ESPLER PROJECT INC.

CALIFORNIANS FOR PRIVACY: HOW THE WAR ON SEX WORK IS STRIPPING YOUR PRIVACY RIGHTS

Index

This report was made possible with a grant from the Rose Foundation, which envisions a future where nature is protected, people's rights are ensured, and environmental justice is advanced, and where these three values are deeply interconnected. Learn more or donate at RoseFdn.org

About Us: The Erotic Service Provider Legal Education and Research Project

This report was produced by ESPLER Project, Inc. (ESPLER), a California-based advocacy nonprofit. The main issue addressed by ESPLER is decriminalization of sex work. To achieve this end, ESPLER's day-to-day work advances worker rights, consumer privacy rights, and sexual privacy rights. We educate erotic service providers, policy makers, and the public through coordinated outreach, research, and legal advocacy.

In 2017, ESPLER brought ESPLERP v Gascón [16-15927], a constitutional challenge to California's anti-solicitation for prostitution law known as Penal Code 647(b) PC to the U.S. Court of Appeals for the Ninth Circuit. The Gascón case argued that criminalizing sex work violates consumers and the sellers right to sexual privacy, based on the groundbreaking 2003 Lawrence v. Texas case, which acknowledged the right to sexual privacy for sexual relations between people of the same sex, thereby decriminalizing homosexuality.

Learn more at esplerp.org

Access the data behind this report at ca4privacy.org

Privacy Protections at the Intersection with Prostitution

We all know things have gone too far with our phones and businesses collecting data about us. Understanding the scope of the problem and its full legal context is daunting. Current discourse and legislative efforts have centered around consumer privacy–but what about criminalized consumers and workers? As usual, sex workers and our clients are excluded from these protections.

The 2018 California Consumer Privacy Act, now the California Privacy Rights Act, gave Californians many rights when it comes to the data collected about them by businesses, but no privacy rights exist to protect any of us from police or nonprofits. As a result, there is no mechanism for sex workers or our clients to access the protections of these privacy rights.

The criminalization of prostitution keeps sex workers and our clients centered–naked–in the public sphere, literally stripping us of our privacy rights. Decriminalization means having our sexual privacy protected and having access to equal protection under the law regardless of whether we utilize commerce in our sex lives or not.

> The power to define problems, terms and solutions rests with social agents, who debate how to get others to behave differently, even save them from themselves – the disadvantaged, unruly, victimized, unhappy, offensive, addicted.
> - Laura Agustin, *Sex at the Margins*

Sex Workers are the Canaries in the Coal Mine

Imagine this: you pick your girlfriend up from work. Maybe the store she works at is in an area known for street prostitution, or maybe it shares a strip mall with an adult massage parlor. A pole camera left by police snaps a picture of your girlfriend getting in your car and feeds it through an Automated License Plate Reader (ALPR) database where it connects it to your name and adds you to a list. The next week you get a Dear John letter in the mail - maybe it's from the local police[1] or maybe from a nonprofit[2]. It's vaguely threatening and shaming, telling you that prostitution is associated with human trafficking, kidnapping, and drugs, and that the police are

[1] LA City Council Considers Sending 'Dear John' Letters To Homes Of Men Who Solicit Prostitutes - CBS Los Angeles
Letter-for-Dear-John.pdf
[2] Oakland Residents Hope 'Dear John' Letters Help Curb Prostitution - CBS San Francisco

cracking down on people like you. Just a misunderstanding, you think. No big deal. But later that year, when you and your girlfriend are traveling home from overseas, you're stopped at customs. They search your phone and laptop. They take your girlfriend aside and ask her where she met you, how long she's known you, if she's okay. Afterwards, she wonders if there's something you're not telling her. You don't know it, but you're in a database. It's 2023 and this is the USA.

Law is the quintessential form of the symbolic power of naming that creates the things named, and creates social groups in particular.
- Bourdieu, *Force of Law*

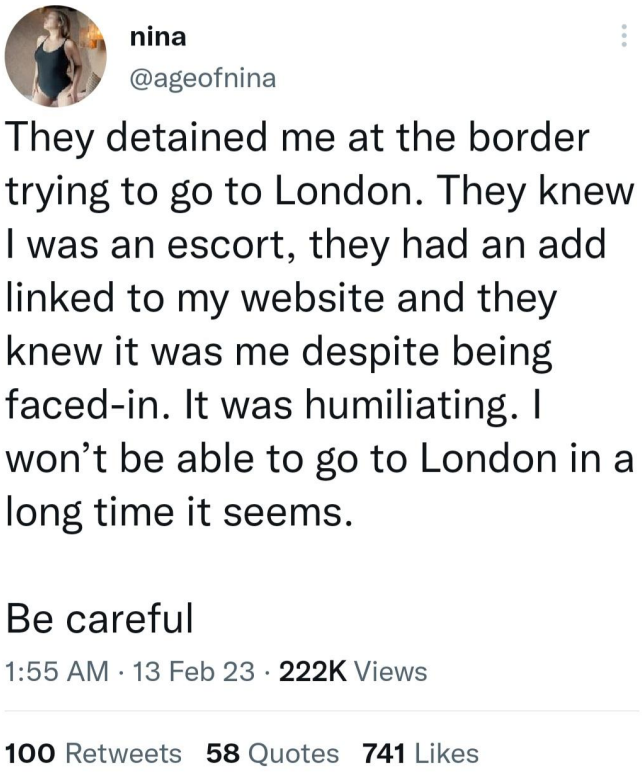
The American Law Institute first voted to recommend decriminalizing sodomy (aka gay sex) in 1955, and published their recommendations in the Model Penal Code in 1962. In the same document they recommended criminalizing prostitution, defining it this way: "*A person is guilty of prostitution, a petty misdemeanor, if he or she: (a) is an inmate of a house of prostitution or otherwise engages in sexual activity as a business; "Sexual activity" includes homosexual and other deviate sexual relations.*"[3]

[3] Model Penal Code. 1962

Sodomy wasn't fully decriminalized in the US until *Lawrence v Texas* in 2003.[4] Until then, it was accepted that police must barge into bedrooms or read gay people's love letters in order to take them to jail, so that children would be safe from them.[5]

> Stigma is a process by which the reaction of others spoils normal identity.
>
> — Erving Goffman

We know that today, police, for-profit businesses, and even nonprofits have bots that build databases with biometric profiles of suspected sex workers, our social media, and even location data. It is unclear whether there are databases which surveil clients of sex workers. Police use pole cameras to surveil areas where they think they will find street based prostitution. The cameras snap pictures of vehicles and their occupants, filing them away with the date, time, and GPS coordinates. They photograph sex workers' faces, bodies, and tattoos for their databases, and it only takes a few clicks for them to download anyone's iCloud, Facebook data, location history, and whole phone's worth of data. They call it phone ripping. There are trainings that teach them how, slideshows where instructions for photographing ALL of sex workers' tattoos appear alongside advice like "what your DA doesn't want to see: you having too much fun."[6] They call it vice enforcement, human trafficking, commercial sexual exploitation, prostitution, or the b-girls program. They can't decide what to call us, what words would make it seem okay that they do all of this because consenting adults are having sex of which they don't approve.



It's all to save the children, they say. If sex workers aren't victims, we must have started out as child trafficking victims and grown up to become child traffickers. It's the same thing they used to say about LGBTQIA+ people.[7] The police can't find enough children to meet the demand they've created with all their public awareness campaigns, so they cast their nets wider and wider. They can find more sex trafficking, they just need broader definitions of sex trafficking.

