laws, which specifically regulate the use of the kinds of technology that landlords increasingly prefer for their buildings (e.g., facial recognition, heat tracking, and iris scanning).[266] Other states such as New York and Arkansas have expanded their consumer protection statutes to cover some aspects of data privacy, but no states beyond California and Virginia have stand-alone data privacy laws, nor, as discussed, is there a nationwide, federal law that regulates data privacy. Colorado and Virginia's privacy laws do not go into effect until 2023.

California, Virginia, and Colorado's data privacy laws, and the Illinois, Washington, and Texas biometric data privacy laws, are consumer protection laws and don't prohibit the use of any technology. Rather, they regulate the manner in which data is collected, stored, and used by companies, including landlord tech companies. They most often have higher notice requirements for the collection and sale of data than companies would be beholden to under national law. These laws could be powerful tools for regulators and activists who have concerns about the storage and usage of landlord tech-generated data, such as entry records or biometric markers.

New York enacted a data breach notification law called the Stop Hacks and Improve Electronic Data Security (SHIELD) Act in March 2020. This act, like many other data breach acts, requires certain data protection standards for businesses operating in New York that own or license private information. The law requires that companies develop cybersecurity standards and imposes fines for data breaches, but enforcement of the Act is only available to the New York Attorney General. New York state also became the first state to ban the use of facial recognition in schools in late 2020, but the moratorium does not extend beyond the education context. Tenant surveillance in New York is largely regulated by common law, landlord-tenant law and by statutes that penalize unlawful surveillance. New York State also has a law specifically regulating the surveillance of backyards by private individuals.[267]

Several other subject specific state laws regulating the use of facial recognition have passed. California also had a law on the books that prohibited police from using facial recognition in body cameras, AB 1215.[268] The law was not a permanent ban, but a three-year moratorium that expired on January 1, 2023. Vermont and Virginia have banned the use of facial recognition by law enforcement and Massachusetts has passed restrictions on its use by law enforcement.[269] Maryland has banned employers from using facial recognition applications during interviews.[270]

Algorithmic regulation that bears on automated decision making in tenant screening largely relies on statewide fair housing and consumer protection laws, as it does in the federal context. For example, the California Department of Fair Employment and Housing, the administrative agency that oversees the state's fair housing laws, issued regulations that went into effect in February 2020, and also expanded protections to include tenants' criminal history. In addition to FEHA, the Unruh Civil Rights Act is an additional source of protection for tenants in California. In New York, the Human Rights Law provides

protections against discrimination. Tenants facing discriminatory tech practices may have success challenging those practices under these kinds of state-wide laws.

Some states have written data protection for tenants into their laws. Specific tenant screening data protections were enacted by the California legislature in 2016, which amended Section 1161.2 and 1167.1 of the Code of Civil Procedure. The amendment changed the California housing law's code that permitted the sale of eviction (known in California as "detainer") proceedings after 60 days of a filing if the defendant did not prevail.[271] The act curtailed the ability of tenant screening bureaus to access court information. Other states, like Washington, have also placed limits on the information tenant screening companies can access. Washington's law places explicit limits on the dissemination of housing court records, but only upon the request of the tenant. RCW 59.18.367 allows tenants to obtain an order limiting the dissemination of an eviction proceeding on their record if: (a) The plaintiff's case was without basis, (b) Tenancy was reinstated, or other good cause exists. If such an order exists in writing, tenant screening providers are not permitted to use eviction records in tenant screening reports to generate tenant ratings or recommendations nor are they permitted to disclose them.[272] Such an order is called an Order of Limited Dissemination. Unlike other jurisdictions that automatically limit the dissemination of such records, tenants have to affirmatively ask for such records to be kept from tenant screening companies, which they often are unaware of having the option to do.

The California Consumer Privacy Act

In November 2020, the California Privacy Rights Act (CPRA; aka Prop 24, CCPA 2.0) was passed.[273] The CPRA, which is enforced by the California Attorney General and the California Consumer Privacy Agency, amends and expands the CCPA and goes into effect in July 2023. Notably, the CPRA defines "sensitive personal information" (i.e., a consumer's racial and genetic data, social security number, precise geolocation, etc.) and adds consumer protections regarding these types of data.[274] Given that California has been the birthplace of a slew of big tech companies, the CCPA and CPRA suite of regulations provide privacy protections for a substantial portion of consumers.

"If people just knew how much we knew about them, they'd be really worried," recounted Alastair Mactaggart, a real estate developer and privacy rights activist, of a conversation with a former Google tech engineer found in an LA Times piece about ballot measures on data sharing.[275] The enormity of personal data collected about individuals–from birthdates and shopping purchases to facial recognition–is difficult to comprehend. Even for tech companies that collect and profit from our data, managing such swaths of information is a feat. In fact, many tech companies are unable to fully account for where the wealth of data they have collected is stored and accessed. As participation in digital spaces increasingly becomes synonymous with participation in society, suspicious data harvesting practices are sometimes dismissed as collateral to play the "game."

Suspicions aside, the collection and sale of consumer data are how companies like Google and Meta make most of their revenue. In 2017, Statista reported that over 86% of Google's revenue came from advertising, which, according to cyber-security expert Maria

Kolokov, involves "violating your privacy."[276] As of 2021, that figure had dropped by only about 5%.[277] Yet, the tendrils of the data economy are not confined to search engines and social media. As we have detailed in this report, various manner of landlord technologies are employed to surveil, police, identify, profile, and beyond. We have also investigated these opaque digital entities to uncover user motivations and implementation of such technology. In this portion of the report, we will examine the historical background and policies, particularly in the San Francisco Bay area which have curbed (or sought to curb) the power amassed by tech giants and exploited by corporate landlords. Though several federal laws concerning the regulation of tech have been proposed, none have yet been passed. Thus, the burden of regulation has often fallen on states and municipalities.

Mactaggart cited the worrisome conversation with the "Xoogler" (ex-Google employee) as inspiration for the ballot measure he later proposed and financially supported which intended to "shift the balance of power over data sharing to consumers and punish businesses that don't toe the line."[278] While Mactaggart's professional background might imply a cocktail of conflicting interests–particularly in this report about landlord tech–the ballot measure became the California Consumer Privacy Act (CCPA) in 2018 after Mactaggart negotiated a deal with the state legislature. Enforcement of the CCPA began in January 2020 and allows consumers several rights.[279] Key points of the CCPA are that consumers may contact a company to 1) request what personal information a company has about them, 2) request that their personal information be deleted, and 3) sue a company if data is unprotected in a breach.[280] Often compared to the European Union's preceding General Data Protection Regulation (GDPR), the CCPA is more strict. For example, the CCPA details clear rights for consumers against retaliatory discrimination from companies if a consumer chooses to exercise their rights introduced in the Act.[281] Depending on the revenue of the company, both the GDPR and the CCPA provide wide-reaching regulations that follow an EU- or California-based company, respectively, if it operates outside California or the European Union.[282]

Cities in California

San Francisco became the first city to ban facial recognition software in 2019, with the "Stop Secret Surveillance" ordinance as part of a larger slate of surveillance oversight bills.[283] The ordinance prohibits the purchase of facial recognition software by city agencies, including the public housing authority. Because the ban is a government ban, private business and public individuals (including private landlords) are not banned from purchasing, using, and deploying this technology.

The lack of a private ban for facial recognition is a cause for concern for advocates. Already, San Francisco police have circumvented the facial recognition ban by following tips generated by a different agency.[284] San Francisco's bill has explicit carve outs for law enforcement's inadvertent use of the technology, and allows law enforcement to deviate from the policy for investigative purposes. Should facial recognition cameras proliferate in privately owned businesses, it's possible that police could use footage from those cameras for similar investigative purposes. Requesting the data from a facial recognition system would not violate the law.

Further, some homeless shelters in San Francisco have implemented monitoring systems such as biometric finger scans and photos to "track shelter usage."[285] Jennifer Friedenbach, executive director at the Coalition for Homelessness, stated that this process has "driven undocumented populations away from these shelters."[286] Thus, it is possible that a displaced tenant who suffered the harm of landlord tech by eviction might later be the victim of similar surveillance systems in a shelter for those who are unhoused.

In Oakland, the City's ban similarly prohibits the usage of facial recognition technology by city departments, including the police department. The Oakland ordinance also explicitly bans the use of information obtained by facial recognition software, a feature that goes further than the San Francisco ordinance.[287] Oakland's surveillance ordinance has a reporting requirement like that of the federal biometric housing ban. It also requires that any potential public use of surveillance be debated in a public discussion. In addition, the cities of Alameda and Berkeley have also placed limits on the use of facial recognition.[288] Like San Francisco, Alameda banned the use of the technology by its city departments, but has an exception for information received as a result of facial recognition used by an outside agency. Berkeley's ban came as an amendment to their general surveillance ordinance and is also an outright ban on the public use of facial recognition surveillance.

Models from other cities

Below, we overview legislation by cities in other states aimed at curbing the abuse of facial recognition technology.

How have cities outside of California addressed landlord tech abuse?

CITIES IN MASSACHUSETTS

Somerville, Massachusetts was one of the first two municipalities to enact a facial recognition ban, and the first jurisdiction on the East Coast to do so. Somerville's ban bars the use of any data collected with facial recognition "in municipal proceedings" — which would include eviction proceedings — and has a cause of action for residents to sue for violations of the law. Somerville is one of the leaders in this area in the country, also publishing an active camera map on its police department website.[289]

Several other Massachusetts towns and cities have followed Sommerville's lead in banning the technology: **Brookline, Cambridge, Northampton, Springfield,** and finally, **Boston,** which passed a ban in June of 2020.[290] Boston's ordinance bans the public use of facial recognition technology. A state-wide ban was nearly passed in December 2020, but was pared back at the last minute, turning to less-strict regulations instead of an outright ban.[291]

PORTLAND, OREGON

Portland's facial recognition ban is the strongest in the country and could serve as a model for the way to regulate landlord tech – it's one of only two bans that prohibit facial recognition use by private business as well as government agencies.[292] However, the ban on private businesses only extends to places of public accommodation, such as restaurants and stores. The use of facial recognition

landlords and private homeowners is not regulated by the Portland ordinance, as homes are not considered public accommodations.[293] However, the use of facial recognition by public entities, such as Portland's public housing agency, would fall under the prohibitions.

BALTIMORE, MD

In August 2021, the Baltimore City Council passed and enacted a bill banning the use of facial recognition by public and private entities within city limits.[294] The bill makes the use of FRS a misdemeanor with a fine of up to $1,000 or 12 months of imprisonment. However, the bill has a major carveout for biometric security systems that "protect against unauthorized access to a particular location", meaning that security systems that landlords use are not covered by the ban. The ordinance automatically expires at the end of 2022, unless an extension is approved by the Baltimore City Council.

NEW YORK, NY

In April 2021, the New York City Council passed a smattering of tenant protection bills including one of the few bills in the country that directly addresses the growing issue of landlord tech and how it interfaces with issues of access and housing justice. The Tenant Data Privacy Act requires that landlords who use smart access systems, such as GateGuard or StoneLock, provide their tenants with data retention and privacy policies, as well as limits the ability of data retention from these systems by requiring consent, restricting sharing of information with third parties, and giving specific data retention limits.[295] The TDPA also forbids the sale of biometric identification data and completely bans its use on minors without parental consent. The legislation will go into effect on January 1, 2023.

Additionally, in July 2021, New York City amended the local administrative code to include regulation of biometric identifier information.[296] The law regulates how businesses keep and use biometric identifiers, including a ban on selling such data, but does not apply to residential buildings. The law also requires that businesses notify consumers of the collection of biometric data. Both laws have a private right of action that provides statutory damages ranging from $200 to $5000 for individuals whose information was sold.

Prior to the 2021 legislation, the City Council considered the The KEYS (Keep Entry To Your Home Surveillance-Free) Act, which required physical keys. That bill would have gone further than the current legislation which only regulates data management.[297] The proposed bill came on the heels of a tenant winning the right to a physical key in settlement after filing suit in 2018.[298] The bill never passed.

History of Housing and Evictions in the Bay Area

The rise of corporate landlords in San Francisco has played a major role in the current eviction crisis, displacing long-term residents to create more rental properties, and decreasing access to the already limited housing pool. The 2007-2009 Great Recession catalyzed the shift of home ownership from residents to corporate landlords, creating a new asset class of single-family rental homes. Amid home foreclosures during the recession, efforts to reorient the housing market back towards community owners failed as real estate investors rapidly bought up properties—facilitating a major transfer of wealth from households to private-equity firms. These investors purchased homes en masse, typically lower-priced properties in neighborhoods with a higher percentage of Black residents,

A SUMMARY OF MAJOR POLICY QUESTIONS

Several important questions guide policy considerations, both in its formulation by legislators and use by tenant organizers. Two biometric privacy acts, the Illinois Biometric Information Privacy Act (BIPA) and the Texas Capture or Use Biometric Identifier Act (CUBI), will serve as a model of how certain factors dictate the range of functional options available to tenants seeking remedy.

Who does it protect?

An important distinction between BIPA and CUBI is the language each uses to describe the information at hand. Where BIPA defines biometric information as well as biometric identifiers, CUBI defines only the latter. While this may seem a minor language substitution, biometric information is generally more expansive, with BIPA defining such information as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." Biometric identifiers, on the other hand, are limited within the context of BIPA to "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." CUBI mirrors this definition almost exactly.

Who can enforce the law?

The ability of individuals to challenge privacy invasions is directly tied to the overall utility of a policy for grassroots organization. Illinois' BIPA has a powerful private right of action, unlike Texas' CUBI, which has led to a significant influx of private challenges utilizing BIPA. In the case of CUBI, only the Texas Attorney General can pursue violations of the law.

What are the damages?

Civil penalties for CUBI are capped at $25,000 per violation, whereas BIPA provides for statutory damages of up to $1,000 per negligent violation and up to $5,000 per intentional or reckless violation.

What is the timescale?

