ANTI EVICTION LAB

PRIVACY AND PROPERTY: A BRIEF ANALYSIS OF CALIFORNIA AND TEXAS TENANT RIGHTS

BY ANDREW LIQUIGAN

ABSTRACT

While often proposed for the purpose of tenant security, surveillance cameras can be an imposing and intrusive force in both public and private housing contexts that may jeopardize tenants' biometric privacy. Lacking strong federal guidance regarding video surveillance, state policies and their controlling principles are the primary determinant factors regulating camera use and installation. An analysis of California and Texas civil and property codes reveal that the degree of protection granted by California's laws creates a more privacy-oriented defense for tenants challenging camera installation, while Texas tenants may find themselves more dependent on property-based claims. Additionally, both California's CCPA and Texas' CUBI Act create limited ability for tenants to control biometric data collected by cameras when compared to Illinois' BIPA.

THIS POLICY BRIEFING BY THE ANTI-EVICTION LAB HAS BEEN MADE IN COLLABORATION WITH THE ANTI-EVICTION MAPPING PROJECT AND HAS RECEIVED FUNDING FROM THE FORD FOUNDATION

INTRODUCTION

ANDREW LIQUIGAN

As private landlords become increasingly connected with new surveillance technologies, the means available to tenants for resisting such intrusions grows more urgent. However, these means are defined by each state's pre-existing frameworks, which vary widely. To illustrate the considerations necessary for creating a legal plan of action for tenants, this brief will compare the difference in options available to tenants in California as compared to those in Texas when challenging intrusions on their privacy, both in terms of surveillance and biometric collection. Private housing contexts (i.e., those that do not receive federal funds) are especially complex because they fall outside of federal regulations governing facial recognition. Privacy is a major legal interest in the state of California, as in article 1, section 1 of its constitution, California explicitly defines privacy as an inalienable right, creating an expansive domain of legal protection.[1] However, Texas does not have an equivalent privilege for rights to privacy in its laws. California's strong privacy protections in its constitution and laws therefore afford tenants more routes to challenge invasive landlord surveillance directly as compared to their Texas counterparts, who may find more leverage through quiet enjoyment rights associated with the Texas Property Code than through the state's existing privacy laws.

[1] California Constitution, Article 1, Section 1

VIDEO SURVEILLANCE AND WIRETAPPING

The installation of video cameras is generally motivated with the hypothetical end of increasing security on a property, which generally aligns with the landlord's common law duty to provide a secure and safe dwelling for residents. Normally, cameras may be placed legally in any common area on the property where a higher degree of privacy would not normally be expected. However, the presence of camera systems can become an intrusive force for tenants, especially when they are actively used by landlords to monitor their normal daily activities. This problem is made worse when facial recognition technologies are also being employed by these camera systems (an issue that will be revisited in the biometrics section).

One of the few common protections that comes into play for camera systems are state and federal wiretapping laws, which generally prohibit the capture and use of audio recordings of confidential communications. California and Texas also each have state laws against wiretapping, though the wording of each law differs. Texas Penal Code Section 16.02 defines the unlawful use, interception, or disclosure of "wire, oral, or electronic communication."[2] The California Invasion of Privacy Act (CIPA), comprising Chapter 1.5 of the California Penal Code, fulfills a similar role, protecting against the capture of "confidential communications"—those where there is no expectation among the attending parties of being overheard—in both audio and video formats.[3] (It's worth noting that conversations occurring in semi-public spaces like apartment common areas may or may not qualify under this standard and will vary depending on the facts of the case at hand.)

[2] Texas Penal Code §16.02
[3] "California Recording Law," Digital Media Law Project, September 10, 2022, https://www.dmlp.org/legal-guide/california-recording-law.

A major difference between the states' treatment of recordings, however, is that Texas is a one-party consent state for recordings (meaning only one party in a conversation must consent for a recording of the conversation to be lawful), whereas California requires that all parties in attendance consent to the recording. As such, even recordings of conversations which include, for example, the landlord may not be considered legal under California's standard, assuming that the conversation occurring falls under the aforementioned definition of confidential communication.