---

[4] "Decriminalizing Sodomy in the United States." *The Decriminalization of Sodomy in the United States | Journal of Ethics | American Medical Association*

[5] Accusations of 'grooming' are the latest political attack — with homophobic origins

[6] ICI Vice Investigations Ethics Law, Stanislaus County, Slide 42

[7] The Problem with the Belief that Child Sexual Abuse Causes Homosexuality / Bisexuality | PFLAG Atlanta

They've cast the nets so widely that, as a matter of national security, the Department of Homeland Security now operates prostitution stings with the purpose of arresting men for agreeing to pay for consensual sex with another adult.[8] In other prostitution stings, Homeland Security has justified having "too much fun" by saying the women they tricked into giving them handjobs before arresting them were actually sex trafficking victims.[9] How wide can the net go?

Readers may wonder whether there is a financial incentive for broadening the definition of sex trafficking. Police departments may claim to be underfunded. However, this is not statistically likely. Historically, spending on police, corrections, and courts has steadily increased since mid-1990s (with a brief dip following the 2008 financial crisis) nationally[10] and locally[11].

As the definitions of sex trafficking stretch to encompass and implicate more and more people, more and more of us are left managing "spoiled identities."[12] Sex workers, our clients, our friends, cab drivers, nannies; we are all implicated as being part of or related to the "sex trafficking industry" now. What does it mean, in the age of social media, and unprecedented police surveillance, to manage such a spoiled identity?

We started this research project to learn about the technologies police use in their surveillance of sex workers and their clients, but we learned that we are just the canaries in the coal mine. The police are watching all of us, even you.

---

[8] HSI Phoenix assists in multi-agency operation, 18 men arrested on prostitution and other charges | ICE

[9] Homeland Security Agents Receive Handjobs in Lake Havasu 'Human Trafficking' Stings - Front Page Confidential

[10] Criminal Justice Expenditures: Police, Corrections, and Courts, *Urban Institute*

[11] Police costs in Southern California: By the numbers *Orange County Register* August 30, 2020

[12] Erving Goffman, *Stigma: Notes on the Management of Spoiled Identities*

Why We Did It

We know that local, state, and federal law enforcement agencies in California are increasingly turning to technology to target sex workers and our clients, from surveillance equipment to online undercover operations. What tools police use to surveil us on a day-to-day or case-by-case basis is a closely guarded secret. The victims of these overzealous prostitution investigations often never learn how digital tools were used against them.

This has led to misinformation being shared within the sex work community. For example, there is a widely held belief that sex workers are often stopped and turned away at borders because a certain advertising website is giving photos of sex workers' IDs to police. It turns out that the way sex workers are most likely identified at borders is through a database called Traffic Jam, or one similar to it, that archives advertisemets from 14 different sex work advertising sites every hour and builds biometric profiles of advertisers, including facial and tattoo recognition, social media information, location data, emails, and phone numbers. In learning about Traffic Jam, we also learned about similar databases that crawl social media, buy location data from certain phone apps, and maintain profiles of virtually everyone who exists online. As sex workers, we are concerned about the technology that is used to hunt our data and our clients', but everyone should be concerned about mass surveillance, doublethink, and manipulation by agencies that are paid for with our tax money.

Public records requests use laws like the California Public Records Act (CPRA) or the federal Freedom of Information Act (FOIA) to make state and federal law enforcement agencies produce records like receipts and invoices for surveillance equipment. FOIA requests can also bring to light the lesson plans, syllabi, presentations, and videos that are used to train police officers to use surveillance technology in prostitution stings. This report draws from tens of thousands of pages of invoices, purchase orders, receipts, and instructional documents obtained through public records requests: Viewed collectively, these records present a vast and alarming threat to worker and consumer privacy.

We picked the time frame of January 1, 2020 through February 28, 2022 for our public records request because it was recent and it covered the time frame of the Super Bowl that was held in Los Angeles in February 2022. Because of COVID lockdowns, we expected to see a decrease in sex worker citations and arrests, though the actual number of citations and arrests was not our primary focus here. We wanted to know what technology they used to make arrests for solicitation of prostitution (647(b) and loitering with the intent to commit prostitution (653.22). Before the rise of the use of so much digital technology in our lives, we used to know how prostitution arrests occurred.

Prostitution arrests generally occur in an undercover fashion, when the police contact a suspected sex worker under the guise of becoming a client, or the other way around. The solicitation of prostitution law in California has three parts that have to be satisfied to make a conviction but not necessarily an arrest:

1. The sex act, aka, the lewd act–the touching of body parts, essentially.
2. The compensation: this can include but is not limited to money–just anything of value.
3. The last part is called 'the act of furtherance'. The first two parts are protected under the First Amendment; anyone can talk about sex acts and compensation but the last part means taking action towards manifesting parts one and two. This could be showing up at a hotel room or getting into an undercover police officer's car, accepting or giving money, saying what kind of sex act, saying you want to use a condom, or asking to bring a condom.

These stings–fraudulent, taxpayer funded affairs–generally happen in hotels whereby the police use a hotel room with the permission of the hotel to host these stings. Another method they use is to contact a suspected sex worker in his or her home for their services followed by an arrest for prostitution; or, in some cases, a citation is issued. In either and in any case, the district attorney has up to a year to file these misdemeanor charges. Sometimes the undercover stings are generated as a result of a complaint that is lodged with police about a specific person or persons. For many of these law enforcement jurisdictions, the anti-prostitution undercover sting operations are conducted by the 'vice' department and have been routine undertakings prior to the digitization of everything.

The loitering with intent to commit prostitution law, PC 653.22 was repealed as of January 1, 2023 because it was most often used by police to arrest transgender women and women of color–many of whom not actual prostitutes–walking in 'known prostitution areas'.

The general public thinks of street-based sex work when it thinks of prostitution, but the profession is not a monolith and includes escorts, massage parlor workers, professional dominatrices and submissives, and other erotic service providers. When arrested for prostitution, sex workers can go to jail, be sentenced to go to diversion programs (similar to church reprogramming for LGBTQIA+ kids), have our names and pictures in the newspapers or online, lose our employment, or be subject to discrimination in housing, employment, child custody matters, and banking for the rest of our lives.

Methodology: What We Did

A Word About the Process

ESPLER Founder and Executive Director Maxine Doogan, the primary instigator of this project, has been doing public records requests of public agencies since 2005 to try to understand how the state views prostitution. In one case, San Francisco's Sunshine Ordinance Task Force found in Maxine's favor that then-District Attorney of San Francisco Kamala Harris' office was in violation of public records law in not providing the records Maxine had requested.[13] The grant ESPLER received from the Rose Foundation provided an opportunity to expand on this type of investigation and to better understand how the ever-expanding use of technology in our world and specifically how prostitution surveillance and arrests affect Californians' privacy rights.

Obtaining the Cases, Invoices, and Purchase Orders

> Reading is one way of appropriating the symbolic power which is potentially contained within the text. Thus, as with religious, philosophical, or literary texts, control of the legal text is the prize to be won in interpretive struggles.
> - Bourdieu, *Force of Law*

Our first round of California Public Records Act (CPRA) requests, crafted with our attorney, asked California county sheriffs departments and police departments if they had made arrests for 647(b) and 653.22 (prostitution and loitering with intent to commit prostitution), and if they had, to provide the citation numbers and what technology they had used. Figuring out which agencies to ask wasn't difficult, since many of them sent out press releases announcing their prostitution arrests during our time period of inquiry, January 1, 2020 through February 28, 2022.