Unlike BIPA's 3-year destruction requirement, CUBI solely requires destruction within a "reasonable amount of time" though no later than one year after the purpose of the collection has lapsed in relevance.

who were targeted by predatory lenders and therefore impacted disproportionately by foreclosures. Today, corporate landlords own roughly half of the rental market, and as the industry expands, their opposition to strengthening tenant protections is closely tethered to their own financial gain––creating a cycle of gentrification, unjust evictions, and housing instability.

Landlords are additionally incentivized to convert properties and evict tenants as the second tech boom in San Francisco and the Bay continues to bring a wave of new, affluent, employees who are willing and able to pay these rent increases. This makes access to housing even more competitive, leaving current residents at a disadvantage as landlords cater to the new tech demographic. Due to tenant protections such as the San Francisco Rent Ordinance of 1979, landlords cannot increase rent by more than a pre-approved percentage determined by the San Francisco Rent Board annually, currently 2.3% as of

2022, complicating their ability to capitalize on the high demand for housing. Under this ordinance, landlords must also have a "just cause" to evict tenants to prevent arbitrary, retaliatory, or discriminatory eviction practices. Just causes for eviction include: nonpayment of rent, unapproved subtenants, breach of contract, substantial damage to a unit, etc. Rent control practices in San Francisco are essential in protecting tenants, however, the ordinance excludes buildings with a certificate of occupancy dated after 1979, as well as single family homes and commercial units, leaving 40% of rental units vulnerable to rent spikes and unjust evictions. During the COVID-19 pandemic, eviction moratoriums for non-payment of rent were passed to ensure tenants would not lose their homes due to pandemic related hardship, which has since seen amendments and extensions into 2022.

Despite these safeguards, landlords employ workarounds to evict current tenants by pursuing nuisance evictions or invoking the Ellis Act. Low-fault or nuisance evictions are subjectively defined as anything that interferes with the comfort and enjoyment of the landlord or other tenants on the property. This acts as a sort of loophole, allowing landlords to evict tenants over minor but easily corrected offenses. For example, residents in a single-room occupancy hotel in Chinatown received eviction notices for hanging laundry outside their windows, or other low-fault "offenses" including leaving a stroller in the hallway or living with a new roommate. While other eviction methods decline in usage due to tenant protections, particularly from moratoriums, notices filed as nuisance evictions have increased by 25% between 2021 and 2022, cementing its use as a workaround. The Ellis Act is a California state law passed in direct response to the California Supreme Court's decision in Nash v City of Santa Monica which provides landlords with the right to evict tenants in order to "go out of business."[299] The usage of Ellis evictions has spread beyond solely landlord retirement, as newly vacant buildings are often converted into condos or group-owned-tenancy-in-common flats (TICs) which then become exempt from rent control ordinances––regardless of the building's age or which long-term residents occupied these rental properties. Without a limit on the number of times a building owner can "go out of business," many use the Ellis Act to mass-evict tenants to flip buildings for a profit or convert housing into short-term rental units, exacerbating the housing crisis.

Interpretation of the Ellis Act by the First Appellate District of the California Court of Appeals affirms tenants' retention of retaliatory rights under Ellis Act evictions, and the San Francisco Tenants Union states that tenants who fight Ellis evictions have greater than expected success, often winning outright or at least finding a settlement on their terms.

New Types of Surveillance

While human biometrics are a developing area of consumer protections, animal biometrics and bio-identifiers remain fair game. Though something of an oddity in the applications of landlord tech, some landlords have taken to writing lease clauses requiring forfeiture of dog DNA and submission to fecal matter testing in an effort to

Atlas of Surveillance Data for SF County

AGENCY	DESCRIPTION	TECHNOLOGY	VENDOR
San Francisco Municipal Transit Authority	The San Francisco Municipal Transit Authority acquired AISight predictive policing in 2012	Predictive policing	AISight
San Francisco State University Police Department	The San Francisco State University Police Department uses body-worn cameras	Body-worn cameras	Axon
Northern California Regional Intelligence Center	The Northern California Regional Intelligence Center, a fusion center, uses face recognition technology, often in support of other law enforcement entities in the San Francisco Bay Area	Facial recognition	Unknown
San Francisco Police Department	The San Francisco Police Department has been using Shotspotter gunshot detection since 2008	Gunshot detection	Shotspotter
Northern California Regional Intelligence Center	The Northern California Regional Intelligence Center is one of 79 fusion centers in the United States. Operated by local and state law enforcement in partnership with the U.S. Department of Homeland Security, a fusion center serves as a command center for gathering, analyzing and disseminating intelligence and other public safety information.	Fusion center	Unknown
Northern California Regional Intelligence Center	About 29 agencies collectively submitted 40 million license plate scans to the Northern California Regional Intelligence Center between October and December 2019.	Automated license plate readers	Vigilant Solutions
San Francisco Police Department	The San Francisco Police Department acquired cell-site simulator technology in 2009, according to data compiled by Kevin Collier for Vocativ.	Cell-site simulator	Unknown
San Francisco Police Department	The San Francisco Police Department operates automated license plate readers and accesses external ALPR data.	Automated license plate readers	Neology/ PIPS
San Francisco Sheriffś Office	The San Francisco Sheriff's Office uses Axon body-worn cameras in San Francisco jails.	Body-worn cameras	Axon
Presidio National Park Police	The San Francisco Recreation and Park Department's Twitter account includes a photo of SF-based Park Rangers wearing the Axon Body 2.	Body-worn cameras	Axon
SF District Attorneyś Office	The San Francisco District Attorney's office maintains a camera registry.	Camera registry	Unknown
U.S. Customs and Border Protection - San Francisco Intl. Airport	SFO International Airport is one of 18 airports where Customs and Border Protection is using face recognition technology as of March 2019. An executive order signed by Pres. Trump in 2019 requires Customs and Border Protection to install face recognition technology at the United States' top 20 airports by 2021.	Face recognition	Unknown
San Francisco Police Department	The San Francisco Police Department purchased Axon body-worn cameras in 2014 as part of a pilot program. It formalized its BWC policy in 2016.	Body-worn cameras	Axon

cull dog waste on their properties. Dogs' mouth cells are swabbed and collected, then registered in a genetic database. If waste is later discovered on the property, it is promptly swabbed and submitted to a lab, and the genetic information gleaned from the sample is matched within the established library of pets at the property. Owners may be subject to a fine ranging $100 to $350 for a single offense under such clauses. Such programs are present in at least 100 properties in the San Francisco area. While such programs may seem like relatively harmless technological gimmicks, they nevertheless have concrete consequences for tenants in their ability to provide petty lease violations which grant landlords just cause required under the San Francisco Rent Ordinance for evictions.

Two companies presently lead this canine genetics niche: BioPet Laboratories, who offer their services through PooPrints, and Mr. Dog Poop. The latter's founder, Mark Guarino, had originally intended on using dog DNA libraries to establish the canine equivalent to CODIS, the FBI's national forensic database, and selling access to the database to law enforcement, but the program failed to get traction and was reworked to provide private services. BioPet Laboratories specializes in animal genomics, holding a proprietary database, the DNA World Pet Registry, and providing (in addition to PooPrints) DNA proof of parentage services as well as a dog bite DNA identification service allowing for preservation of evidence after bites occur.

These companies claim their analyses' dog identification to be nearly incontrovertible (with PooPrints, for example, claiming a 1 in 24 sextillion chance of inaccuracy), but it is impossible to assess the accuracy of such a claim. This is in part because the genotyping panels utilized by the laboratories are proprietary, meaning that the genes of interest in each analysis are not shared with the public. Nevertheless, there are several reasons to be suspicious of the true accuracy rate of these companies' DNA assays. Random match probability is cited as the primary means of matching genetic signatures obtained from samples to implicate a specific dog with great accuracy, but without more detail on the gene assay itself, the usefulness of the established gene panel remains unclear. Furthermore, fecal matter is a relatively poor sample for DNA analysis to begin with. Not only is DNA low-abundance in these samples, they are also subject to enzymatic and environmental degradation which can compromise the fidelity of amplification signals in subsequent genotyping. Furthermore, apartment complexes are often prime sites for sample cross-contamination due to the high density of dogs living in a relatively small community, further increasing the chance of compromising the fidelity of the final genetic signals. Given the potential complications involved in DNA assays of pet waste, it is not unreasonable to imagine that dog waste fines might be used as a pretext to evict some pet-owning tenants.

A final note regarding these technologies is their contributions toward normalization of invasive informatics practices which are far outside of the normal purview of health. While dog waste sleuthing remains an outlandish application of biometric and genetic surveillance, its presence contributes another step toward encroachment on personal privacy.

CHARACTERIZING THE LEGAL LANDSCAPE FOR TENANTS IN SAN FRANSISCO

Fair Housing

As discussed in the earlier Tenant Screening section of this report, tenants are often subject to scrutiny during the application process along the lines of criminal background, credit score, and eviction reports, which are compounded and aggravated by algorithmic processes. Several legal routes are, however, available as potential remedies for discrimination.

Harrassment and Retaliation

Landlord use of cameras can constitute harassment when cameras are installed and misused, often for the purpose of eavesdropping on tenant activities or as retaliation when tenant-landlord relations diminish. As such, surveillance equipment which is demonstrably installed for the purpose of intimidation in response to tenant complaints, or for monitoring tenant activities in a manner that violates their privacy, can be challenged under the California Civil Code or San Francisco's Administrative Code. California's Civil Code prohibits landlords from harassing or retaliating against tenants exercising their legal rights in Section 1940.2, specifying that landlords may not engage in "menacing conduct constituting a course of conduct that interferes with the tenant's quiet enjoyment of the premises."[300] Furthermore, under Section 37.10B of San Francisco's Rent Ordinance, $1,000 may be awarded for each harassment offense, while $2,000 statutory damages may be pursued for each such threat under California Civil Code §1940.2.[301] Documented proof of retaliation or harassment in such challenges (for example, written documents that establish a paper trail of deteriorating tenant-landlord communications) can strengthen the cases of tenants pursuing lawsuits under these laws.

Fair Housing Act (Civil Rights Act of 1968 Titles VIII and IX)

The Fair Housing Act (42 U.S.C. 3601 et seq.) forbids direct housing providers from making housing unavailable on the basis of race or color, religion, sex, national origin, familial status, and disability.[302] The Supreme Court established in Texas Department of Housing and Community Affairs v The Inclusive Communities Project (2015) that disparate-impact claims could be made through the Fair Housing Act under similar requirements to Title VII of the Civil Rights Act of 1964. Plaintiffs are required to demonstrate an available alternative which would eliminate or reduce the disparate-impact claim at issue, while housing providers are given opportunity to offer a valid interest rationale for denial of housing.[303] As with Title VII, the Court identifies prevention of racial quota enforcement as a major legislative motive behind disparate-impact analysis, though it

"[p]olicies, whether governmental or private, are not contrary to the disparate-impact requirement unless they are 'artificial, arbitrary, and unnecessary barriers" as established in Griggs v Duke Power Co (1971).

Tenants may file challenges against a housing provider if they believe that discrimination on any of the bases above is functioning to deny individuals housing. Practically, however, pursuit of challenges through the Fair Housing Act tends to be prohibitively costly for many tenants, both in terms of finance and time spent, and there is not a requirement that the housing in question be awarded to the plaintiff upon successful challenge.[304]

California Fair Employment and Housing Act

At the state level, California Fair Employment and Housing Act of 1959 prohibits harassment or discrimination in all aspects of housing if such actions are based on protected characteristics such as race, color, national origin, ancestry, religion, sex, gender, marital status, military status, familiar status, income source, disability, or genetic information.[305]

Unruh Civil Rights Act

The Unruh Civil Rights Act of 1959 (California Civil Code §52) prohibits all California businesses from engaging in discrimination against consumers. If a housing provider qualifies as a business, this act protects tenants against discrimination based on citizenship, immigration status, primary language, and age.[306]

Privacy

California is among the most protective states in terms of privacy, particularly in regards to personal data. In 1972, Article I, Section 1 of the California constitution was amended to include privacy as an inalienable right, a value which is reflected often in the state's subsequent policy developments.[307]

California Penal Code

The California Invasion of Privacy Act (CIPA) is outlined by Chapter 1.5 of the California Penal Code (Sections 630-638.55). Section 630 defines not only the scope of privacy concerns that motivate the introduction of wiretapping regulations but also a general intent by the Legislature not to "place greater restraints on the use of listening devices and techniques by law enforcement."[308]

While the original text of CIPA regards telegraphic and telephonic communications, videotaping has come to be included under the umbrella of regulation. In People v Gibbons (1989), the Fourth District Court of Appeals of California held that while sections 630 and 632 do not make explicit determinations on the applicability of CIPA to videotaping, the court nevertheless finds "that a video recorder is an instrument which, if used in the

manner proscribed under section 632, is a recording device for purposes of the privacy act."[309] As such, video cameras may be considered tools for eavesdropping that may be challenged under CIPA.

Separately, §647 subdivision j of the California Penal Code establishes that it is a misdemeanor to, "by means of any instrumentality," look through a hole or opening of any area "in which the occupant has a reasonable expectation of privacy, with the intent to invade the privacy of a person or persons inside."[310] Examples of spaces falling under this protection include bedrooms, bathrooms, and dressing rooms, but the nature of intrusion also plays a factor in how an instance of surveillance may be challenged. For example, in Claudia Tirado et al. v Jack Halprin et al., a case filed after Google lawyer Jack Halprin attempted Ellis evictions on tenants in San Francisco, Halprin had installed a security camera directly outside a tenant's door without their consent, an action the plaintiffs challenged as a violation of their privacy under CIPA.[311]

San Francisco Administrative Code Sec. 19B (Acquisition of Surveillance Technology)

Section 19B is an amendment to the San Francisco Administrative Code made effective July 15, 2019. It requires that departments of the city of San Francisco that seek to acquire surveillance technology or access surveillance information from non-city entities submit both a Surveillance Technology Policy ordinance as well as a Surveillance Impact Report to the Board of Supervisors.[312] The original ordinance (Ord. 107-19) amending the Administrative Code also provides the power of annual auditing to the California State Controller to ensure that standards in accordance with Sec. 19B are maintained.[313] In an ongoing challenge, Williams et al. v. City and County of San Francisco (CCSF), the ACLU of Northern California has filed suit against the San Francisco Police Department, alleging that police violated Section 19B of the San Francisco Administrative Code by exploiting live footage from a large private camera network, an action that was recorded and reported by the Electronic Frontier Foundation, to perform mass surveillance on activists during demonstrations following George Floyd's murder.[314] The plaintiffs filed their original complaint in October of 2020, and at the time of this report's writing, the case remains ongoing, with an amicus brief filed in January of 2023 by the Asian Law Caucus and Black Movement-Law Project along with additional amici.[315]

Consumer Protection

Fair Credit Reporting Act

The Fair Credit Reporting Act establishes standards of practice for accurate and fair reporting of credit, requiring that agencies behave "in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information."[316] Authorization and responsibility for the enforcement of this act is given to the Federal Trade Commission.