Furthermore, a common fair housing protection is available in cases where surveillance may be regarded as harassment. California and Texas have laws prohibiting tenant harassment (respectively defined in California Civil Code Section 1942.5 and Texas Property Code Section 92.331). For example, because California and Texas both prohibit retaliation and harassment of tenants by landlords, any installation of cameras or recording devices that could constitute harassment can readily be challenged. If after a tenant makes a lawful challenge or complaint against their landlord, the landlord chooses to install an intrusive camera immediately outside of their doorstep, a tenant may challenge this action in a suit.

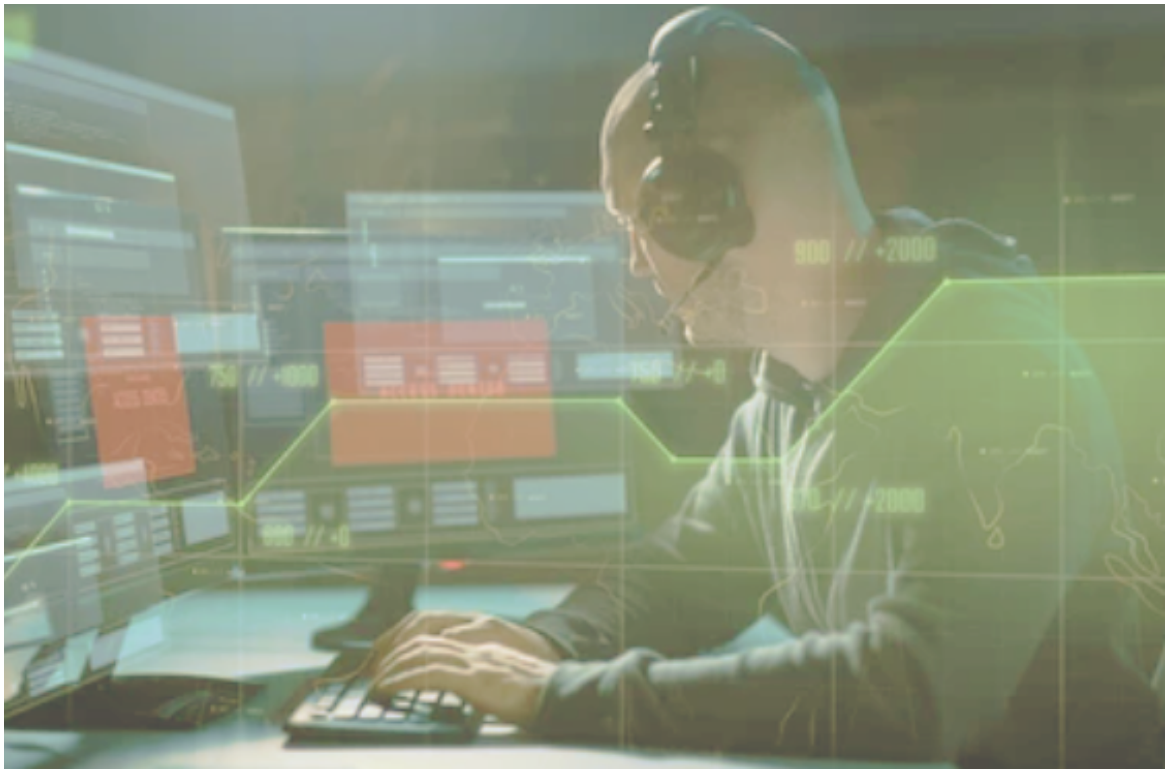
Finally, California and Texas both have laws prohibiting recording of private spaces such as bedrooms; however, there is a significant difference in the way that each state constructs its protections. Whereas California creates prohibitions against viewing areas where an occupant has a reasonable expectation of privacy (such as bedrooms, bathrooms, and dressing rooms) through the privacy protections established by CIPA, Texas' laws regarding invasive video recording are codified in Section 21 of its penal code, which dictates sexual offenses. As such, invasive video recording is constructed in the Texas penal code to focus on video capture occurring "without the other person's consent and with intent to arouse or gratify the sexual desire of any person."[4] As a result of Texas' penal code being less generalized, the applicability of Texas' penal code to housing contexts is much more limited than is California's.

Given the limits of the legal construction of invasive video prohibitions in Texas, the Property Code appears a more controlling force in the legal framework available to tenants seeking remedy against invasive landlord surveillance in Texas. Namely, Chapter 24 of the Texas Property Code outlines the covenant for "quiet enjoyment" and "constructive eviction."[5]

[4] Texas Penal Code §21.15
[5] Fambrough and Adams III, "Landlord and Tenants Guide."