Our first CPRA request asked for:

- All citation and arrest statistics for California Penal Code Section 647(b) and 653.22 for the time period of January 1, 2020 through February 28, 2022.
- All police and incident reports (or equivalent summaries of police interactions) and field interview cards associated with all citations and arrests conducted in reference to violations of 647(b) and 653.22.
- All available technologies and platforms used in the investigation and securing of 647(b) and 653.22 citations and arrests.
- Any policies regarding an agency's use of the applicable technologies.
- Responsive materials including all policies and procedures related to:

[13] Order of Determination, October 23, 2007

    - the acquisition of the technology, including guidance regarding procurement through the bidding process, third parties, or any other method
    - the use of the technology, including data collection, retention, and disposal
    - training on and coordination of the technology
    - any application, affidavit, or similar records created in the course of use of this technology
    - the sharing of the equipment itself
    - the sharing of any information gathered by the technology, either with other police departments, the district attorney, or any other entity, inside or outside of the local criminal justice system
- Materials regarding this agency's acquisition of the applicable technologies, including all bidding and procurement materials, such as the initial Request for Bids, Request for Proposals, and equivalent bidding records.
- Invoices, receipts, and any equivalent financial documentation related to payments for the technologies

Over the course of the project, we sent this request to 58 district attorneys, 37 probation departments, 58 sheriff's departments, and 52 police departments across the state of California. We received partial, but varying records from most agencies. Those agencies that did not drag out the process denied the public records requests outright (read on for examples). Not one agency provided all of the records we requested, as they are required to do by the CPRA.

The first round of public records requests (PRR) was made through the individual law enforcement websites of the 52 police departments and 58 county sheriff's departments. The first requests received a low level of acknowledgements and responses. While following up, attempts to find the direct contact information of the person responsible for responding to PRR within each agency led to learning that many of the online portals didn't work for a number of reasons. In some cases, these law enforcement agencies had moved their online presence to another URL. For example, the Santa Ana police department's online portal does not work. In a phone call, we were told to go through the city of Santa Ana website to make the request. Why doesn't the police department just have that on their website? Law enforcement websites aren't likely broken due to lack of funding. For the record, the average California City's top budget line item is spending on policing[14]. In fiscal year 2020, California topped the nation in per capita state and local governments spending on police[15].

We spent 21 minutes on hold with the San Jose Police Department to get an email address. When we called the Ventura Police Department we were told we had to submit our request in writing via mail so that they could charge us for hard copies of records. Eventually we found their police

[14] Law Enforcement Staffing in California, *Public Policy Institute of California* February 2023
[15] State and Local General Expenditures, Per Capita, *Tax Policy Center* August 2022

chief's and records specialist's email addresses online. Ventura PD, like several other law enforcement agencies, never provided any documents, even after their initial acknowledgment, which means they're in violation of the California Public Records Act. Several agencies did their due diligence searches and found no responsive documents, meaning they'd not done any arrests for 647(b) or 653.22.

The tedium of making these requests began to feel deliberate. Many agencies used an online portal called nextrequest.com for PRR that required log in for each individual agency. It has a double opt-in system. You have to fill out a form, then wait for the link to come to your email to activate your account in order to submit a request. The drop down menu on this platform allows you to pick which department within a particular city or county to direct your records request to. In several cases, the drop down menu didn't have the county sheriff or city police agency listed as an option, which prompted more phone calls to each of those individual agencies to find out who the public records request agent was and obtain their contact information. In some cases, we were directed to another website to submit the public records request that wasn't linked on the public facing website. Note the public facing websites all have something called 'Records' which refers to people who want to get a copy of their police record but this information rarely applied in the type of records requests made for this report.

A number of agencies didn't bother responding; for those that did, the response was often confusing and sloppy. The City of Richmond Police Department didn't assign a tracking or reference number during communications. Several county sheriffs departments responded by providing the technology used in the arrests but didn't provide the citations we asked for as proof of the arrests. Or vice versa, some agencies would respond with the citations of arrests but no technology. The Santa Barbara Sheriff's Department denied our request because they "could not provide the identity of sex trafficking victims". This jurisdiction did not have an administrative appeal process, and their response was odd since we'd not asked anything about sex trafficking or identities. This led us to wonder whether they were arresting sex trafficking victims for prostitution. Then there was the Los Angeles County Sheriff's Department response, which provided us with their Human Trafficking Report, which clearly showed 90% of those arrested were for prostitution related offenses. These half responses, or in many cases no responses at all, prompted letters from our attorney, which in a few cases resulted in additional records shared. Ultimately, after eleven months of these departments dodging their responsibilities under the law, we made the decision to proceed with the records we did receive.

Another workaround we came up with to circumvent these CPRA violations was to expand our requests to include 58 county district attorney's offices. Records gained from these requests gave us a means to verify the arrest and subsequent charges by jurisdiction. Also, we wanted access to some of the police reports and charging documents so we could examine the exact way in which phone searches were being conducted, for example. While many DAs responded with case numbers of those charged, several provided their county's human trafficking reports and no case

numbers. These DAs referred us to their county courthouses to access the requested documents. Some county courts have an online portal to order case files and many do not. We went to the San Bernardino Courthouse and waited in line for an hour to fill out a form, only then to be told to wait to be contacted by a clerk at some point in the future (this contact never materialized).

In the next round of requests to these agencies about the training materials for prostitution arrests and the technology used, human trafficking was added since so many law enforcement agencies responded with information about human trafficking, in addition to their online press releases that clearly showed they had renamed those they had targeted in prostitution sting operations as sex trafficking victims and perpetrators. The question remained, were those victims of human trafficking who had been arrested for prostitution?

We asked 37 probations departments what technology they were using to supervise or further investigate those who had 647(b) and 653.22 arrests/cases, just to round out our requests. Several of them also mentioned human trafficking, which led once again to the question, were sex trafficking victims being arrested for prostitution? It seems that they were, given the many ways that law enforcement conflated prostitution with forced labor in the sex industry.

Obtaining the Trainings

We used an online platform called Muckrock.com, with the help of researchers Beryl Lipton, Dave Maass, and Paul Tepper of the Electronic Frontier Foundation, who took on the task of identifying the training materials used in prostitution investigations.

The California Commissions on Peace Officers Standards and Training (POST) is the central state agency charged with peace officer certification and approving training materials. In response to SB 978, a 2018 law requiring information about such trainings to be posted online, POST released an "open data" hub on its website, where members of the public can review the outlines for all certified trainings in California. In most cases, the trainings are not presented by POST, but by local agencies and police academies. Once identified, we set out to request copies of the full training presentations under CPRA.

Using the open data site, we identified 14 relevant training courses related to either vice investigations or human trafficking and reviewed their outlines. Of these, 12 courses were attributed to eight government agencies and therefore subject to CPRA. Two were produced by private entities (the California Narcotics Officers Association and the Lake Family Resource Center), which are not subject to CPRA.

> There is no evidence that disempowered or oppressed women and men do not also gaze, or gaze back, at the eyes that make them objects.
>
> - Agustin, *Sex at the Margins*

CPRA allows members of the public to request copies of documents (e.g., training presentations, videos, etc.) from government agencies. Typically, agencies have 10 days to respond to a request; however, they can extend the period for providing a response 14 days at a time. While agencies do have limited ability to withhold or redact information related to law enforcement intelligence techniques, that right is not absolute, and the law must be construed in favor of public access, rather than secrecy.