California Civil Rights Department (CRD)

The California Civil Rights Department (formerly known as the California Department of Fair Employment and Housing) is responsible for the enforcement of California civil rights laws in order to "protect the people of California from unlawful discrimination in employment, housing, businesses, and state-funded programs, and from bias-motivated violence and human trafficking."[317] As such, tenants may file housing discrimination complaints (such as with CRD).

Department of Housing and Urban Development (HUD)

At the federal level, the Department of Housing and Urban Development is responsible for handling complaints about violations of civil rights in any programs under their jurisdiction. Complaints may be filed under the Fair Housing Act for both public and private housing operations or under a number of laws embodying protected classes if the complaint regards housing and community development programs (including Title VI of the 1964 Civil Rights Act, Section 109 of the Housing and Community Development Act of 1974, Section 504 of the Rehabilitation Act of 1973, Title II of the Americans with Disabilities Act of 1990, the Architectural Barriers Act of 1968, the Age Discrimination Act of 1975, and Title IX of the Education Amendments Act of 1972).[318]

Federal Trade Commission (FTC) and Consumer Financial Protection Bureau (CFPB)

If outdated or incorrect information that may jeopardize an applicant's access to housing is present in a tenant profile, requests may be filed with the Federal Trade Commission and Consumer Financial Protection Bureau to correct the inaccuracies.

LOOKING FORWARD

This report has highlighted numerous harms associated with landlord technologies in San Francisco and beyond. In addition to historicizing the utilization of surveillance technologies by landlords, police, and public housing authorities, it has illustrated new examples of private landlord technologies such as digital doormen and neighborhood app-based policing. It also has mapped out ongoing struggles against sharing economy rental platforms and tenant screening systems–both of which also comprise invasive landlord technologies of property and data grabbing, and both of which also lay out some potential precedent for legislating against the private use of landlord tech. Our policy section meanwhile has traced relevant housing and privacy legislation implicated in contemporary landlord tech contexts in San Francisco, California, and the broader United States.

So what to do next? Luckily there is much inspiration to draw from in conceptualizing anti-landlord tech organizing. Groups such as the Tech Equity Collaborative for instance have put together a "Residential Proptech Ethical Practice Guide," which offers suggestions for companies themselves to embrace data minimization policies and to learn from groups actively engaged in studying the harms of algorithmic bias and in organizing against housing injustice.[319] They also suggest that employees working for many landlord tech companies also have the power to organize for better and less harmful products, and that there remains much to do regarding labor organizing in proptech companies. There is also much to do by way of testing products before they are deployed in tenants' homes and communities, and by way of providing accessible and accurate information regarding where data collected about tenants lives and transits, and how it could be used against tenants. Tenants arguably should have the option to consent into using and being used by landlord tech.

Meanwhile, abolitionist groups such as Critical Resistance have long been organizing and providing resources to embolden the abolition of the prison industrial complex, or "the overlapping interests of government and industry that use surveillance, policing, and imprisonment as solutions to economic, social, and political problems."[320] And as Michelle Alexander reminds us,"'Mass incarceration' should be understood to encompass all versions of racial and racial and social control wherever they can be found, including prisons, jails, schools, forced 'treatment' centers, and immigrant detention centers, as well as homes and neighborhoods converted to digital prisons."[321] As landlord technologies make clear, incarceration and policing transfer policing power to landlords and neighbors, where homes and neighborhoods become laboratories of surveillance and corollary gentrification.

Rather than relying upon techniques that seek to mitigate police power by handing it over to local civilians (ie. NextDoor), Critical Resistance argues to shift funding priorities from those of law enforcement to those of community well-being."[322] This means prioritizing housing, education, health care, meaningful work, and other critical needs. This aligns with the broader movement to defund the police amplified in the aftermaths of the police murder of George Floyd.

A.I.M.S.

1 AUDACITY TO ASK

You have a right to ask, WHO, WHAT, WHERE, WHEN, & WHY?" when your landlord is doing anything that brings you concern or worry. It is your right to question that of which you're not sure of. ALWAYS EXERCISE THAT RIGHT. ALWAYS HAVE THE AUDACITY TO ASK. QUESTION EVERYTHING.

2 INFORM YOURSELF & OTHERS

RESEARCH the technologies your landlord is investing in and SHARE it with your neighbors. It isn't likely that you will get full transparency about their motives & intentions, but you and your fellow tenants can INFORM & EQUIP yourselves with the information to push back step by step.

3 MOBILIZE YOURSELF & OTHERS

Organize your fellow tenants & yourself. Having recurring meetings with your neighbors helps build the COMMUNAL VOICE, PRESENCE, & CONFIDENCE necessary to push back against tech deployment in your community. Pro Tip: divide the responsibilities to avoid burnout.

#NOTMYBIOMETRICS

Art and agency are key elements in strengthening the voice of our community. Art will allow us to create space of trust through which we can achieve common goals through series of workshops lead by The OceanHill-Brownsville Alliance

#NOTMYBIOMETRICS

WE ARE RE-THINKING;
how we interact with tech. Acknowledging the fact that it's ok to decline permissions and weigh the outcomes of sharing our data.

AGENCY
One's agency is one's independent capability or ability to act on one's will. The belief that your own actions matter. This ability is affected by the belief structure which one has formed through one's experiences, and the perceptions held by the society and the individual, of the structures and circumstances of the environment one is in and the position they are born into.

PRIVACY
the state or condition of being free from being observed or disturbed by other people.

OCEANHILL-BROWNSVILLE ALLIANCE

We are LOCAL.
OceanHillBrownsvilleAlliance@gmail.com
Find helpful links & resources at:
www.OceanHillBrownsvilleAlliance.com

THE GOAL.

Equipt members of gentrifying neighborhoods with the knowledge of artificial intelligence technology, biometric collecting systems, hardware, apps, and automated decision making systems. Through workshops, collaborative art sessions and coaching we plan to instill the confidence and information on tech advancements and policy needed for community members to advocate for themselves and to have agency over the spaces they occupy and call home.

TURN THE HEAT UP!

4 MEET OTHER GROUPS

5 MAINTAIN PUBLIC PRESENCE & PRESSURE

6 STRATEGIZE

7 SEIZE THE MOMENT & SPEAK

8 SUPPORT (GIVE & ACCEPT)

You can find the expanded version of these steps at:

www.OceanHillBrownsvilleAlliance.com

PRIVACY IS A RIGHT TO EVERY INDIVIDUAL AND THERE DATA.

LET'S EQUIP OURSELVES TO PROTECT OUR DATA FUTURES

DATA PRIVACY AWARENESS

A bite sized brochure for the everyday tenant; someone who has to defend themselves from unwanted and deceitful surveillance and tracking technologies.

The Pocket Pack

We are LOCAL.
OceanHillBrownsvilleAlliance@gmail.com
www.OceanHillBrownsvilleAlliance.com
(347) 454-6629

OBA Ocean Hill–Brownsville Alliance
EMPOWERING COMMUNITIES. PROTECTING FUTURES.

TALK TO YOUR ELECTED OFFICIALS

...KNOW YOUR DISTRICT

41st [Council District]

9th [Congressional District]

55 [Assembly District]

16 [Brooklyn Community Board]

WE NEED YOUR INPUT !

Help organizers and tenants push back against invasive landlord tech by sharing your experiences about the ways that your building and neighborhood is installing technology. Has your landlord introduced new tech for managing your building?

RESOURCE 01.
Log on to:
https://antievictionmappingproject.github.io/landlordtech/

Fill out this survey and let us know.

The team at OBA feels this is a great introduction landlord tech and a way for us to find and assist those being effected.

WHY?

Residents in gentrifying and marginalized areas must have a say and be involved in the deployment of any tech that will have the capacity to identify and/or track individuals. As the implications of this tech could lead to very dangerous outcomes for those having to interact with them while giving companies more leverage and data to improve their systems and software.

#NOTMYBIOMETRICS

Info Packet: Action Plan for Tenants Who Want to Defend Themselves from Landlord Tech by the Ocean-Hill-Brownsville Alliance

ORGANIZING

As a project, the Anti-Eviction Mapping Project and Anti-Eviction Lab have been inspired by tenants and privacy advocates working organizing against the private use of landlord tech in New York City. On April 30th, 2019, Brooklyn Legal Services filed legal action with New York State's Home and Community Renewal on behalf of 130 residents of Atlantic Plaza Towers (APT) . Meanwhile, direct action organizing, media campaigns, and solidarity building led to the tenants' fight receiving significant attention. By November 2019, Nelson Management announced that they would rescind their application to install StoneLock Frictionless Solutions in their housing complex. This housing justice and anti-surveillance victory was the result of a two-year long tenant-led organizing campaign that utilized a combination of direct action, media outreach, and alliance building. Their victory serves as inspiration for all those looking to keep landlord tech out of their buildings, and for those invested in bringing together the work of housing and technological justice.

OceanHill-Brownsville Alliance Guide After successfully fighting Nelson Management's deployment of facial recognition at APT, Tranae' Moran co-founded the OceanHill-Brownsville Alliance in order to create knowledge and share tactics for fighting back against landlord tech at Atlantic Towers and beyond.

On page 76 we include the group's Action Plan for Tenants Who Want to Defend Themselves from Landlord Tech, to further share this knowledge.

There are many lessons to learn from APT and the OceanHill-Brownsville Alliance for tenant organizers in San Francisco. There is also much research to be done to better understand the landscape. Some of the resources below are aimed to help. However, if you are a tenant in San Francisco seeking immediate support, we recommend you contacting a tenant support group. There are many resources listed on the website of the SF Anti-Displacement Coalition, which can be a good starting place.[323]

DATA SCRAPING GUIDE

Landlords constantly surveil tenants — yet data about how and where landlords are deploying new technologies of surveillance is not readily available. Landlords do not have to disclose when they install new tracking systems in their buildings — and oftentimes, tenants are not even notified nor asked to opt-in. As tenants, researchers, and organizers, we often need to be creative with our research tactics. One unlikely, but valuable, source of data that can help track where landlord tech is being deployed is Instagram. Certain companies that install new high-tech building-entry systems like to flaunt them on their social media feeds, and sometimes they go as far as tagging the neighborhood as the "location" for the post, and/or indicating the exact building address in the post description. For this reason, we have begun scraping data from landlord tech companies' Instagram accounts. Below is a short guide based on what we have tried so far.

Step 1: Identify Social Media Presence

If you want to research a specific landlord tech company, the first step is to go to their website and see if they have any social media accounts. Sometimes, these can be found in the footer of the website, or you might want to look up "Instagram + 'Company Name'" on a search engine and see what comes up. If the company has an Instagram account, read a few posts and see if there is any information about specific locations (cities, neighborhoods, buildings) that could locate where their technology is being deployed.

Step 2: Scrape Data

Once you have identified one or more companies whose social media accounts could be fruitful as a data source, you are going to need to "scrape" the data — in other words, find a way to bulk download the information they have posted on their social media page. Alternatively, you could do it manually and write down the information contained in each post into a spreadsheet — but that takes a long time.

There are many ways to scrape data. One platform is Octoparse,191 a web scraping tool that comes with a handful of free templates. Templates are great if you do not have software engineering experience — they allow you to scrape data without writing your own code. One shortcoming of Octoparse however, is that the free version only lets you scrape up to 8,000 hours (roughly 300 days) of social media posts — so you won't be able to scrape the entire company's social media account. Alternatively, if you have some coding experience, you could look for a code repository that guides you through the steps involved in data scraping. For example, the following GitHub repository guides you through using a data scraper built with Python: https://github.com/arc298/instagram-scraper

Step 3: Export and Clean Data

Upload the data you scraped into Google Sheets, Airtable, Excel, LibreOffice, or other spreadsheet software of your choice. Read through your data and clean up the spreadsheet to only keep information that you are interested in. This is a sample spreadsheet with data scraped from the Instagram account of virtual doorman company Carson (@carson.live). Each row represents a different Instagram post from Carson. Each column contains a different set of information scraped from the post (ex: description, location, photo, hashtags, etc).

Step 4: Additional Data Sources

Once you have a clean spreadsheet with scraped social media data, you may want to add more information based on how you'd like to use it. For example: If you want to visualize your data by mapping it, you will need to "geocode" it. That means, for any post with a specific location (ex: San Francisco, CA or "55 Dolores Street, San Francisco, CA"), you will need a "latitude" and a "longitude" to place it on a map. You can geocode points individually by inputting addresses into LatLong.Net,[324] or using a batch geocoder like Geocod.io.[325]

Step 5: Ground Truthing

Digital data and maps often include blind spots, misrepresentations, and inaccuracies. They also tend to obscure on-the-ground observations and present a top-down view, gazing down on our cities. If you are able to, it could be fruitful to "ground-truth" the data you have found through web scraping. Find a data point near you, in your neighborhood for example, and go check out the building. Do you see a new video intercom installed in the entrance way, or any other signs of landlord tech? If you feel comfortable, Left and above: Carson boasts of new systems that they have set up in San Francisco on Instagram. take a picture to show what you find, and contribute it to our growing body of crowdsourced data on the Landlord Tech Watch site.[326]

Data Scraping Guide by the Anti-Eviction Mapping Project

PUBLIC RECORD REQUESTS

The State of California is beholden to the Brown Act and the Public Records Act, which allows local city and county governments to enact ordinances allowing a greater right of access to public records. These are known as the Sunshine Laws, or the Sunshine Ordinance. In San Francisco, it's established under Chapter 67 of the city's Administrative Code.