Under the quiet enjoyment covenant, a landlord and/or any individual deriving title from the landlord may not disturb a tenant's quiet use and enjoyment of the property.[6] Constructive interference is defined as interference with tenant use and enjoyment that is substantial enough to force the tenant to abandon the property (in essence, constructing eviction by creating a disturbance that forces the tenant out).[7] Tenants who feel that the installed video surveillance systems interfere with their peace and privacy on the premises could therefore consider challenges of violation of the quiet enjoyment covenant or, in an especially severe case of invasive action, of constructive interference.

[6] Judon Fambrough and E.V. "Rusty" Adams III, "Landlord and Tenants Guide," March 2019, https://assets.recenter.tamu.edu/Documents/Articles/866.pdf.
[7] Fambrough and Adams III, "Landlord and Tenants Guide."



BIOMETRICS

Biometric markers are a significant piece of personal information that is under increasing pressure for collection by various entities. With the progressive advent of improvements to AI and camera quality, facial recognition has seen an increase in adoption throughout the country. In Texas, Atlas of Surveillance presently lists 19 documented facial recognition system purchases since 2002, with activity increasing especially after 2018.[8] Many surveillance systems, even those available to standard, non-governmental consumers, are beginning to advertise facial recognition abilities as well. For example, both Bosma and Wyze, two smart home companies, offer services that utilize cloud facial recognition, and several other home monitoring services offer facial recognition locally.[9]

Even in lieu of built-in facial recognition functionality, recordings collected and used by police can still be run through facial recognition software separately, as is the case with Ring, which heavily partners with police to allow sweeping access to video recordings through their Neighbors network.[10] It is worth noting, furthermore, that Ring itself has been subject to scrutiny by the FTC for utilizing user data to develop image algorithms without affirmative consent.[11] As such, consumers may unwittingly allow recognition softwares to operate on their data when installing them in private contexts.

[8] Atlas of Surveillance. “Texas - Atlas of Surveillance.” Accessed September 1, 2023. https://atlasofsurveillance.org/search?utf8=%E2%9C%93&location=Texas&technologies%5B87%5D=on.

[9] Wroclawski, Daniel. “Facial Recognition Is Coming to Your Neighborhood through Home Security Cameras and Video Doorbells.” Consumer Reports, May 2, 2023. https://www.consumerreports.org/electronics/privacy/facial-recognition-and-home-security-cameras-video-doorbells-a9500287020.

[10] Kelley, Jason, and Matthew Guariglia. “Ring Reveals They Give Videos to Police without User Consent or a Warrant.” Electronic Frontier Foundation, July 15, 2022. https://www.eff.org/deeplinks/2022/07/ring-reveals-they-give-videos-police-without-user-consent-or-warrant.

[11] Fair, Lesley. “Not Home Alone: FTC Says Ring’s Lax Practices Led to Disturbing Violations of Users’ Privacy and Security.” Federal Trade Commission, May 31, 2023. https://www.ftc.gov/business-guidance/blog/2023/05/not-home-alone-ftc-says-rings-lax-practices-led-disturbing-violations-users-privacy-security.

Biometric entry systems have also emerged on the market, often portrayed as a "smarter" means of validating the identities of those entering. In such systems, fingerprints, palm prints, or face scans are normally used by apartment complexes as an alternative to electronic fob-based entry validation, and they have not gone unnoticed. In 2019, Nelson Management Group made the news for planning a transition away from key entry to facial recognition at its Atlantic Plaza Towers property, against which over one hundred tenants filed a formal complaint with the state of New York.[12] At this junction, housing and consumer protection overlap significantly, as the deployment of biometric solutions by landlords and the companies that store the data itself create separate but related agents. In the absence of strong federal guidelines dictating how this data is collected, stored, accessed, and destroyed, state policies have been the primary arena for creating and enforcing regulations.