Using the data we retrieved from POST's Open Data website, we filed CPRA requests with seven agencies: Los Angeles Police Department (LAPD), Oakland Police Department, Riverside County Sheriff's Department, San Bernardino County Sheriff's Department, San Jose Police Department, Vacaville Police Department, South Bay Regional Training Consortium[16] (also known as "The Academy"), and the State Threat Assessment Systems[17] (STAS), which is a resource-sharing collaboration between multiple agencies and fusion centers (a type of law enforcement information and surveillance center operated in partnership with the U.S. Department of Homeland Security). Each agency–with the exception of LAPD–provided us with comprehensive records related to each of these trainings. In some cases, the records we received from one agency included presentations generated by officers assigned to other agencies.

We focused on two general categories of trainings–vice investigations and human trafficking investigations–under the assumption that there would be significant overlap between the two. Indeed, our research proved this theory, as many of the human trafficking courses often started by invoking commercial sexual exploitation of children (CSEC) but quickly shifted to consensual transactions between adults.

Unfortunately, research based on public records requests only allows for a review of the hard materials used in a training, such as slides and handouts. Without the oral information that was delivered with these presentations, we can only draw inferences from the materials about the context. However, this is not a flaw in the research method; it is a flaw in the transparency of law enforcement agencies, who generally do not allow for public access to the actual training classes themselves.

There are two other important, parallel observations we feel are important to share:

First, law enforcement agencies are required under SB 978 to post these documents online. In other words, it should not require a public records request to obtain the training materials; they should be readily available on the agencies' websites. None of the agencies covered in this report were in compliance with this law.

[16] The Academy, South Bay Regional Public Safety Training
[17] California State Threat Assessment System

Second, the presentations are offensive. They ridicule sex workers and evoke gross racial stereotypes, and some turn a serious issue into a game. Combined, these two elements reveal a level of unprofessionalism that is difficult to separate from a fully objective analysis.

How They Use Surveillance Technology to Hunt Sex Workers and Spy on Everyone

> The prostitution trial, conducted in a blaze of publicity, exposes its own structuring paradox, staging in public, as a vicarious spectacle, that which it renders criminally deviant outside the juridical domain. Through the mechanism of the prostitution trial, contradictions in the distribution of money, pleasure, and power are isolated as crimes and are then performed again in the theatrical ceremony of the trial as confession.
> - Anne McClintock 1992, *Screwing the System*

We're All In Databases

"Open source" information is publicly available online, through the media, and through public records. However, the databases that are used by law enforcement today maintain information on all of us that is beyond what anyone imagines when they hear "open source information."

Tools like TransUnion's TLOxp,[18] Thomson Reuters CLEAR,[19] LexisNexis Accurint,[20] and Coplink X[21] use web bots and scripts to capture and connect information from sex workers' social

[18] Crook Sells Access to Data Tool Used by Private Investigators, *Vice*
[19] Thomson Reuters, CLEAR
[20] Accurint® for Law Enforcement | LexisNexis Risk Solutions
[21] Coplink X - ShotSpotter

media, online reviews, and profiles on various sites. Various databases also integrate things like:

- Location data either from publicly available sources, purchased from various phone apps, integrated from automated license plate reader databases, or integrated from other businesses owned by the same company.
- Information from tax records about your home and vehicles.
- Information from other third party companies, such as car insurance, mortgage companies, and hotel chains.
- Information from sales websites such as craigslist, cross referenced with your contact information.
- Facial recognition and biometric profiling software to help the database recognize pictures of you all over the Internet by your face, tattoos, body type, etc.

All of this information is constantly scraped and archived in the databases to be accessed by police anytime. Some databases even allow police to find a location that you visit frequently, and then query the database for other phones that also visit that location frequently.

Databases Full of Sex Workers

At least two databases–Spotlight (by Thorne) and TrafficJam (by Marinus Technologies)–focus solely on sex workers. Access to Spotlight is free to law enforcement. Spotlight archives advertisements from 14 different sex work advertising websites every three hours, using phone numbers, email addresses, and facial recognition technologies to make connections between advertisements. TrafficJam archives information hourly from 14 sex work advertising websites and uses Amazon's Rekognition[22] tool, which is no longer available to law enforcement outside of the TrafficJam database,[23] to connect sex work advertisements to social media profiles and more.

For many years, sex workers have reported being stopped at border crossings, where they are intimidated, shown pictures of their old escort advertisements, and turned away from entering countries. In one case, a sex worker described being stopped driving across the Canadian border in 2011 and shown print outs of her ads, her website, and her professional social media. She was denied entry and told she would not be able to enter Canada for 10 years. Now, when she travels, she says, "[I] noticed my passport was flagged every time I had to use it when traveling internationally, and often had security officials question me in regards to prostitution. I had learned not to carry any obvious work stuff in my carry-on, factory reset all devices prior to departure, and to wait to post online ads until after I got to my destination as ways to avoid suspicion and downplay whatever assumptions they had."

[22] How Amazon Rekognition helps in the fight against some of the worst types of crime
[23] Amazon extends moratorium on police use of facial recognition software | Reuters

Within the sex work community, the popular understanding has been that some advertising websites that require IDs to make sure that advertisers are adults were providing these records to police. Now, it seems far more likely that it's actually databases like TrafficJam that archive escort ads, social media, and websites.

What the Trainings Tell Us

Police are often instructed to monitor a variety of websites[24] as part of their training on human trafficking and prostitution, from escort advertisements to dating sites to social media. A number of police trainings provide lists of certain sites to check, like those, for example, provided by Riverside County Sheriff's Department in its training for human trafficking[25] and from The Academy.[26] These lists usually include dating sites, social media, and "review websites".

*Riverside County Sheriff's Department, "*Prostitution and Human Trafficking 101*,"*[27] *page 7*

Officers at RCSD are instructed to "preserve all accounts ASAP" if they're deemed to be related to sex work. A training from RCSD[28] claims officers can learn information about the "location and layout of the business", physical and experiential details about an individual, and what services are provided from review websites, where clients review sex workers. A large portion of

[24] Websites.xlsx
[25] rcsd-no_redactions_-_prostitution_ht_101.pdf p. 7
[26] Copy of Prostitution Websites.docx
[27] rcsd-no_redactions_-_prostitution_ht_101.pdf p. 7
[28] rcsd-no_redactions_-_prostitution_ht_101.pdf p. 7

RCSD's training slides about massage parlors focuses on review pages.[29] This use of review websites by police officers is corroborated in an account by an Alaskan escort, who reported that after he received oral sex from her, and then arrested her, a police officer told her he had "seen her reviews online and wanted to see for himself what it was all about".[30]

Law enforcement can also subscribe to platforms like Spotlight[31] and TrafficJam.[32] Vacaville[33] and San Bernardino County both reference TrafficJam in their materials, although neither provided invoices showing that they use TrafficJam. Using Amazon's Rekognition[34] face recognition technology, TrafficJam allows an officer to submit an image of a person's face to see if it matches anyone in TrafficJam's database.