San Francisco, Oakland, and a number of other cities also now use the platform NextRequest, a Freedom of Information Act (FOIA) service. This enables members of the public to request government records online.[327] Interested parties can also send requests to any city or state agency that regulates housing. For publicly funded buildings that are facing installation of facial recognition access systems.

COMMUNITY-PRODUCED RESEARCH

Public record requests can be very useful for requesting data related to public housing, registered alarm companies with the city, or police surveillance. There is no database of what private landlords use landlord technologies as this data isn't recorded with the city. There is also no database of evictors or of Airbnb mega hosts.

This is in part why the Anti-Eviction Mapping Project has created Evictorbook, a tool that allows tenants to see landlords' portfolios and eviction histories,[328] and why groups like Inside Airbnb have created their own public system of revealing Airbnb information.[329] Lack of information about private landlord use of surveillance is in part what has motivated the writing of this report, alongside projects such as Landlord Tech Watch.

Resources on how to understand landlord tech from a tenant harms perspective, as well as a growing crowdsourced map of landlord tech deployment can be found on Landlord Tech Watch.[330] Visit the site to add your own story to the map and learn more about other tenant experiences. Landlord Tech Watch was created by the Anti-Eviction Mapping Project, [people power media], the OceanHill-Brownsville Alliance, and the AI Now Institute as a resource for tenants and those working at the intersections of housing, racial, and technological justice. It has since partnered with the Anti-Eviction Lab, hence this report. As a project, it calls for the abolition, rather than only the reform of landlord tech. This does not mean adopting a neo-luddite position towards all technology, and on contrary, Landlord Tech Watch participates in what Steve Mann calls "sousveillance," or "surveillance from below," engaging in practices like recording police behavior or using cameras to prove that landlords are unlawfully evicting tenants.[331] Practices such as this get at what Ruha Benjamin describes as "abolitionist tools" to be used against what she describes as "the new Jim Code," or the racist designs baked into today's

technologies.[332] As an abolitionist tool, Landlord Tech Watch flips the gaze back upon the landlord technologies often used to spy on tenants, execute evictions, and abet racial dispossession, while offering resources on how to organize against facial recognition from being deployed in one's home. Our report on landlord tech serves as an extension of Landlord Tech Watch, aiming to produce knowledge useful in abolishing the harmful systems currently targeting and capitalizing upon tenant lives, data, and homes. By better understanding landlord tech, its geographies, and its associated harms, we can better fight back against it.

ENDNOTES

1 McElroy, Erin, Manon Vergerio, and Paula Garcia-Salazar. Landlord Technologies of Gentrification: Facial Recognition and Building Access Technologies in New York City Homes. Anti-Eviction Mapping Project, 2022. https://doi.org/10.13140/RG.2.2.24726.11841.

2 Anti-Eviction Lab, "Landlord Tech Watch," Anti-Eviction Lab, accessed April 25, 2023, https://www.antievictionlab.org/landlord-tech-watch.

3 Joe Kokura, "Supervisors Approve 60-Day Extension of SF Eviction Moratorium," SF Fist, March 22, 2023, https://sfist.com/2023/03/22/supervisors-approve-60-day-extension-of-sf-eviction-moratorium/.

4 Dani Anguiano, "Ex-San Francisco Official Accused of 'Terrorizing' Unhoused People with Bear Spray," The Guardian, April 27, 2023, sec. US news, https://www.theguardian.com/us-news/2023/apr/26/san-francisco-bear-spray-attacks.

5 Tana Ganeva, "Upheaval in the San Francisco DA's Office After Brooke Jenkins Appointment," The Intercept, July 17, 2022, https://theintercept.com/2022/07/17/brooke-jenkins-san-francisco-district-attorney-chesa-boudin/.

6 Nellie Bowles, "How San Francisco Became a Failed City," The Atlantic, June 8, 2022, https://www.theatlantic.com/ideas/archive/2022/06/how-san-francisco-became-failed-city/661199/.

7 Brad Dress, "San Francisco OKs Surveillance Plan Allowing Police to Access Private Cameras in Real Time," Text, The Hill, September 22, 2022, https://thehill.com/homenews/state-watch/3656738-san-francisco-oks-surveillance-plan-allowing-police-to-access-private-cameras-in-real-time/.

8 Josh Barbanel, "Outside Public Housing, Cameras Abound." The Wall Street Journal, June 5, 2014, https://www.wsj.com/articles/police-identify-suspect-in-prince-joshua-avittos-fatal-stabbing-in-brooklyn-by-matching-dna-on- the-knife-1401906762.

9 Nick Pinkerton, "A Thousand Unblinking Eyes: A History Cinema and surveillance from Fritz Lang to Michael Mann." The Baffler, No. 40 (JUL-AUG 18), pp. 36-43.

10 Christopher Williams. "Police Surveillance and the Emergence of CCTV in the 1960s." Crime Prev Community Saf 5, 27–37 (2003); Gary C. Robb, "Police Use of CCTV Surveillance: Constitutional Implications and Proposed Regulations, 13, p. 573. U. MICH. J. L. REFORM 571 (1980).

11 Michael Batty, The New Science of Cities, (MIT Press, 2013).

12 Shannon Mattern, A City Is Not a Computer: Other Urban Intelligences, (Princeton University Press, 2021).

13 Brian Jefferson, Digitize and Punish: Racial Criminalization in the Digital Age. (University of Minnesota Press, 2020), p. 174.

14 Eric L. Piza, "The Crime Prevention Effect of CCTV in Public Places: A Propensity Score Analysis," John Jay College of Criminal Justice Publications & Research (2018).

15 Andrew Dudley, "Lights, Cameras, Inaction: San Francisco's Broken Surveillance State." Hoodline, October 19, 2014, https://hoodline.com/2014/10/lights-cameras-inaction-san-francisco-s-broken-surveillance-state.

16 Heather Knight, "50 Cameras Set for Public Housing Sites." SF Gate, September 9, 2006, https://www.sfgate.com/bayarea/article/SAN-FRANCISCO-50-cameras-set-for-public-housing-2489168.php.

17 Richard Gonzales, "San Francisco Considers Video Surveillance," NPR, November 4, 2005, sec. National, https://www.npr.org/templates/story/story.php?storyId=4990088.

18 Gonzales, "San Francisco Considers Video Surveillance."

19 Gonzales, "San Francisco Considers Video Surveillance."

20 Ross Mirkarimi, "Providing for public notice of installation of community safety cameras." Board of Supervisors, June 6, 2006.

21 Heather Knight, "50 Cameras Set for Public Housing Sites."

22 Heather Knight, "S.F. Public Housing Cameras No Help in Homicide Arrests." SF Gate, April 14, 2007. https://www.sfgate.

com/news/article/S-F-public-housing-cameras-no-help-in-homicide-2510907.php

23 Dudley, "Lights, Cameras, Inaction: San Francisco's Broken Surveillance State."

24 Dudley, "Lights, Cameras, Inaction: San Francisco's Broken Surveillance State."

25 Dudley, "Lights, Cameras, Inaction: San Francisco's Broken Surveillance State."

26 Dudley, "Lights, Cameras, Inaction: San Francisco's Broken Surveillance State."

27 King, Jennifer, Deirdre K. Mulligan, and Steven P. Raphael. "CITRIS Report: The San Francisco Community Safety Camera Program - An Evaluation of the Effectiveness of San Francisco's Community Safety Cameras." SSRN Scholarly Paper. Rochester, NY, December 17, 2008. https://doi.org/10.2139/ssrn.2183381.

28 Dudley, "Lights, Cameras, Inaction: San Francisco's Broken Surveillance State."

29 Bowles, Nellie. "Why Is a Tech Executive Installing Security Cameras Around San Francisco?" The New York Times, July 10, 2020, sec. Business. https://www.nytimes.com/2020/07/10/business/camera-surveillance-san-francisco.html.

30 Community Benefit Districts (CBDs) emerged in the US in the 1970s in response to white flight and racist policies having left urban centers neglected. It was in 1989 that California first introduced them to the state.

31 Business Improvement Districts (BIDs) are privately directed and funded, and publicly authorized, groups that supplement public services in defined areas.

32 Dave Maass, "The San Francisco District Attorney's 10 Most Surveilled Neighborhoods," Electronic Frontier Foundation (blog), February 6, 2019, https://www.eff.org/deeplinks/2019/02/san-francisco-district-attorneys-10-most-surveilled-places.

33 American Legal Publishing, "CHAPTER 19B: ACQUISITION OF SURVEILLANCE TECHNOLOGY," accessed June 1, 2023, https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-47320.

34 Electronic Frontier Foundation, "Williams v. San Francisco," Electronic Frontier Foundation, October 7, 2020, https://www.eff.org/cases/williams-v-san-francisco.

35 Williams, "2020-10-06 - Hope Williams' Statement," Electronic Frontier Foundation, October 6, 2020, https://www.eff.org/document/2020-10-06-hope-williams-statement.

36 Hardcastle, Jessica Lyons. "San Francisco Cops Can Use Private Cameras for Surveillance." Accessed April 17, 2023. https://www.theregister.com/2022/09/21/san_francisco_private_cameras/.

37 Matthew Guariglia, "SFPD Obtained Live Access to Business Camera Network in Anticipation of Tyre Nichols Protest," Electronic Frontier Foundation, May 23, 2023, https://www.eff.org/deeplinks/2023/05/sfpd-obtained-live-access-business-camera-network-anticipation-tyre-nichols.

38 The City and County of San Francisco, "Surveillance Technology Policy," accessed June 1, 2023, https://sfgov.legistar.com/View.ashx?M=F&ID=11308461&GUID=3413B582-95F4-4B4C-A146-1919CEEAAEB7.

39 SFGov. "Surveillance Technology Inventory." Accessed April 12, 2023. https://sf.gov/resource/surveillance-technology-inventory.

40 Terra Graziani et al., "Property, Personhood, and Police: The Making of Race and Space through Nuisance Law," Antipode 54, no. 2 (2022): 439–61; Erin McElroy and Alex Werth, "Deracinated Dispossessions: On the Foreclosures of 'Gentrification' in Oakland, CA," Antipode 51, no. 3 (2019): 878–98; Ethan Silverstein, "Life, Liberty, and Rental Property: Oakland's Nuisance Eviction Program," Hastings Journal of Crime and Punishment 1, no. 1 (January 1, 2020): 2642–8342.

41 Douglas MacMillan, "Eyes on the Poor: Cameras, Facial Recognition Watch over Public Housing," Washington Post, May 16, 2023, https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/.

42 U.S. Department of Housing and Urban Development, "Capital Fund Emergency/Natural Disaster Funding," HUD.gov / U.S. Department of Housing and Urban Development (HUD), accessed June 1, 2023, https://www.hud.gov/program_offices/public_indian_housing/programs/ph/capfund/emfunding.

43 MacMillan, "Eyes on the Poor."

44 Dave Maass, "San Francisco Police Nailed for Violating Public Records Laws Regarding Face Recognition and Fusion Center Documents," Electronic Frontier Foundation, June 2, 2022, https://www.eff.org/deeplinks/2022/06/san-francisco-police-nailed-violating-public-records-laws-regarding-face.

45 U.S. Department of Housing and Urban Development,

"Emergency Safety and Security Grants Annual Funding Notification and Application Process," April 21, 2023, https://www.hud.gov/sites/dfiles/PIH/documents/2023PIH10.pdf.

46 Dave Paresh. "Focus: U.S. Cities Are Backing off Banning Facial Recognition as Crime Rises." Reuters, May 12, 2022.

47 MacMillan, "Eyes on the Poor."

48 Desjardins, Lisa, and Andrew Corkery, "How Surveillance Cameras Are Being Used to Punish Public Housing Residents." PBS NewsHour, June 4, 2023. https://www.pbs.org/newshour/show/how-surveillance-cameras-are-being-used-to-punish-public-housing-residents.

49 Desjardins and Corkery, "How Surveillance Cameras Are Being Used to Punish Public Housing Residents."

50 Jordan McDonald, "House Reps Ask HUD to End Use of Facial-Recognition Tech in Public Housing." Tech Brew, June 15, 2023. https://www.emergingtechbrew.com/stories/2023/06/15/hud-facial-recognition-tech-public-housing.

51 Maxine Waters and Ayanna Pressley. "Ranking Member Committee on Financial Services." United States House of Representatives Committee on Financial Services, May 25, 2023.

52 Wolford Wayne LLP. "Tenant's Rights Regarding Security Cameras | Wolford Wayne LLP | San Francisco Tenant Lawyer," May 24, 2023. https://wolford-wayne.com/tenants-rights-regarding-security-cameras/.

53 San Francisco Administrative Code. "SEC. 37.10B. TENANT HARASSMENT." Accessed July 5, 2023. https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-16480.

54 Boom: The Sound of Eviction. (US: Whispered Media, 2001)

55 Rebecca Solnit, "Death by Gentrification: The Killing That Shamed San Francisco," The Guardian, March 21, 2016, sec. US news, https://www.theguardian.com/us-news/2016/mar/21/death-by-gentrification-the-killing-that-shamed-san-francisco.

56 Jack Ross, "San Francisco-Based Veritas Investments Accused of Harassing Renters," September 30, 2021, https://capitalandmain.com/san-francisco-based-veritas-investments-accused-of-harassing-renters.

57 Anti-Eviction Mapping Project et al., "Landlord Tech Watch," 2020, https://antievictionmappingproject.github.io/landlordtech/.