While Texas boasts the Capture or Use of Biometric Identifier Act (CUBI), its application is quite limited when compared to its legal predecessor, the Illinois' Biometric Information Privacy Act (BIPA), which passed one year earlier in 2008 and remains the most famous state biometric regulation.[13] The difference in wording between "identifier" and "information" is one key manner in which the two differ. Retina scans, fingerprints, voiceprints, and records of facial and hand geometries are classified in both acts as biometric identifiers. However, BIPA also defines biometric information as any information "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual" so long as the information is not excluded under the parameters defining biometric identifiers.[14] This additional definition grants BIPA more power against the capture and storage of individuals' biometrics. Furthermore, CUBI does not include a private right of action, whereas BIPA does. Private individuals are not at liberty to file challenges under CUBI—instead, the Texas attorney general holds the power to bring action under the law. However, CUBI does hold the advantage for consumers in terms of limiting the duration during which biometrics may be stored. While BIPA defines a timeframe of three years to destroy biometric data,

[12] Durkin, Erin. "New York Tenants Fight as Landlords Embrace Facial Recognition Cameras." The Guardian, May 30, 2019. https://www.theguardian.com/cities/2019/may/29/new-york-facial-recognition-cameras-apartment-complex.

[13] Browning, John G. "The Battle Over Biometrics." Texas Bar Journal, October 2018.

[14] Illinois General Assembly. "740 ILCS 14/ Biometric Information Privacy Act." www.ilga.gov, n.d. https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

CUBI requires that information be destroyed in a "reasonable amount of time," though no later than one year after the purpose of collection has expired.[15]

California's digital privacy landscape features several initiatives at the city and state level to curb inordinate use and capture of biometrics. In particular, San Francisco and Oakland imposed an outright ban on the use of facial recognition technologies by their city government agencies in 2019.[16] However, in lieu of a particular piece of legislation targeting biometric privacy, the state opted to amend the California Consumer Privacy Act (CCPA) in 2018 to define biometric information as one of several types of sensitive personal information it regulates. This strategy of generalized protection is an approach it shares with Colorado, Virginia, Connecticut, and Utah.[17]

Under the CCPA, consumers have the right to know what types of information are being collected about them. Therefore, as is required also by both BIPA and CUBI, individuals whose biometrics are being collected must be informed that collection is taking place, and CCPA further requires maintenance of a detailed privacy policy by business entities. CCPA also enforces standards of security and practice in businesses' handling of biometric data and provides individuals rights to deletion and limiting of use and disclosure for that data.[18] Finally, CCPA has elements of similarity with both Texas and Illinois' biometric laws. It does provide for a private right of action like BIPA, though only in a particular instance. Consumers may file litigation under CCPA if their data is compromised in a breach for which the storing entity failed to maintain the defined security measures. [19] Otherwise, enforcement of CCPA rests exclusively with the California attorney general.[20]

[15] Tex. Bus. & Com. Code Ann. § 503.001
[16] Haskins, Caroline. "Oakland Becomes Third U.S. City to Ban Facial Recognition." www.vice.com, July 17, 2019. https://www.vice.com/en/article/zmpaex/oakland-becomes-third-us-city-to-ban-facial-recognition-xz.
[17] Nahra, Kirk, Ali Jessani, and Samuel Kane. "Biometric Privacy Law Update." www.wilmerhale.com, February 24, 2023. https://www.wilmerhale.com/insights/client-alerts/20230224-biometric-privacy-law-update.

[19] Blank Rome LLP. "Analyzing the CCPA's Impact on the Biometric Privacy Landscape." Blank Rome LLP, October 14, 2020. https://www.blankrome.com/publications/analyzing-ccpas-impact-biometric-privacy-landscape.
[20] Blank Rome LLP. "Analyzing the CCPA's Impact on the Biometric Privacy Landscape."
[18] State of California Department of Justice. "California Consumer Privacy Act (CCPA)." State of California - Department of Justice - Office of the Attorney General, May 10, 2023. https://oag.ca.gov/privacy/ccpa.

Without improved frameworks governing how biometric information is ethically used and stored, it is likely that the issues associated with biometrics will continue to grow, both in terms of their frequency and complexity. Apart from state regulations, the federal landscape for protections remains turbulent, and the federal government has wrestled with its own deployment of facial recognition in public housing.[21] As mentioned previously, landlord technologies like biometrics present a legal nexus between housing and digital privacy. It is therefore worthwhile for housing advocates and tenants to keep a watchful eye over legal developments, whether at the city, state, or federal level, that can be informative toward what defines suitable use of surveillance and entry systems which depend on biometric markers.

[21] MacMillan, Douglas. “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.