San Bernardino County Sheriff's Office, "Human Trafficking Investigations,"[35] page 76

What the Invoices Tell Us

This list must be considered incomplete, as law enforcement agencies provided either no records or incomplete records (for example, only manuals). While San Bernardino provided what seemed

[29] rcsd-redacted_-_massage_redacted_r.pdf p. 27
[30] People in Alaska's Sex Trade: Their Lived Experiences And Policy Recommendations, p. 10
[31] Spotlight: Human Trafficking Intelligence and Leads | Thorn
[32] Traffic Jam — Marinus Analytics
[33] investigative-tools_redacted.pdf
[34] Marinus Analytics fights human trafficking using Amazon Rekognition | AWS Machine Learning Blog
[35] san-bernardino-county-sheriff-ht-basic-8-hour-part-1_redacted.pdf p. 76

to be the most complete records, they did not provide records for TrafficJam, which their training indicates that they use. Here's what we do know:

County	Database Invoices, Purchase Orders, etc.
San Bernardino	**21**
San Diego	**8**
Solano	**6**
Los Angeles	**5**
Kern	**4**
Ventura	**3**
Orange	**2**
Marin	**1**
Santa Barbara	**1**

Databases Used

- Cellebrite
- Callyo
- Axon
- Forensic Logic CopLink
- Eventide NexLog
- Vigilant Solutions
- CLEAR
- TransUnion Risk
- CopLink IBM i2
- PenLink
- CellHawk
- ARJIS
- AFR Engine
- TriTech
- Whooster

Automated License Plate Readers and Pole Cameras

Law enforcement presentations also reveal that police are encouraged to use mass surveillance devices in public spaces to investigate sex workers and their clients. Two in particular were named: Automated License Plate Readers (ALPRs) and pole cameras.

ALPRs are cameras that are designed to recognize and capture information about vehicles, including license plates, makes, models, and colors. The cameras upload that data, along with photos, GPS coordinates, and a time stamp, to searchable databases run by police, private companies, and, often, the vehicle repossession industry. These cameras can be attached to a fixed location like a street light, collecting data on all vehicles that pass. ALPRs can also be attached to patrol cars, so they can capture data as they drive around. ALPRs can be used in connection with motor vehicle databases to track vehicles and their drivers, and they can be set to let police know when a particular license plate number is seen. Pole cameras are video cameras usually mounted on a utility pole outside a particular location. They can be controlled remotely, allowing police to surveil an area in real time, 24/7. One presentation on investigative techniques[36] in human trafficking cases notes that ALPR is a tool used in a high-profile human trafficking investigation involving underage victims.

This technology isn't limited to child exploitation cases, though. In one presentation[37] on prosecuting lewd acts and loitering, attributed to the Los Angeles Police Department, the trainer discusses both ALPR and pole cameras as enforcement techniques.

[36] 09-investigative-methods.pdf p. 36
[37] lewd-act-loitering-pp.pdf

Los Angeles Police Department, "Lewd & Loitering,"[38] page 10

In the same slide, the trainers also suggest "letters to residence," presumably directed at clients. Although not explicitly referenced in the document, it's worth noting that in 2014, Los Angeles City Council forwarded a proposal[39] to allow police to use ALPRs to identify possible prostitution clients in order to send them "John Letters", i.e., shaming and mildly threatening letters letting people know they were seen in an area known for street prostitution. The Oakland Police Department has used the same techniques.[40]

The Sacramento Police Department, in a presentation about "Customers & Demand" goes into a little more depth about how ALPR technology would be

[38] lewd-act-loitering-pp.pdf p. 10
[39] LA City Council Considers Sending 'Dear John' Letters To Homes Of Men Who Solicit Prostitutes - CBS Los Angeles
[40] Oakland Residents Hope 'Dear John' Letters Help Curb Prostitution - CBS San Francisco

used in this context. One slide[41] talks about "john stings" ("john" being an epithet used by police to refer to sex workers' clients) and releasing mugshots of clients to the media and on the Internet, and notes that ALPRs should be placed "near the stroll" to identify these clients–and anyone who drives by. Pole cameras can serve a similar function; in a presentation on street prostitution from The Academy, pole cameras are also mentioned as an "enforcement option."[42]

What the Invoices Tell Us

As with the database invoices above, this list must be considered incomplete, as law enforcement agencies provided no records or incomplete records. Frequently, the only information received was that a type of automated license plate reader was used, without any indication as to the length or extent that it had been utilized. Here's what we do know:

County	ALPR Invoices, Purchase Orders, etc.
San Bernardino	7
Los Angeles	5
Ventura	4
Placer	2
Solano	2
Marin	1
Orange	1
San Diego	1
Shasta	1
Sonoma	1
Stanislaus	1
Riverside	1

ALPRs Used

- Vigilant Solutions
- Flock Safety Cameras

[41] 04-customers-demand.pdf
[42] street-prostitution-pp.pdf p. 33

- Rekor Watchman
- IntelliSite UiG

Traditional Digital and Body-Worn Cameras

In general, digital cameras are a common tool used by police in a wide variety of criminal investigations. For example, cameras are generally used to document crime scenes. This is also true for investigations targeting sex work. For example, in one presentation on "Investigative Methods and Tools,"[43] the Riverside County Sheriff's Department lists both video and still cameras as equipment that should be used in surveillance operations and stakeouts (along with water and a sun visor).

Riverside County Sheriff's Department, "Investigative Methods and Tools," page 4

The Riverside County Sheriff's Department (RCSD) instructs investigators to document the spaces where alleged sex workers operate. For example, in a presentation[44] about raiding massage parlors, police are instructed to keep an eye out for "items that typically don't belong inside the business, left out in the open," such as personal lubricant, and to photograph "all logs and receipts".[45]

In cases undertaken by vice and human trafficking units, police often treat the bodies of sex workers as crime scenes. For example, the aforementioned massage parlor presentation instructs

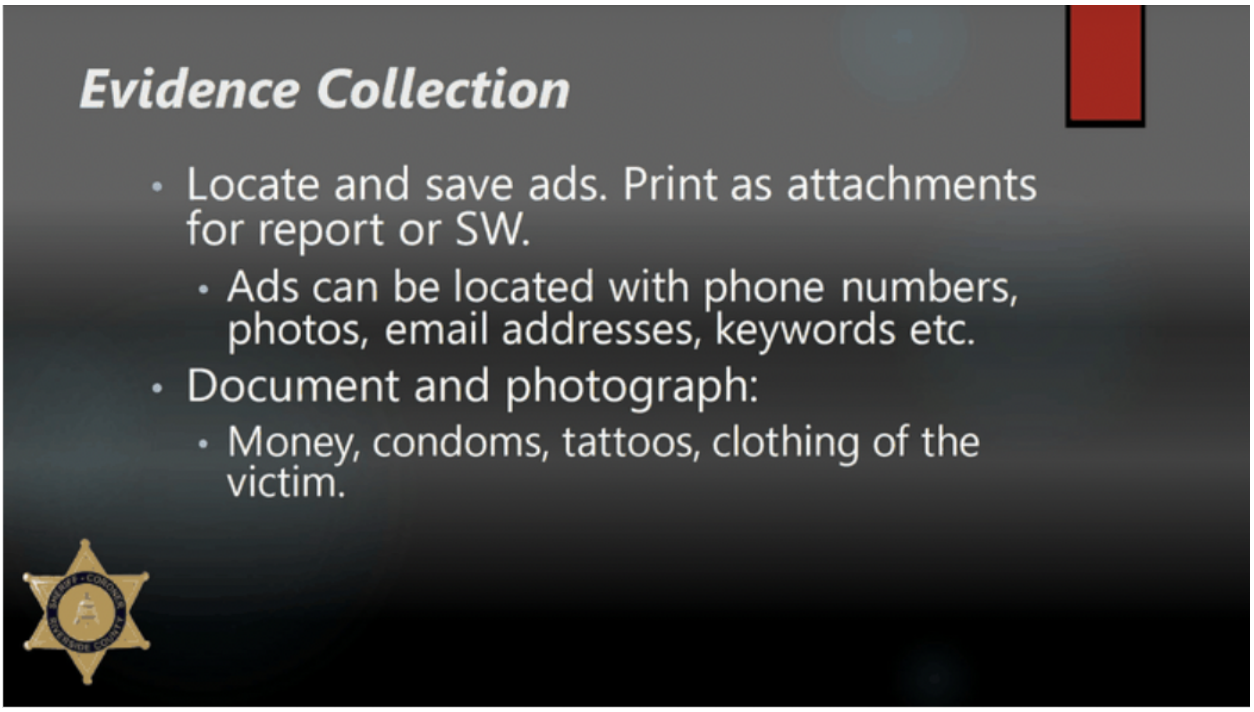
[43] Redacted Investigative Methods and Tools
[44] Rcsd-redacted_-_massage_redacted_r.pdf p. 48
[45] rcsd-redacted_-_massage_redacted_r.pdf p. 50