58 Alexander Ferrer, "Beyond Wall Street Landlords: How Private Equity in the Rental Market Makes Housing Unaffordable, Unstable, and Unhealthy," Los Angeles: Strategic Action for a Just Economy, (2021): 1-58, https://doi.org/https://www.saje.net/wp-content/uploads/2021/03/Final_A-Just-Recovery-Series_Beyond_Wall_Street.pdf.

59 Desiree Fields. "Automated Landlord: Digital Technologies and Post-Crisis Financial Accumulation." Environment and Planning A: Economy and Space 54, no. 1 (February 1, 2022): 160–81; McElroy, Erin, Wonyoung So, and Nicole Weber. "Keeping an Eye on Landlord Tech." Shelterforce (blog), March 25, 2021. https://shelterforce.org/2021/03/25/keeping-an-eye-on-landlord-tech/.

60 Ferreri, Mara, and Romola Sanyal. "Digital Informalisation: Rental Housing, Platforms, and the Management of Risk." Housing Studies 37, no. 6 (December 5, 2021): 1035–53; Fields, Desiree, and Dallas Rogers. "Towards a Critical Housing Studies Research Agenda on Platform Real Estate." Housing, Theory and Society 38, no. 1 (2019): 72–94; Shaw, Joe. "Platform Real Estate: Theory and Practice of New Urban Real Estate Markets." Urban Geography 41, no. 8 (September 13, 2020): 1037–64.

61 Raymond, Elora, Richard Duckworth, Ben Miller, Michael Lucas, and Shiraj Pokharel. "Corporate Landlords, Institutional Investors, and Displacement: Eviction Rates in Single-Family Rentals." Accessed April 17, 2023. https://www.atlantafed.org/community-development/publications/discussion-papers/2016/04-corporate-landlords-institutional-investors-and-displacement-2016-12-21.

62 Jackson, Bo McMillan, Reggie. "Corporate Landlords Profit from Segregation, at Cost of Black Homeownership and Wealth." Shelterforce, October 19, 2022. https://shelterforce.org/2022/10/19/corporate-landlords-profit-from-segregation-at-cost-of-black-homeownership-and-wealth/.

63 Katz, Lily, and Sheharyar Bokhari. "Investors Bought a Record 18% of Homes That Sold in the Third Quarter." Redfin. Accessed April 17, 2023. https://www.redfin.com/news/investor-home-purchases-q3-2021/.

64 ButterflyMX, "From Amenity to Necessity," Video Intercom System for Apartment Buildings | ButterflyMX (blog), accessed April 25, 2023, https://butterflymx.com/resources/ebooks/from-amenity-to-necessity/.

65 Statista, "Smart Home - United States | Statista Market Forecast." Accessed April 17, 2023. https://www.statista.com/outlook/

dmo/smart-home/united-states.

66 Grand View Research Inc, "Smart Home Market Size Worth $537.01 Billion by 2030: Grand View Research, Inc.," accessed May 30, 2023, https://www.prnewswire.com/news-releases/smart-home-market-size-worth-537-01-billion-by-2030-grand-view-research-inc-301567467.html.

67 Maalsen, Sophia, and Robyn Dowling. 2020. "Covid-19 and the Accelerating Smart Home." Big Data & Society 7 (2): https://doi.org/10.1177/2053951720938073; McElroy, Erin, Meredith Whittaker, and Genevieve Fried. 2020. "COVID-19 Crisis Capitalism Comes to Real Estate." Boston Review, April 30, 2020. https://bostonreview.net/class-inequality-science-nature/erin-mcelroy-meredith-whittaker-genevieve-fried-covid-19-crisis.

68 Harding, Scharon. "Smart Home Tech Is Thriving Right Now." Ars Technica, December 9, 2021. https://arstechnica.com/gadgets/2021/12/smart-home-tech-is-thriving-right-now/.

69 McElroy, Erin. 2020. "Landlord Tech and Racial Technocapitalism in the Times of Covid-19." Foundry. https://uchri.org/foundry/landlord-tech-and-racial-technocapitalism-in-the-times-of-covid-19/.

70 Smart Sentry AI. "Best-in-Class AI for Security Monitoring." https://smartsentry.ai/

71 Benjamin, Ruha. 2019. Race After Technology: Abolitionist Tools for the New Jim Code. John Wiley & Sons; Buolamwini, Joy, and Timnit Gebru. 2018. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." In Conference on Fairness, Accountability and Transparency, 77–91. PMLR; Chun, Wendy Hui Kyong. 2021. Discriminating Data: Correlation, Neighborhoods, and the New Politics of Recognition. Cambridge, MA, USA: MIT Press.

72 Najibi, Alex. "Racial Discrimination in Face Recognition Technology." Science in the News. Harvard University, October 24, 2020. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

73 Eufy. "4G Camera S230." https://us.eufy.com/products/e8150121?ref=navimenu_4_img

74 Eufy. "Video Doorbell 2K Wired." https://us.eufy.com/products/t82001j1?ref=navimenu_3_img

75 The Verge, "Anker's Eufy lied to us about the security of its security cameras", Nov 30, 2022 https://www.theverge.com/2022/11/30/23486753/anker-eufy-security-camera-cloud-private-encryption-authentication-storage

76 Kevin Purdy, "Eufy's "No clouds" cameras upload facial thumbnails to AWS", Nov 30, 2022 https://arstechnica.com/gadgets/2022/11/eufys-no-clouds-cameras-upload-facial-thumbnails-to-aws/

77 AppleInsider, "Anker admits that Eufy cameras were never encrypted", Jan 31, 2023. https://appleinsider.com/articles/23/01/31/anker-admits-that-eufy-cameras-were-never-encrypted

78 The Verge, "SimpliSafe's new camera lets agents talk to intruders inside your home". Feb 2, 2023 https://www.theverge.com/2023/2/2/23581461/simplisafe-live-guard-feature-new-smart-alarm-indoor-security-camera

79 Lorex, "Lorex Fusion 4K 16 Camera", https://www.lorex.com/products/n845-4l-fusion-nvr-system-with-spotlight-indoor-outdoor-wifi-6-cameras?variant=42192692117654

80 Lorex, "Lorex Website and product Privacy policy', https://www.lorex.com/policies/privacy-policy

81 Doorbird, "Gallery", https://www.doorbird.com/en/references

82 Virtual Doorman, "How It Works", https://virtualdoorman.com/how-it-works/

83 Virtual Doorman, "Our Remote Doorman Technology", https://virtualdoorman.com/technology/

84 Q5id, "Know Your Employee (KYE)", https://q5id.com/business/know-your-employee-kye

85 NATIX, "Virtual Doorman", https://www.natix.io/products/virtual-doorman

86 Carson Living (@carson.living) Instagram Profile, accessed May 23, 2021, https://www.instagram.com/carson.living.

87 Based upon a conversation with a Carson representative in 2019.

88 CRETECH, "Carson Raises $3 Million Series Seed Led by BuildingLink," accessed May 23, 2021, https://www.cretech.com/news/carson-raises-3-million-series-seed-led-by-buildinglink.

89 Latch, "Getting Started – Latch," accessed May 23, 2021, https://support.latch.com/hc/en-us/sections/115002780748-Getting-Started.

90 Corina Knoll, "When a Phone App Opens Your Apartment Door, but You Just Want a Key," The New York Times, March 23, 2019, https://www.nytimes.

com/2019/03/23/nyregion/keyless-apartment-entry-nyc.html.

91 Latch, "Latch and UPS Are Opening More Doors Nationwide," January 22, 2019, https://www.latch.com/press/latch-and-ups-are-opening-more-doors-nationwide.

92 Latch, "Making Buildings Better Places to Live, Work, and Visit," accessed May 23, 2021, https://www.latch.com.

93 IT Risk Managers. "ButterflyMX Intercom Systems are Taking Chicago by Storm," IT Risk Managers, September 16, 2018, https://www.itriskmgrs.com/blog/butterflymx-intercom-system.

94 A. J. Sidransky, "Virtual Doormen: Deliveries in the Age of Virtual Staff," Cooperator News NYC, September 13, 2018, https://cooperatornews.com/article/virtual-doormen.

95 ButterflyMX, "From Amenity to Necessity: How 2020 Has Changed Multi-Family Housing," Report, 2020, https://butterflymx.com/resources/ebooks/from-amenity-to-necessity.

96 ButterflyMX (@_ ButterflyMX), "'Once COVID started and we couldn't get people in the buildings, self-guided tours and virtual tours became the go-to for COVID-era leasing agents everywhere.' Read more from @NAAhq on connectivity challenges in #multifamily buildings. https://hubs.li/H0JBm8X0 #RealEstate," Twitter, March 22, 2021, https://twitter.com/_ButterflyMX/status/1374014486974234629.

97 ButterflyMX, "Video Intercom System for Apartment Buildings | ButterflyMX," accessed May 23, 2021, https://butterflymx.com.

98 San Francisco District Attorney. "Register Your Camera." Accessed February 20, 2023. https://www.sfdistrictattorney.org/resources/register-your-camera/.

99 Lancaster, Joe. "San Francisco Police Can Now Have Live Access to Nearly Any Camera in the City." Reason, September 26, 2022. https://reason.com/2022/09/26/san-francisco-police-can-now-have-live-access-to-nearly-any-camera-in-the-city/.

100 Ring, "Ring Video Doorbells | Smart Doorbell Cameras, Wireless and Wired," Ring, accessed May 13, 2023, https://ring.com/doorbell-cameras.

101 Investigate: A Project of The American Friends Service Committee, "Amazon.Com Inc | AFSC Investigate," Amazon.com, accessed February 20, 2023, https://investigate.afsc.org/company/amazon.

102 Ring, "Advanced Motion Detection in Ring Devices – Ring Help," accessed May 13, 2023, https://support.ring.com/hc/en-us/articles/360042728431-Advanced-Motion-Detection-in-Ring-Devices.

103 American Legal Publishing, "SEC. 3706. PROHIBITION AGAINST ALARM SYSTEMS WHICH EMIT FALSE ALARMS.," American Legal Publishing, accessed May 13, 2023, https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_police/0-0-0-7670.

104 Investigate: A Project of The American Friends Service Committee, "Amazon.Com Inc.," accessed February 20, 2023, https://investigate.afsc.org/company/amazon.

105 Kim Lyons, "Amazon's Ring Now Reportedly Partners with More than 2,000 US Police and Fire Departments," The Verge, January 31, 2021, https://www.theverge.com/2021/1/31/22258856/amazon-ring-partners-police-fire-security-privacy-cameras.

106 Investigate: A Project of The American Friends Service Committee, "Amazon.Com Inc."

107 "Administrative Code - Surveillance Technology Policy for Police Department Use of Non-City Entity Surveillance Cameras," September 12, 2022. https://sfgov.legistar.com/View.ashx?M=F&ID=11240602&GUID=8E192C3D-24AF-4851-A25A-DC5DA85E7E77.

108 Electronic Frontier Foundation. "Williams v. San Francisco." Electronic Frontier Foundation, October 7, 2020. https://www.eff.org/cases/williams-v-san-francisco.

109 Ion. "Amazon's Ring Doorbell Could Use Biometrics to Surveil Neighborhoods." Gizmodo, December 17, 2021. https://gizmodo.com/in-the-future-amazons-ring-doorbell-might-use-biometri-1848230784.

110 Investigate: A Project of The American Friends Service Committee. "Amazon.Com Inc | AFSC Investigate." Amazon.com. Accessed February 20, 2023. https://investigate.afsc.org/company/amazon.

111 Haskins, Caroline. "Everything You Need to Know About Ring, Amazon's Surveillance Camera Company." Vice, August 8, 2019. https://www.vice.com/en/article/qvg48d/everything-you-need-to-know-about-ring-amazons-surveillance-camera-company.

112 Haskins, Caroline. "US Cities Are Helping People Buy Amazon Surveillance Cameras Using Taxpayer Money." Vice (blog), August 2, 2019. https://www.vice.com/en/article/d3ag37/us-cities-are-helping-people-buy-amazon-surveillance-cameras-using-taxpayer-money.

113 Haskins, Caroline. "Everything You Need to Know About Ring, Amazon's Surveillance Camera Company."

114 Harris, Mark. "Video Doorbell Firm Ring Says Its Devices Slash Crime—but the Evidence Looks Flimsy." MIT Technology Review. Accessed February 20, 2023. https://www.technologyreview.com/2018/10/19/103922/video-doorbell-firm-ring-says-its-devices-slash-crimebut-the-evidence-looks-flimsy/.

115 Herring, Chris. "Complaint-Oriented Policing: Regulating Homelessness in Public Space." American Sociological Review 84, no. 5 (October 1, 2019): 769–800.

116 Smiley, Lauren. "The Porch Pirate of Potrero Hill Can't Believe It Came to This." The Atlantic, November 1, 2019. https://www.theatlantic.com/technology/archive/2019/11/stealing-amazon-packages-age-nextdoor/598156/.

117 Lancaster, "San Francisco Police Can Now Have Live Access to Nearly Any Camera in the City."

118 Erin McElroy, "Landlord Tech and Racial Technocapitalism in the Times of Covid-19," Foundry, November 2020, https://uchri.org/foundry/landlord-tech-and-racial-technocapitalism-in-the-times-of-covid-19/.

119 Erin McElroy, Meredith Whittaker, and Genevieve Fried, "COVID-19 Crisis Capitalism Comes to Real Estate," Boston Review, April 30, 2020, https://bostonreview.net/class-inequality-science-nature/erin-mcelroy-meredith-whittaker-genevieve-fried-covid-19-crisis.

120 Desiree Fields, "Automated Landlord: Digital Technologies and Post-Crisis Financial Accumulation," Environment and Planning A: Economy and Space 54, no. 1 (February 1, 2022): 160–81.

121 https://www.cnet.com/home/smart-home/vivint-and-airbnb-join-forces-to-protect-your-rental-ces-2017/

122 Purenne, Anaik, and Gregoire Palierse. Towards Cities of Informers? Community-Based Surveillance in France and Canada. Surveillance & Society 15, no. 1 (2016): 79-93.