officers[46] that "employees dressed inappropriately" can be used as evidence in prosecutions, and it includes photos of handcuffed massage parlor workers in lacy shirts, tank tops and shorts.

Another presentation[47] on "Investigative Methods"[48] from The Academy instructs attendees to take a "clear photo" of the victim's face and a photo of the victim's clothing and "photos of all tattoos on the victim." Similar instruction is given for photographing the bodies of suspects. The inclusion of "all" implies officers include tattoos located on intimate parts of the body.

A San Francisco Police Department presentation[49] released by The Academy that instructs police how to manipulate sex workers and human trafficking victims devotes several slides[50] to the practice of collecting photos of tattoos, including using images of suspects being forced to open their shirts to expose their tattoos.

The RCSD also emphasizes the importance of documenting tattoos,[51] listing it behind "money" and "condoms" as important items to photograph on the first slide of its "Evidence Collection and Search Warrants" presentation.



Riverside County Sheriff's Department, "Evidence Collection and Search Warrants,"[52] page 2

[46] rcsd-redacted_-_massage_redacted_r.pdf p. 48
[47] 09-investigative-methods.pdf
[48] 09-investigative-methods.pdf p. 4
[49] 11-interviews.pdf
[50] 11-interviews.pdf p. 11
[51] rcsd-redacted_-_evidence_and_search_warrants_redacted.pdf
[52] rcsd-redacted_-_evidence_and_search_warrants_redacted.pdf

Faces and tattoos are forms of biometrics,[53] which are physical characteristics that are more or less unique to an individual, similar to fingerprints. Law enforcement agencies across the U.S. compile databases of faces and tattoos that they can use to identify individuals using automated recognition software. In 2019, the California legislature passed Assembly Bill 1215,[54] a three-year moratorium on using biometric identification algorithms on cameras carried by police officers. However, this law expired on January 1, 2023.

An open question remains: What do agencies do with face and bodily images captured by law enforcement? Are they stored in databases? Who is allowed to access them?

One thing we do know is that law enforcement will exploit these images in presentations for other officers.

For example, the Riverside County Sheriff's Department advises investigators to take photos of the tattoos of their subjects,[55] whether they are victims of human trafficking or women engaged in "street prostitution". RCSD included pictures of women's faces and unclothed chests[56]–an apparent disregard for the privacy and bodily autonomy of "victims".

These presentations do not address the trauma this intrusion may cause to "victims" or the threat presented to the dignity and human rights of subjects during the capture of their bodily information.

This lack of protection for privacy and bodily autonomy mirrors practices that have been documented in the field. In 2014, exotic dancers sued the San Diego Police Department,[57] following a raid where police forced the dancers to undress and pose in semi-nude state while officers photographed their tattoos. The dancers claimed that police made "arrogant and demanding comments"[58] while taking the photos.

TS Angela Marie, a sex worker who participated in ESPLER's survey about surveillance technologies, shared this story:

> In approximately 2009, I agreed to a text-only date with someone posing as a potential client. Sadly I was in truly terrible need of the income at the time, and I let down my standards and did this one thing which I have never done again since then (make a "text

[53] Biometrics | Electronic Frontier Foundation
[54] California Governor Signs AB 1215 | Electronic Frontier Foundation
[55] rcsd-redacted_-_evidence_and_search_warrants_redacted.pdf
[56] rcsd-redactions_-_commercial_sex_trafficking_redacted.pdf p. 6
[57] Strip Club Dancers File Lawsuit Against City, SDPD Chief – NBC 7 San Diego
[58] Strip Club Dancers File Lawsuit Against City, SDPD Chief – NBC 7 San Diego

only" date).... I was very suggestively dressed at that point, in a mini dress, stockings, heels, etc....

The gentleman arrived at my place (I have a nice, upscale apartment home in a good area) - and after greeting me and confirming that he was, in fact, there to see me from my local EROS ad posted in one of the nearby higher-end localities, he then pulled out a badge and police ID card, identified himself, but did not say I was under arrest.

I tried to find some type of excuse about being on a dating site, but he told me I needed to be honest with him and this would go a lot easier.

He told me to stay put and that he had to get some things from his car and would be right back...

He came back about a minute later, I never even sat down.... he had a folder and a camera, and told me he was going to register me as well as photograph me for the file he was carrying.

I tried every possible way to talk him out of doing anything that would endanger my income or my residence, but he was insistent that either I agree to be documented or be arrested. He wasn't mean but he was firm and matter of fact.

He had me stand in my hallway and take a full body and face shot…and then he had me sign official documents for the local police sex crimes division apparently, and gave me a stern warning as well as his legitimate official police business card.

It became very clear from the type of file he created and had me sign as well as taking my photo (almost like a mugshot) that a database was being/ had been built and maintained within the local police departments closest to me.

What the Invoices Tell Us

County	Camera Invoices, Purchase Orders, etc.
Los Angeles	**9**
Merced	**9**
Solano	**7**
Orange	**6**

San Diego	**6**
San Joaquin	**4**
Humboldt	**3**
Kern	**3**
Placer	**3**
Riverside	**3**
San Bernardino	**3**
Santa Barbara	**3**
Amador	**2**
Calaveras	**2**
Contra Costa	**2**
Stanislaus	**2**
Ventura	**2**
Alameda	**1**
Kings	**1**
Lake	**1**
Marin	**1**
San Mateo	**1**

Digital Cameras Used

- Axon Body Worn
- Watchguard
- Hanwha
- Hikvision
- Weldex Dome
- Body Worn Motorola G7
- Canon Digital Cameras
- Milestone XProtect
- Lenslock
- Genetec

- StarWitness Field Interviewer
- Olympus Tough
- SafeFleet
- Arlo Wireless
- CML Security

Device Searches, AKA Phone Ripping

California police departments report copying the entire phones of sex workers and sex work clients detained during prostitution stings. What incredible circumstances would give the government the right to copy a person's whole phone: pictures, location data, credit card information, fitness journal, phone numbers, text and messenger conversations, social media accounts, and more? These searches are so invasive that one law enforcement officer called the technology a "window to the soul".[59]

In *California v Riley* the United States Supreme Court decided that police do not have the right to search cell phones of people they arrest without a warrant. Without a warrant or the justification to get one, police coerce sex workers, sex trafficking survivors, and clients into consenting to their phones being copied by threatening to keep their phones.