123 Rahim Kurwa, "Building the Digitally Gated Community: The Case of Nextdoor," Surveillance & Society 17, no. 1/2 (March 31, 2019): 111–17.

124 Nellie Bowles, "How San Francisco Became a Failed City," The Atlantic, June 8, 2022, https://www.theatlantic.com/ideas/archive/2022/06/how-san-francisco-became-failed-city/661199/.

125 Makena Kelly "Inside Nextdoor's 'Karen Problem.'" The Verge, June 8, 2020, https://www.theverge.com/21283993/nextdoor-app-racism-community-moderation-guidance-protests.

126 Sarah Emerson, "The Police Are Watching on Nextdoor." OneZero, June 3, 2020. https://onezero.medium.com/the-police-are-watching-on-nextdoor-718996fcbd6a.

127 Lauren Smiley, "The Porch Pirate of Potrero Hill Can't Believe It Came to This." The Atlantic, November 1, 2019. https://www.theatlantic.com/technology/archive/2019/11/stealing-amazon-packages-age-nextdoor/598156

128 Anti-Eviction Mapping Project, "Killings by Police, San Francisco, 1985-2020," Anti-Eviction Mapping Project, June 8, 2020, https://antievictionmap.com/blog/2020/6/8/killings-by-police-san-francisco-1985-2020.

129 Granate Kim, "False Arrest, Racial Profiling: Why the Citizen App Is a Threat to Vulnerable Communities," Fast Company, July 22, 2021, https://medium.com/fast-company/false-arrest-racial-profiling-why-the-citizen-app-is-a-threat-to-vulnerable-communities-c85d0ad8d3c5.

130 Joseph Cox and Jason Koebler, "'Find this Fuck:' Inside Citizen's Dangerous Effort to Cash In On Vigilantism," Vice, accessed February 7, 2023, https://www.vice.com/en/article/y3dpyw/inside-crime-app-citizen-vigilante.

131 Smiley, "The Porch Pirate of Potrero Hill Can't Believe It Came to This."

132 Joseph Smooke and Dyan Ruiz, "Exclusive Exposé: The Wild West of Landlord Technology," People Power Media, September 29, 2020, https://www.peoplepowermedia.org/solutions/exclusive-expose-wild-west-landlord-technology.

133 Andrew Baum, Andrew Saull, and Fabian Braesemann, "PropTech 2020: the Future of Real Estate" (University of Oxford Saïd Business School, February 2020), https://www.sbs.ox.ac.uk/sites/default/files/2020-02/proptech2020.pdf.

134 Anne-Cécile Mermet, "Who Is Benefiting from Airbnb? Assessing the Redistributive Power of Peer-to-Peer Short-Term Rentals," The Professional Geographer 73, no. 3 (May 4, 2021): pp. 553-566, https://doi.org/10.1080/00330124.2021.1906921.

135 Baum et al, "PropTech 2020: the Future of Real Estate."

136 Budget and Legislative Analyst's Office, "Policy Analysis Report: Short-Term Rentals 2016

Update" (San Francisco, CA: City and County of San Francisco Board of Supervisors, 2016), pp. 1-31.

137 Stephanie Rosenbloom, "Navigating the New Airbnb," The New York Times (The New York Times, November 28, 2016), https://www.nytimes.com/2016/11/28/travel/airbnb-expansion.html.

138 Statista Research Department, "Company Value of Airbnb Worldwide 2016-2021," Statista (Statista Research Department, July 27, 2022), https://www.statista.com/statistics/339845/company-value-and-equity-funding-of-airbnb/.

139 Is the Sharing Economy a SHAM?, YouTube (PBS: Two Cents, 2021), https://www.youtube.com/watch?v=6RfDvO5gaXk&t=316s.

140 Jessica Edgson, "28 Intriguing Airbnb Statistics and Facts for 2022," ComfyLiving (CafeMedia, January 21, 2022), https://comfyliving.net/airbnb-statistics/.; Marija Kovachevska, "28 Amazing Airbnb Statistics You Should Know before Booking," CapitalCounselor (CafeMedia, March 18, 2022), https://capitalcounselor.com/airbnb-statistics/.

141 Airbnb, "The Airbnb Story Timeline," Airbnb, April 8, 2018, https://press.airbnb.com/wp-content/uploads/sites/4/2018/08/The-Airbnb-Story-Timeline-EN-GLOBAL.pdf.; Airbnb, "Live There: Introducing Our New Airbnb Experience," Airbnb.Design, October 13, 2022, https://airbnb.design/live-there/.

142 Comfy Living, "28 Intriguing Airbnb Statistics." https://comfyliving.net/airbnb-statistics/

143 San Francisco Tenants Union, "Airbnb & Short-Term Rentals," San Francisco Tenants Union, December 2021, https://sftu.org/short-term-rentals/.

144 Anne-Cécile Mermet, "Who Is Benefiting from Airbnb? Assessing the Redistributive Power of Peer-to-Peer Short-Term Rentals," The Professional Geographer 73, no. 3 (May 4, 2021): pp. 553-566, https://doi.org/10.1080/00330124.2021.1906921.

145 McElroy, Erin, and Tim Redmond. 2015. "Up against a Serial Evictor." 48 Hills. July 1, 2015. https://48hills.org/2015/06/up-against-a-serial-evictor/.

146 "Danny Haber and Alon Gutman." n.d. Anti-Eviction Mapping Project. Accessed February 8, 2023. https://antievictionmap.com/danny-haber-and-alon-gutman.

147 Tadayon, Ali. 2019. "Oakland Landlord to Pay SRO Tenants $575,000 in Wrongful Eviction Case." East Bay Times, May 16, 2019. https://www.eastbaytimes.com/2019/05/16/sro-tenants-settle-wrongful-eviction-lawsuit-for-575k/.

148 Together, Sens. Cory Booker and Elizabeth Warren also petitioned the Consumer Financial Protection Bureau in March of 2021 for information regarding the use of tenant screening technology by landlords. In their seven-page letter, the senators emphasized the erroneous data often provided by tenant screening companies and their disproportionate impact upon people of color. See https://www.warren.senate.gov/imo/media/doc/2021.03.01%20Letter%20to%20CFPB%20on%20Oversight%20of%20Tenant%20Screening%20Technology%20Companies.pdf.

149 Edelman et al. and Kakar et al. studied racial discrimination on Airbnb and similar sharing platforms. In both studies, they found that Black and Asian hHosts whose names and profile photos offer apparent racial signifiers experience discrimination in the form of fewer listing rentals when compared to similar listings from hosts with apparently white profile names and photos. Further, of those listings by Black and Asian hosts, properties with comparable offerings in similar locations rented for less per night indicating less income for hosts of color. Likewise, Guests with Black and Asian profile names and photos that were indicative of their race also experienced discrimination by being disproportionately denied stays when compared to white guests with similar profiles. Such findings show that the peer-to-peer model of sharing platforms allows for less anonymity and may exacerbate racial bias. In contrast, traditional lodging models (i.e. hotels) are unable to determine a guest's race during the booking process and thus, have limited opportunity to discriminate without direct auditory and/or visual interaction with a guest (i.e. phone call, reception desk check-in).

150 https://www.schatz.senate.gov/imo/media/doc/Letter%20to%20FTC%20re%20short%20term%20rental%20platforms%207-13-16.pdf

151 https://abc7ny.com/jersey-city-new-airbnb-short-term-lease/5643857/ & https://news.airbnb.com/what-makes-airbnb-airbnb/

152 Kwan Booth, "Protesters Occupy Airbnb HQ Ahead of Housing Affordability Vote," The Guardian (Guardian News and Media, November 2, 2015), https://www.theguardian.com/us-news/2015/nov/02/airbnb-san-francisco-headquarters-occupied-housing-protesters.

153 Heather Somerville and Dan Levine, "Airbnb, San Francisco Settle Lawsuit over Short-Term

Rental Law," Reuters (Thomson Reuters, May 1, 2017), https://www.reuters.com/article/us-airbnb-sanfrancisco-settlement-idUSKBN17X254.

154 Otis R. Taylor, "Meet the Man behind Proposition F," Medium (Ripple News, November 2, 2015), https://medium.com/on-ripple/meet-the-man-behind-proposition-f-a56eef8e4334.; Carolyn Said, "Prop. F: S.F. Voters Reject Measure to Restrict Airbnb Rentals," SFGATE (San Francisco Chronicle, November 3, 2015), https://www.sfgate.com/bayarea/article/Prop-F-Measure-to-restrict-Airbnb-rentals-6609176.php#photo-8901293.; Ballotpedia, "City of San Francisco Initiative to Restrict Short-Term Rentals, Proposition F (November 2015)," Ballotpedia, accessed November 10, 2022, https://ballotpedia.org/City_of_San_Francisco_Initiative_to_Restrict_Short-Term_Rentals,_Proposition_F_(November_2015).

155 Ballotpedia, "City of San Francisco Initiative to Restrict Short-Term Rentals, Proposition F (November 2015)," Ballotpedia, accessed November 10, 2022, https://ballotpedia.org/City_of_San_Francisco_Initiative_to_Restrict_Short-Term_Rentals,_Proposition_F_(November_2015).

156 Carolyn Said, "Prop. F: S.F. Voters Reject Measure to Restrict Airbnb Rentals," SFGATE (San Francisco Chronicle, November 3, 2015), https://www.sfgate.com/bayarea/article/Prop-F-Measure-to-restrict-Airbnb-rentals-6609176.php#photo-8901293.

157 Ballotpedia, "City of San Francisco Initiative to Restrict Short-Term Rentals, Proposition F (November 2015)," Ballotpedia, accessed November 10, 2022, https://ballotpedia.org/City_of_San_Francisco_Initiative_to_Restrict_Short-Term_Rentals,_Proposition_F_(November_2015).

158 Amanda Zoch, "Initiative and Referendum States," National Conference of State Legislatures, accessed November 10, 2022, https://www.ncsl.org/research/elections-and-campaigns/chart-of-the-initiative-states.aspx.

159 Ballotpedia, "City of San Francisco Initiative to Restrict Short-Term Rentals, Proposition F (November 2015)," Ballotpedia, accessed November 10, 2022, https://ballotpedia.org/City_of_San_Francisco_Initiative_to_Restrict_Short-Term_Rentals,_Proposition_F_(November_2015).

160 Ballotpedia, "City of San Francisco Initiative to Restrict Short-Term Rentals, Proposition F."

161 Ballotpedia, "City of San Francisco Initiative to Restrict Short-Term Rentals, Proposition F."

162 Stephen Fishman, "Overview of Airbnb Law in San Francisco," NOLO (MH Sub I, LLC, August 27, 2019), https://www.nolo.com/legal-encyclopedia/overview-airbnb-law-san-francisco.html.

163 Adam Brinklow, "City Says 76 Percent of Airbnb Listings Are Illegal," Curbed San Francisco (Vox Media, April 8, 2016), https://sf.curbed.com/2016/4/8/11394592/airbnb-study-illegal-san-francisco.

164 Statista Research Department, "Company Value of Airbnb Worldwide 2016-2021," Statista (Statista Research Department, July 27, 2022), https://www.statista.com/statistics/339845/company-value-and-equity-funding-of-airbnb/.

165 dam Brinklow, "City Says 76 Percent of Airbnb Listings Are Illegal," Curbed San Francisco (Vox Media, April 8, 2016), https://sf.curbed.com/2016/4/8/11394592/airbnb-study-illegal-san-francisco.; Colin Dwyer, "Airbnb Settles Suit With San Francisco, Aims To Smooth Host Registration," NPR (NPR: The Two-Way, May 1, 2017), https://www.npr.org/sections/thetwo-way/2017/05/01/526421009/airbnb-settles-suit-with-san-francisco-aims-to-smooth-host-registration.

166

167 Colin Dwyer, "Airbnb Settles Suit With San Francisco, Aims To Smooth Host Registration," NPR (NPR: The Two-Way, May 1, 2017), https://www.npr.org/sections/thetwo-way/2017/05/01/526421009/airbnb-settles-suit-with-san-francisco-aims-to-smooth-host-registration.

Steve Dent, "Airbnb Cuts Half of San Francisco Listings as New Laws Kick In," Engadget (Yahoo, January 19, 2018), https://www.engadget.com/2018-01-19-airbnb-san-francisco-listings-cut-in-half.html.

San Francisco Planning, "Intermediate Length Occupancy (ILO) Dwelling Units," San Francisco Planning, 2022, https://sfplanning.org/project/intermediate-length-occupancy-ilo-dwelling-units#about.

168 Joseph Smooke, Dyan Ruiz, and Frederick Noland, "Post-Coronavirus We Need a New Way to Plan Cities," People Power Media, June 6, 2020, https://www.peoplepowermedia.org/housing/post-coronavirus-we-need-new-way-plan-cities.

169 Joseph Smooke, Dyan Ruiz, and Frederick Noland, "Post-Coronavirus We Need a New Way to Plan Cities," People Power Media, June 6, 2020, https://www.peoplepowermedia.org/housing/post-coronavirus-we-need-new-way-plan-cities.; Jackson Fuller Real Estate, "Intermediate Length Occupancy Rental Law in San Francisco," YouTube (YouTube, January 22, 2021), https://www.youtube.com/watch?v=FB0nkQ-ymdY.

170 Joseph Smooke, Dyan Ruiz, and Frederick Noland, "Post-Coronavirus We Need a New Way to Plan Cities," People Power Media, June 6, 2020, https://www.peoplepowermedia.org/housing/post-coronavirus-we-need-new-way-plan-cities.

171 Tiffany Cassidy, "Eight Ways Travelers Can Fight 'the Airbnb Effect' on Local Housing Costs," The Washington Post (WP Company, January 23, 2020), https://www.washingtonpost.com/lifestyle/travel/eight-ways-travelers-can-fight-the-airbnb-effect-on-local-housing-costs/2020/01/22/68145b50-3714-11ea-bf30-ad313e4ec754_story.html.

172 Tiffany Cassidy, "Eight Ways Travelers Can Fight 'the Airbnb Effect' on Local Housing Costs," The Washington Post (WP Company, January 23, 2020), https://www.washingtonpost.com/lifestyle/travel/eight-ways-travelers-can-fight-the-airbnb-effect-on-local-housing-costs/2020/01/22/68145b50-3714-11ea-bf30-ad313e4ec754_story.html.

173 Suna Erdem, "The Cities Hitting Back at Airbnb," The New European (The New European, November 4, 2021), https://www.theneweuropean.co.uk/fight-against-airbnb-cities/.

174 Reuters Staff, "Amsterdam to Allow Airbnb Rentals in City Centre after Court Order," Reuters (Thomson Reuters Corporation, March 16, 2021), https://www.reuters.com/article/us-netherlands-airbnb-amsterdam/amsterdam-to-allow-airbnb-rentals-in-city-centre-after-court-order-idUSKBN2B81NS.

175 Paige McClanahan, "Barcelona Takes on Airbnb," The New York Times (The New York Times, September 22, 2021), https://www.nytimes.com/2021/09/22/travel/barcelona-airbnb.html.

McClanahan, "Barcelona Takes on Airbnb."

176 While this report uses the acronym "STR" to refer to short-term rental, the European Union uses the acronym "STHR" to denote short-term holiday rental. STRs and STHRs both refer to units rented for less than 30 days. Additionally, this report refers to the "sharing economy" which is similar to the "collaborative economy" referenced in the Digital Services Act.

177 European Commission, "The Digital Services Act Package," Shaping Europe's digital future (European Commission, November 24, 2022), https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

178 European Commission, "The Digital Services Act Package."

179 European Commission, "The Digital Services Act Package."

180 Wilma Dragonetti, "Digital Services Act, Why Should You Care?," Eurocities (Eurocities, May 4, 2021), https://eurocities.eu/latest/digital-service-act-why-should-you-care/.

181 Dragonetti, "Digital Services Act, Why Should You Care?"

182 Patrick Sisson, "Airbnb's Data 'Portal' Promises a Better Relationship With Cities," Bloomberg (Bloomberg, September 23, 2020), https://www.bloomberg.com/news/articles/2020-09-23/why-airbnb-launched-a-data-sharing-tool-for-cities.

183 Airbnb Airbnb, "One Year Later: Airbnb's City Portal," Airbnb Newsroom, September 30, 2021, https://news.airbnb.com/one-year-later-airbnbs-city-portal/.

184 Sisson, "Airbnb's Data 'Portal' Promises a Better Relationship With Cities."

185 Inside Airbnb. n.d. "About." Accessed February 8, 2023. http://insideairbnb.com/about/.

186 Katz, Miranda. 2017. "A Lone Data Whiz Is Fighting Airbnb — and Winning." Wired, February 10, 2017. https://www.wired.com/2017/02/a-lone-data-whiz-is-fighting-airbnb-and-winning/.

187 Paula Garcia-Salazar, Erin McElroy, and Manon Vergerio, "Landlord Technologies of Gentrification: Facial Recognition and Building Access Technologies in New York City Homes" (Anti-Eviction Mapping Project, 2022), pp. 13-25.

188 Alex Hern, "Airbnb to Use 'Anti-Party Technology' to Crack down on Rowdy Guests," The Guardian (Guardian News and Media, August 17, 2022), https://www.theguardian.com/technology/2022/aug/17/airbnb-to-use-anti-party-technology-to-crack-down-on-rowdy-guests.; Airbnb, "New Anti-Party Technology Successfully Cracks down on Unauthorised Parties," Airbnb Newsroom, August 18, 2022, https://news.airbnb.com/en-au/new-anti-party-technology-successfully-cracks-down-on-unauthorised-parties/.

189 Hern, "Airbnb to Use 'Anti-Party Technology'."

190 Erin McElroy, "Dis/Possessory Data Politics: From Tenant Screening to Anti-Eviction Organizing," International Journal of Urban and Regional Research, Vol.47 (21 December 2022), 60.

191 Stauffer, Robert R. "Tenant Blacklisting: Tenant Screening Services and the Right to Privacy," Harvard Journal on Legislation, Vol.24, no.239 (Winter 1987), 239.

192 McElroy, "Dis/Posessory Data Politics," 60.

193 Rosen, Eva, Philip M.E. Garboden, and Jennifer E. Cossyleon. "Racial Discrimination in Housing: How Landlords Use Algorithms and Home Visits to Screen Tenants," American Sociological Review, Vol. 86, no. 5 (October 2021), pp.787-822.

194 McElroy, "Dis/Posessory Data Politics," 60.

195 McElroy, "Dis/Posessory Data Politics," 60.

196 Didi Rankovic, "Naborly Asks Landlords To Report If Tenants Are "Delinquent" On April Rent," April 4, 2020.

197 Rankovic, "Naborly Asks Landlords To Report If Tenants Are "Delinquent" On April Rent."

198 Joseph Lynak and Nicholas A.J. Vlietstra, "The U.S. Supreme Court's Decision in Texas Department of Housing & Community Affairs v. Inclusive Communities Project, Inc," Dorsey & Whitney LLP, June 30, 2015.

199 Wonyoung So, "Which Information Matters? Measuring Landlord Assessment of Tenant Screening Reports." Housing Policy Debate, 30 August 2022.

200 So, "Which Information Matters?"

201 So, "Which Information Matters?"

202 "Blocklisting" is used in place of the customary term "blacklisting" to more descriptively represent the exclusionary character of TSB databases.

203 Tech Equity Collaborative, "Tech, Bias, and Housing Initiative: Tenant Screening."

204 McElroy, "Dis/Posessory Data Politics," 64.

205 Philip Garboden and Eva Rosen, "Serial Filing: How Landlords Use The Threat of Eviction."

206 McElroy, "Dis/Posessory Data Politics," 64.

207 Cyrus Farivar, "Tenant Screening Software Faces National Reckoning," NBC, March 14, 2021.

208 National Housing Law Project, "Arroyo v. CoreLogic," July 31, 2018.

209 Communications with attorneys from the Connecticut Fair Housing Center.

210 Communications with attorneys from the Connecticut Fair Housing Center.

211 Communications with attorneys from the Connecticut Fair Housing Center.

212 Communications with attorneys from the Connecticut Fair Housing Center.

213 Communications with attorneys from the Connecticut Fair Housing Center.

214 Communications with attorneys from the Connecticut Fair Housing Center.

215 National Housing Law Project, "Arroyo v. CoreLogic," July 31, 2018.

216 National Housing Law Project, "Arroyo v. CoreLogic," July 31, 2018.

217 Dean Dabney et al., "Who Actually Steals? A Study of Covertly Studied Shoplifters," Justice Quarterly 21(4):693-728, December 2004.

218 FBI UCR, "Crime in the United States: Table 43: Arrests, By Race And Ethnicity, 2019," 2019.

219 Farivar, "Tenant Screening Software Faces National Reckoning."

220 San Francisco Planning Department, "San Francisco Housing Needs and Trends Report: Final Report – July 2018, July 2018, 51.

221 San Francisco Planning Department, "San Francisco Housing Needs and Trends Report", 60.

222 So, "Which Information Matters?"

223 McElroy, "Dis/Posessory Data Politics," 63-64.

224 McElroy, "Dis/Posessory Data Politics," 64.

225 McElroy, "Dis/Posessory Data Politics," 63.

226 McElroy, "Dis/Posessory Data Politics," 63.

227 McElroy, "Dis/Posessory Data Politics," 65.

228 Shwanika Narayan, "This Bay Area County Could Be The Country's First To Prohibit Criminal Background Checks On Tenants," The SF Chronicle, December 20, 2022.

229 California Legislature, "Bill Text – SB-460 Hiring Of Real Property: Criminal History." California Legislative Information. February 13, 2023.

230 Collins, Jeff, "Governor Newsom Signs Reusable Tenant Screening Bill," Silicon Valley.com, September 15, 2022.

231 Collins, "Governor Newsom Signs Reusable Tenant Screening

Bill."

232 Robert D. Bickel, Susan Brinkely, and Wendy White, "Seeing Past Privacy: Will the Development and Application of CCTV and Other Video Security Technology Compromise an Essential Constitutional Right in a Democracy, or Will the Courts Strike a Proper Balance?" Stetson Law Review, (2003): 33, 299.

233 Josh Barbanel, "Outside Public Housing, Cameras Abound," The Wall Street Journal, June 5, 2014, https://www.wsj.com/articles/police-identify-suspect-in-prince-joshua-avittos-fatal-stabbing-in-brooklyn-by-matching-dna-on-the-knife-1401906762.

234 Eric L. Piza, "The Crime Prevention Effect of CCTV in Public Places: A Propensity Score Analysis," John Jay College of Criminal Justice Publications & Research (2018).

235 Maass, "The San Francisco District Attorney's 10 Most Surveilled Neighborhoods."

236 Burgos v. Aqueduct Realty Corp., 92 N.Y.2d 544 (N.Y. 1998)

237 People v. Funches, 89 N.Y.2d 1005 (N.Y 1997)

238 TRD Staff, "Landlords Get High-Tech in Housing Court," The Real Deal, January 12, 2017, https://therealdeal.com/2017/01/12/landlords-get-high-tech-in-housing-court.

239 UpCounsel, "Video Surveillance Laws by State: Everything You Need to Know," accessed June 4, 2021, https://www.upcounsel.com/video-surveillance-laws-by-state.

240 Grant Clauser, "Security Cameras, Ethics, and the Law," The New York Times, September 23, 2016, https://www.nytimes.com/wirecutter/blog/security-cameras-ethics-and-the-law.

241 Cacye C. Hughes, "A House but Not a Home: How Surveillance in Subsidized Housing Exacerbates Poverty and Reinforces Marginalization," Social Forces 100, no. 1 (2021): 293–315.

242 Tyler Sonnemaker, "Property Tech Companies are Helping Landlords Spy on Residents, Collect Their Data, and Even Evict Them. Critics are Calling it an Invasion of Privacy that Could Reinforce Inequality," Business Insider, September 3, 2020, https://www.businessinsider.com/map-landlords-spying-on-residents-with-surveillance-technology-2020-9.

243 U.S. Congress, House, No Biometric Barriers to Housing Act of 2019, HR 4008, 116th Congress, https://www.congress.gov/bill/116th-congress/house-bill/4008?r=9&s=1.

244 Congresswoman Yvette D. Clarke, "Reps. Clarke, Pressley & Tlaib Announce Bill to Ban Public Housing Usage of Facial Recognition & Biometric Identification Technology," accessed May 24, 2021.

245 Congress.gov. "H.R.3907 - 117th Congress (2021-2022): Facial Recognition and Biometric Technology Moratorium Act of 2021." June 15, 2021. https://www.congress.gov/bill/117th-congress/house-bill/3907.

246 Senator Jeff Merkley, "Merkeley, Colleagues Introduce Legislation to Ban Government Use of Facial Recognition and Other Biometric Technology," accessed June 26, 2020, https://www.merkley.senate.gov/news/press-releases/merkley-colleagues-introduce-legislation-to-ban-government-use-of-facial-recognition-and-other-biometric-technology-2020.

247 H.R 6580 - Algorithmic Accountability Act of 2022, https://www.congress.gov/bill/117th-congress/house-bill/6580/text?r=1&s=1

248 H.R.2644 - Reasonable Policies on Automated License Plate Readers Act, https://www.congress.gov/bill/113th-congress/house-bill/2644.

249 Stanford University Human-Centered Artificial Intelligence, "Summary of AI Provisions from the National Defense Authorization Act 2021," accessed May 1, 2021, https://hai.stanford.edu/policy/policy-resources/summary-ai-provisions-national-defense-authorization-act-2021.

250 Samp, Tony, Steven R. Phillips, and Daniel Tobey. "US Congress Tries to Decode Algorithms." DLA Piper, January 27, 2022. https://www.dlapiper.com/en/insights/publications/ai-outlook/2022/us-congress-tries-to-decode-algorithms.

251 Congress.gov. "H.R.6302 - 112th Congress (2011-2012): Reasonable Policies on Automated License Plate Readers Act." September 7, 2012. https://www.congress.gov/bill/112th-congress/house-bill/6302.

252 Congress.gov. "Text - S.4400 - 116th Congress (2019-2020): National Biometric Information Privacy Act of 2020." August 3, 2020. https://www.congress.gov/bill/116th-congress/senate-bill/4400/text.

253 Congress.gov. "H.R.1816 - 117th Congress (2021-2022): Information Transparency & Personal Data Control Act." March 12, 2021. https://www.congress.gov/bill/117th-congress/house-bill/1816.

254 Congress.gov. "S.1667 -

117th Congress (2021-2022): Social Media Privacy Protection and Consumer Rights Act of 2021." May 18, 2021. https://www.congress.gov/bill/117th-congress/senate-bill/1667.

255 Congress.gov. "H.R.3451 - 117th Congress (2021-2022): Social Media DATA Act." May 31, 2021. https://www.congress.gov/bill/117th-congress/house-bill/3451.

256 Congress.gov. "Text - H.R.3611 - 117th Congress (2021-2022): Algorithmic Justice and Online Platform Transparency Act." May 31, 2021. https://www.congress.gov/bill/117th-congress/house-bill/3611/text.

257 Congress.gov. "Text - S.2024 - 117th Congress (2021-2022): Filter Bubble Transparency Act." June 10, 2021. https://www.congress.gov/bill/117th-congress/senate-bill/2024/text.

258 Congress.gov. "H.R.5596 - 117th Congress (2021-2022): Justice Against Malicious Algorithms Act of 2021." October 18, 2021. https://www.congress.gov/bill/117th-congress/house-bill/5596.

259 Congress.gov. "Text - H.R.6580 - 117th Congress (2021-2022): Algorithmic Accountability Act of 2022." February 4, 2022. https://www.congress.gov/bill/117th-congress/house-bill/6580/text.