> the sex buyer that he was in the area of location #1. I then instructed the sex buyer to the hotel where the operation took place and instructed him to advise when he arrived. Moments later, the sex buyer stated he arrived at the hotel and he was then provided with the room number. After a short time, Detectives who were working surveillance observed the sex buyer approach the decoy room. Once the sex buyer knocked on the door, the arrest team contacted the suspect and placed him under arrest without incident. Once in the hotel room, the suspect was identified as [redacted] and the phone number which the undercover Detectives communicated with was matched to [redacted] cellular phone, which was located in his right back pant pocket at the time a search of his person incident to arrest was conducted. $80 was also located within [redacted] right front pant pocket along with a Durex condom, which were ultimately seized as evidence. [redacted] consented in having his cellular phone imaged by SBSO Detectives and signed a consent form to do so. Upon completion of the cellular phone imaging process, [redacted] was issued a citation for the violation of PC 647(b)(1) - Solicitation of Prostitution and released on scene.

[59] Mass Extraction | Upturn

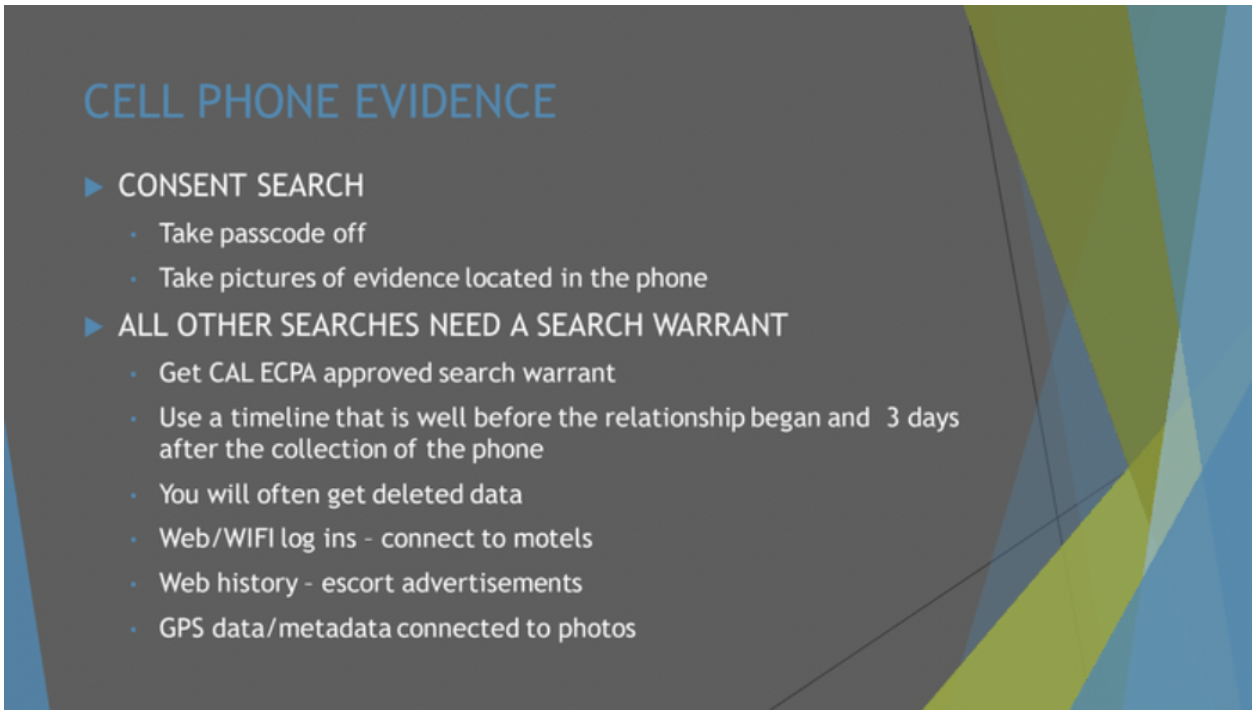
This client consented to having his phone searched and was allowed to leave with it. In this case a condom, used to prevent the spread of infections and protect public health, is used as evidence in violation of Section 782.1 of California's Evidence Code.

If a sex worker, sex trafficking survivor, or client doesn't consent to having their phone copied, police place it in a faraday bag so that it can't be remote wiped and keep it. Based on reports from our community members, it seems that many of these phones are never searched by police.

A device rip (the term "search" is misleading, since they're actually copying the data from the phones) involves accessing, browsing, and extracting[60] information and metadata (like times and locations associated with certain on-device actions) from an individual's electronic device, such as a cell phone or a laptop. Law enforcement has the ability, through mobile device forensic tools (MDFT), to create a full copy of the data on a device, including emails, messages, photos, and location information (Upturn[61] has a report on this use). The California Electronic Communications Privacy Act[62] generally requires law enforcement to use a warrant to search devices. For this reason, law enforcement may ask or coerce an individual to consent to search or access of a device in order to bypass this requirement. San Bernardino County Sheriff's Department, in a slidedeck[63] for a human trafficking basic training presentation, highlights that the consent search is the only type of search that doesn't need a search warrant.

> We're talking here of the violence inherent in a system: not only direct physical violence, but also the more subtle forms of coercion that sustain relations of domination and exploitation, including the threat of violence.
> Zizek, *Violence*

[60] A Technical Look At Phone Extraction
[61] Upturn: Mass Extraction
[62] https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201520160SB178
[63] san-bernardino-county-sheriff-ht-basic-8-hour-part-1_redacted.pdf p. 81