260 Farivar, "Tenant Screening Software Faces National Reckoning."

261 Farivar, "Tenant Screening Software Faces National Reckoning."

262 Federal Trade Commission, "Texas Company Will Pay $3 million to Settle FTC Charges that it Failed to Meet Accuracy Requirements for its Tenant Screening Reports," Release, October 16, 2018, https://www.ftc.gov/news-events/press-releases/2018/10/texas-company-will-pay-3-million-settle-ftc-charges-it-failed.

263 CFPB takes action to stop false identification by background screeners. Consumer Financial Protection Bureau. (2021, November 4).

264 NIST evaluates face recognition software's accuracy for flight boarding. (2021, July 13). NIST. Retrieved April 15, 2022, from https://www.nist.gov/news-events/news/2021/07/nist-evaluates-face-recognition-softwares-accuracy-flight-boarding

265 JD Supra Data Security Law Blog, "Virginia Joins California with Passage of New State Data Privacy Law," accessed May 26, 2021, https://www.jdsupra.com/legalnews/virginia-joins-california-with-passage-3929540.

266 Natalie Prescott, "The Anatomy of Biometric Laws: What U. S. Companies Need to Know in 2020," The National Law Review, January 15, 2020, https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020.

267 New York State, "Governor Cuomo Signs Legislation Cracking Down on Unauthorized Private Property Surveillance," accessed June 14, 2021, https://www.governor.ny.gov/news/governor-cuomo-signs-legislation-cracking-down-unauthorized-private-property-surveillance.

268 Electronic Privacy Information Center, "EPIC—State Facial Recognition Policy," accessed May 26, 2021, https://epic.org/state-policy/facialrecognition.

269 Ban Facial Recognition, "Ban Facial Recognition Map," accessed May 26, 2021, https://www.banfacialrecognition.com/map.

270 Labor and Employment - Use of Facial Recognition Services - Prohibition, House Bill 1202, Chapter 446, 2020, https://mgaleg.maryland.gov/2020RS/Chapters_noln/CH_446_hb1202t.pdf

271 Bill Text—AB-2819 Unlawful Detainer Proceedings, accessed May 26, 2021, https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160AB2819.

272 RCW 59.18.367: Unlawful Detainer Action—Limited Dissemination Authorized, accessed May 26, 2021, https://app.leg.wa.gov/RCW/default.aspx?cite=59.18.367.

273 Bloomberg Law, "CCPA vs CPRA: What's the Difference?," Bloomberg Law (Bloomberg Industry Group, Inc., October 22, 2022), https://pro.bloomberglaw.com/brief/the-far-reaching-implications-of-the-california-consumer-privacy-act-ccpa/.

274 Bloomberg Law, "CCPA vs CPRA: What's the Difference?"

275 John Myers, "Column: How Your Data Are Shared and Sold Could Be California's Marquee Ballot Battle in 2018," Los Angeles Times (Los Angeles Times, November 26, 2017), https://www.latimes.com/politics/la-pol-ca-road-map-privacy-consumers-ballot-measure-20171126-story.html.

276 How the California Consumer Privacy Act (CCPA) Will Affect You and Your Business | TECH(Talk), YouTube (TECH(talk), 2019), https://www.youtube.com/watch?v=DsEgs-MNKN4.; Statista Research Department, "Distribution of Google Segment Revenues from 2017 to 2021," Statista (Statista, December 2, 2022), https://www.

statista.com/statistics/1093781/distribution-of-googles-revenues-by-segment/.; Maria Korolov, "Biography," Maria Korolov, accessed December 1, 2022, https://www.mariakorolov.com/new-page/bio/

277 Statista Research Department, "Distribution of Google Segment Revenues from 2017 to 2021," Statista (Statista, December 2, 2022), https://www.statista.com/statistics/1093781/distribution-of-googles-revenues-by-segment/.

278 John Myers, "Column: How Your Data Are Shared and Sold Could Be California's Marquee Ballot Battle in 2018," Los Angeles Times (Los Angeles Times, November 26, 2017), https://www.latimes.com/politics/la-pol-ca-road-map-privacy-consumers-ballot-measure-20171126-story.html.; Shira Ovide, "Nope to Metamates, Googlers and Puritans," The New York Times (The New York Times, February 16, 2022), https://www.nytimes.com/2022/02/16/technology/metamates-googlers.html.

279 Katelyn Ringrose and Jeremy Greenberg, "California Privacy Legislation: A Timeline of Key Events," Future of Privacy Forum, July 1, 2020, https://fpf.org/blog/california-privacy-legislation-a-timeline-of-key-events/.

280 Ben Adler, "California Passes Strict Internet Privacy Law With Implications For The Country," NPR: Morning Edition (NPR, June 29, 2018), https://www.npr.org/2018/06/29/624336039/california-passes-strict-internet-privacy-law-with-implications-for-the-country.

281 Alice Marini et al., "Comparing Privacy Laws: GDPR v. CCPA" (OneTrust DataGuidance & Future of Privacy Forum, December 2019), https://fpf.org/wp-content/uploads/2019/12/ComparingPrivacyLaws_GDPR_CCPA.pdf.

282 How the California Consumer Privacy Act (CCPA) Will Affect You and Your Business | TECH(Talk), YouTube (TECH(talk), 2019), https://www.youtube.com/watch?v=DsEgs-MNKN4.

283 Shirin Ghaffary, "San Francisco's Facial Recognition Technology Ban, Explained," Vox, May 14, 2019, https://www.vox.com/recode/2019/5/14/18623897/san-francisco-facial-recognition-ban-explained.

284 Megan Cassidy, "Facial Recognition Tech Used to Build SFPD Gun Case, Despite City Ban," San Francisco Chronicle, September 25, 2020, https://www.sfchronicle.com/bayarea/article/Facial-recognition-tech-used-to-build-SFPD-gun-15595796.php.

285 Kate Conger, Richard Fausset, and Serge F. Kovaleski, "San Francisco Bans Facial Recognition Technology," May 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html.

286 Conger et al, "San Francisco Bans Facil Recognition Technology."

287 Sarah Ravani, "Oakland bans use of facial recognition technology, citing bias concerns," San Francisco Chronicle, July 17, 2019, https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php.

288 Peter Hegarty, "East Bay City Becomes Latest to Ban Use of Facial Recognition Technology," East Bay Times, December 18, 2019, https://www.eastbaytimes.com/2019/12/18/east-bay-city-becomes-latest-to-ban-use-of-facial-recognition-technology.

289 City of Somerville, "Police Department," accessed May 26, 2021, https://www.somervillema.gov/departments/police.

290 Nik DeCosta-Klipa, "Boston City Council Unanimously Passes Ban on Facial Recognition Technology," Boston.com, June 24, 2020.

291 Kashmir Hill, "How One State Managed to Actually Write Rules on Facial Recognition," The New York Times, February 27, 2021, https://www.nytimes.com/2021/02/27/technology/Massachusetts-facial-recognition-rules.html.

292 Rachel Metz, "Portland Passes Broadest Facial Recognition Ban in the U.S.," CNN Business, September 9, 2020, https://www.cnn.com/2020/09/09/tech/portland-facial-recognition-ban/index.html.

293 Courtney Linder, "Why Portland Just Passed the Strictest Facial Recognition Ban in the U.S.," Popular Mechanics, September 12, 2020, https://www.popularmechanics.com/technology/security/a33982818/portland-facial-recognition-ban.

294 Baltimore City Council, "Ordinance #21-038: Surveillance Technology in Baltimore."

295 Cordilia James, "NYC Council Passes Tenant Data Privacy Act," The Real Deal, April 29, 2021, https://therealdeal.com/2021/04/29/nyc-council-passes-tenant-data-privacy-act.

296 Aponte, Claudia Irizarry. "Facial Recognition Finds Its Match in Once Crime-Plagued Bronx Housing Complex." THE CITY. THE CITY, December 13, 2021. https://www.thecity.nyc/bronx/2021/12/12/22831457/facial-recognition-bronx-housing-

complex.

297 Kathryn Brenzel, "NYC Seeks to Rein in Keyless Technology in Apartment Buildings," The Real Deal, October 7, 2019, https://therealdeal.com/2019/10/07/nyc-seeks-to-rein-in-keyless-technology-in-apartment-buildings.

298 Elizabeth Kim, "Hell's Kitchen Landlord Sued For Keyless Entry System Agrees To Provide Keys," Gothamist, May 8, 2019, https://gothamist.com/news/hells-kitchen-landlord-sued-for-keyless-entry-system-agrees-to-provide-keys.

299 Green, Matthew. "Meet the Ellis Act, the Law Driving Many San Francisco Evictions." KQED, November 8, 2013. https://www.kqed.org/news/117540/the-ellis-act-and-san-francisco-evictions-a-primer.

300 Cal. Civ. Code §1940.2.

301 "Harassment by Landlord," San Francisco Tenants Union. https://sftu.org/harass/

302 The United States Department of Justice, "The Fair Housing Act," Justice.gov, August 6, 2015, https://www.justice.gov/crt/fair-housing-act-1.

303 Texas Department of Housing and Community Affairs v. Inclusive Communities Project, Inc., 576 U.S. 519 (2015)

304 TechEquity, "Tech, Bias, and Housing Initiative: Tenant Screening," TechEquity Collaborative, February 23, 2022, https://techequitycollaborative.org/2022/02/23/tech-bias-and-housing-initiative-tenant-screening/.

305 State of California Civil Rights Department, "FAIR HOUSING FACT SHEET ," November 2022. https://calcivilrights.ca.gov/wp-content/uploads/sites/32/2022/11/Fair-Housing-Fact-Sheet_ENG.pdf

306 State of California Civil Rights Department, "FAIR HOUSING FACT SHEET."

307 Cal. Const. art. I, §1.

308 Cal. Penal Code §§630-638.55.

309 People v. Gibbons, 215 Cal. App. 3d 1204, 263 Cal. Rptr. 905, 1989 Cal. App. LEXIS 1186 (Court of Appeal of California, Fourth Appellate District, Division Two November 17, 1989).

310 Cal. Penal Code §647.

311 Carson, Biz. "This Is What It Looks like When a Google Lawyer Tries to Evict a Beloved Tenant." Business Insider, June 10, 2015. https://www.businessinsider.com/jack-halprin-protestors-fight-eviction-2015-6.

312 "San Francisco Administrative Code Chapter 19B: Acquisition of Surveillance Technology," American Legal Publishing, June 14, 2019, https://codelibrary.amlegal.com/codes/san_francisco/latest/sf_admin/0-0-0-47320.

313 "San Francisco Administrative Code Chapter 19B: Acquisition of Surveillance Technology."

314 American Civil Liberties Union of Northern California, "Williams v. City and County of San Francisco (Illegal Surveillance) | ACLU of Northern CA," www.aclunc.org, January 20, 2023, https://www.aclunc.org/our-work/legal-docket/williams-v-san-francisco.

315 Williams, Nathan Sheard, and Nestor Reyes, "APPLICATION for LEAVE to FILE AMICI CURIAE BRIEF – ASIAN LAW CAUCUS and BLACK MOVEMENT- LAW PROJECT, et AL. IN SUPPORT of PLAINTIFFS- APPELLANTS," n.d., https://www.aclunc.org/sites/default/files/2023-01-20%20-%20Williams%20v%20CCSF%20-%20amicus%20brief%20of%20ALC%20%2B19.pdf.

316 Federal Trade Commission, "Fair Credit Reporting Act," 2023, https://www.ftc.gov/system/files/ftc_gov/pdf/fcra-may2023-508.pdf.

317 State of California Civil Rights Department, "CRD | Civil Rights Department," n.d., https://calcivilrights.ca.gov/.

318 US Department of Housing and Urban Development, "File a Complaint – Main Page | HUD.gov / U.S. Department of Housing and Urban Development (HUD)," https://www.hud.gov/program_offices/fair_housing_equal_opp/online-complaint.

319 Tech Equity Collaborative "Residential Proptech Ethical Practice Guide." TechEquity Collaborative, April 25, 2023. https://techequitycollaborative.org/2023/04/25/residential-proptech-ethical-practice-guide/.

320 Critical Resistance. "What Is the PIC? What Is Abolition?" Accessed July 6, 2023. https://criticalresistance.org/mission-vision/not-so-common-language/.

321 Michelle Alexander, foreword to Prison by Any Other Name: The Harmful Consequences of Popular Reforms, by Maya Schenwar and Victoria Law (New Press, 2020), p. xiii.

322 Beth Richie, Dylan Rodriguez, Mariame Kaba, Melissa Burch, Rachel Herzing, and Shana Agid, "Problems with Community Control and Policing Alternatives." Critical Resistance, June 19, 2020. https://criticalresistance.org/resources/problems-with-

community-control-of-police-proposals-for-alternatives/, pg. 3.

323 SFADC, "SFADC Home." SF Anti-Displacement Coalition. Accessed April 22, 2021. http://sfadc.org/.

324 LatLong.net, "Latitude and Longitude Finder on Map Get Coordinates." Accessed July 30, 2023. https://www.latlong.net/.

325 Geocod.io. "Hassle-Free Geocoding." Accessed July 30, 2023. https://www.geocod.io/.

326 Anti-Eviction Lab, "Landlord Tech Watch." Anti-Eviction Lab. Accessed April 25, 2023. https://www.antievictionlab.org/landlord-tech-watch.

327 City and County of San Francisco, "Open Public Records: NextRequest." Accessed July 30, 2023. https://sanfrancisco.nextrequest.com/.

328 Anti-Eviction Mapping Project. "Evictorbook." Accessed July 30, 2023. https://evictorbook.com.

329 Inside Airbnb. "About." Accessed July 30, 2023. http://insideairbnb.com/about/.

330 Anti-Eviction Mapping Project, People Power Media, Ocean Hill Brownsville Tenants Alliance, AI Now Institute, and UT Austin. "Landlord Tech Watch," 2020. https://antievictionmappingproject.github.io/landlordtech.

331 Steve Mann, "Sousveillance," 2002. http://wearcam.org/sousveillance.htm.

332 Ruha Benjamin, Race After Technology: Abolitionist Tools for the New Jim Code. John Wiley & Sons, 2019.