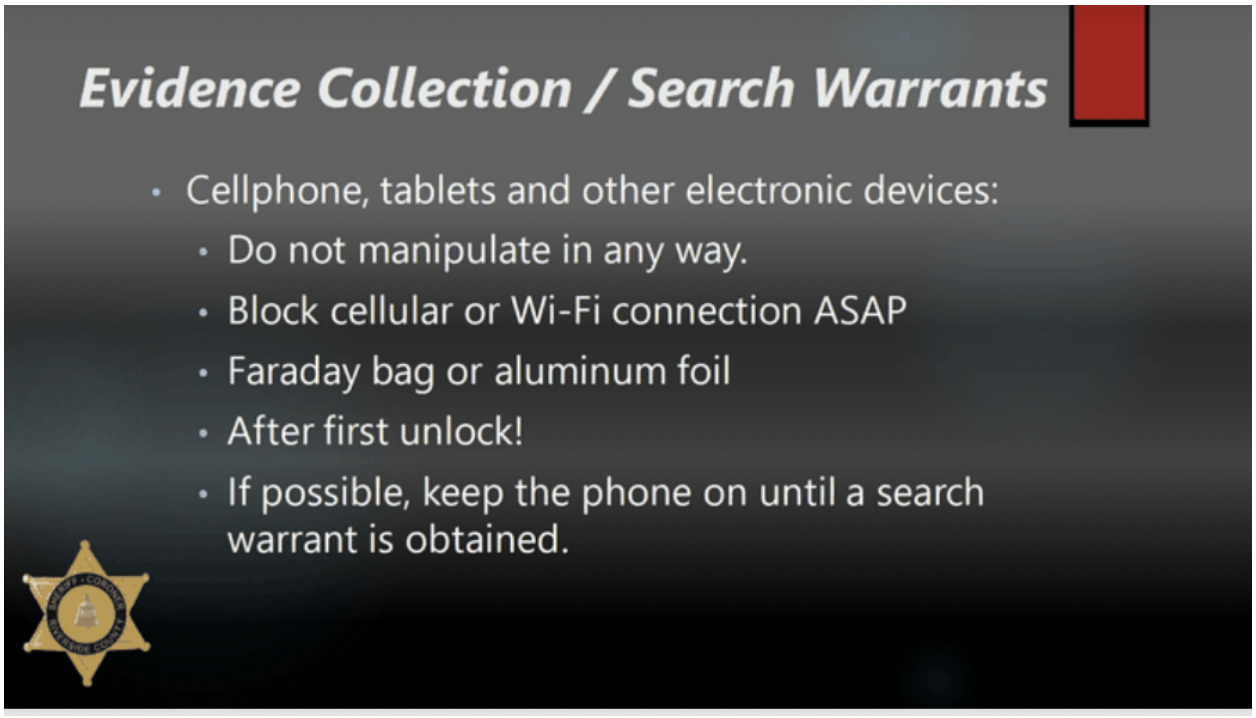


San Bernardino County Sheriff's Office, "Human Trafficking Investigations,"[64] page 81

Through other collection methods, however, some or all of a device's data may still be accessed by law enforcement. These include via cell phone service providers, social media sites, and IP providers, as well as the use of call detail record (CDR) software like CellHawk,[65] paid services like Callyo, and device extraction tools.

In Oakland, law enforcement has utilized the Cellebrite UFED (Universal Forensics Extraction Device) to conduct "phone ripping," the extraction and analysis of data pulled from an individual's cell phone. Training documents[66] from the Oakland Police Department claim that the technique can be used by an investigator to "retrieve data stored on cell phones," including phone calls, text messages, and photos, which can later be "reviewed when needed by investigator[s] and may prevent having to retain a victim's personal cell phone for an extended period".

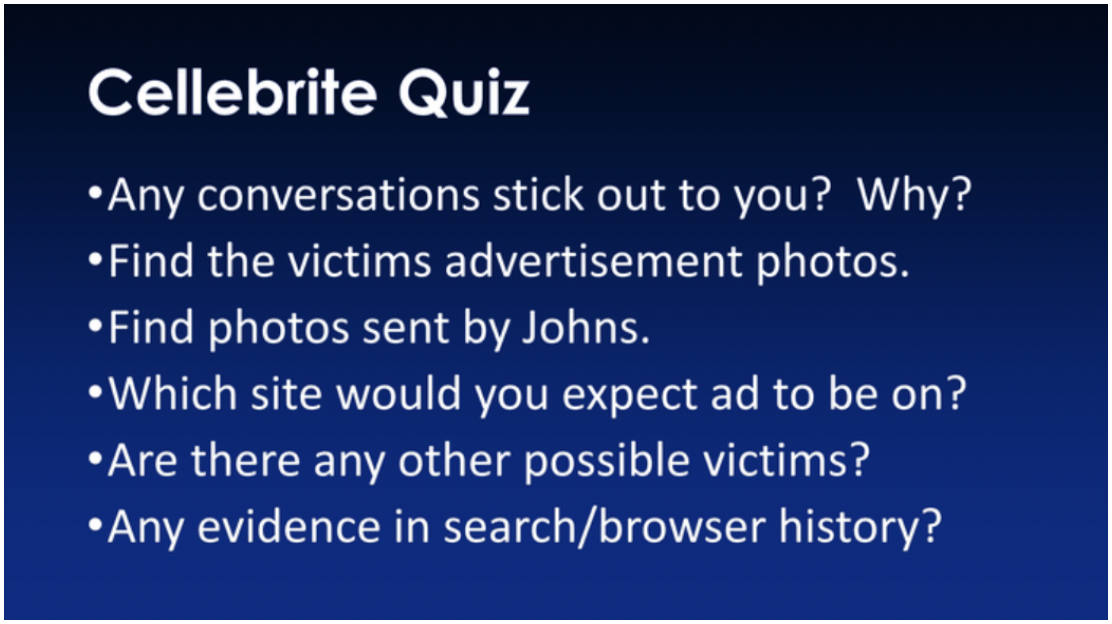
[64] San-bernardino-county-sheriff-ht-basic-8-hour-part-1_redacted.pdf p. 81
[65] investigative-tools_redacted.pdf
[66] undercover-expanded-course-outline-r7apr14-10-and-11.pdf p. 7



Riverside County Sheriff's Department, "Evidence Collection and Search Warrants,"[67] *page 13*

The Vacaville Police Department also has included a hands-on workshop on the use of the Cellbrite Reader tool[68] as part of its 40-hour sex trafficking investigation training. Materials from the department[69] suggest that they use it to extract current, and sometimes deleted, data from the phone, including photos, searching browser histories, and monitoring conversations. The tool can also be used to extract information like the advertising ID associated with apps on the device, which can then be used to access information and location via other means.

[67] Redacted - Evidence and Search Warrants
[68] P.O.S.T. Course Online
[69] Day 3 Morning Redacted



Vacaville Police Department, "Day 3 Morning_Redacted,"[70] page 8

A presentation[71] from the San Francisco Police Department discusses the pros and cons of seizing a human trafficking victim's cell phone. One on hand, the presenter says that these personal devices have the "best evidence" but that the phone may be the victim's only way to communicate.

What the Invoices Tell Us

County	Phone Ripping Invoices, Purchase Orders, etc.
Solano	**4**
Ventura	**2**
Marin	**1**
Santa Clara	**1**

Phone Ripping Devices Used

- Cellebrite
- GrayKey

[70] day-3-morning_redacted.pdf
[71] 11-interviews.pdf

Undercover Operations Online

Law enforcement regularly uses online spaces and profiles to gather information on individuals.

Social media platforms[72] like Facebook and Instagram host publicly available information that is gathered by police, but training slides also discuss creating accounts in order to further interact with and observe people. For officers at San Bernardino County Sheriff's Department,[73] the use of undercover social media profiles is considered a top type of "field investigation."

One technique discussed[74] in training materials[75] is the act of "friending" people in order to learn more about them and to determine others with whom they associate. "Most," the slide says, "don't have a strenuous vetting out process." Officers are encouraged to use anonymous email services and to use a new email for each fake profile they create.

Vacaville Police Department has an entire presentation[76] about setting up a fake profile, which outlines steps like creating a usable photo bank based on photos from sting operations, search phrases to use on Tumblr to find ideal pictures of sex workers to use without permission, and setting up a new Google account before creating fake Facebook and Tumblr accounts. The training emphasizes the need to make a profile appear convincing by regularly adding memes and other content, and it stresses the utility of having an undercover officer with "Mad Selfie Skills". A Texas lawsuit filed by three female police officers in 2021 [77] alleged sexual misconduct by their male supervisors during prostitution stings, saying that "prostitution stings soon grew into a booze-fueled playground for sexual exploitation in which young, untrained deputies were subject to disgusting abuse".

[72] Redacted - Investigative Methods and Tools
[73] Redacted - Sheriff Human Trafficking 8 Hour Training
[74] ICI Human Trafficking Investigations - Digital Evidence
[75] ICI Human Trafficking Investigations - Digital Evidence
[76] Day 3 Afternoon Redacted
[77] Current and former Texas constable's deputies file lawsuit alleging abuse from commanding officers

Vacaville Police Department, "Let's Make A UC Profile,"[78] *page 3*

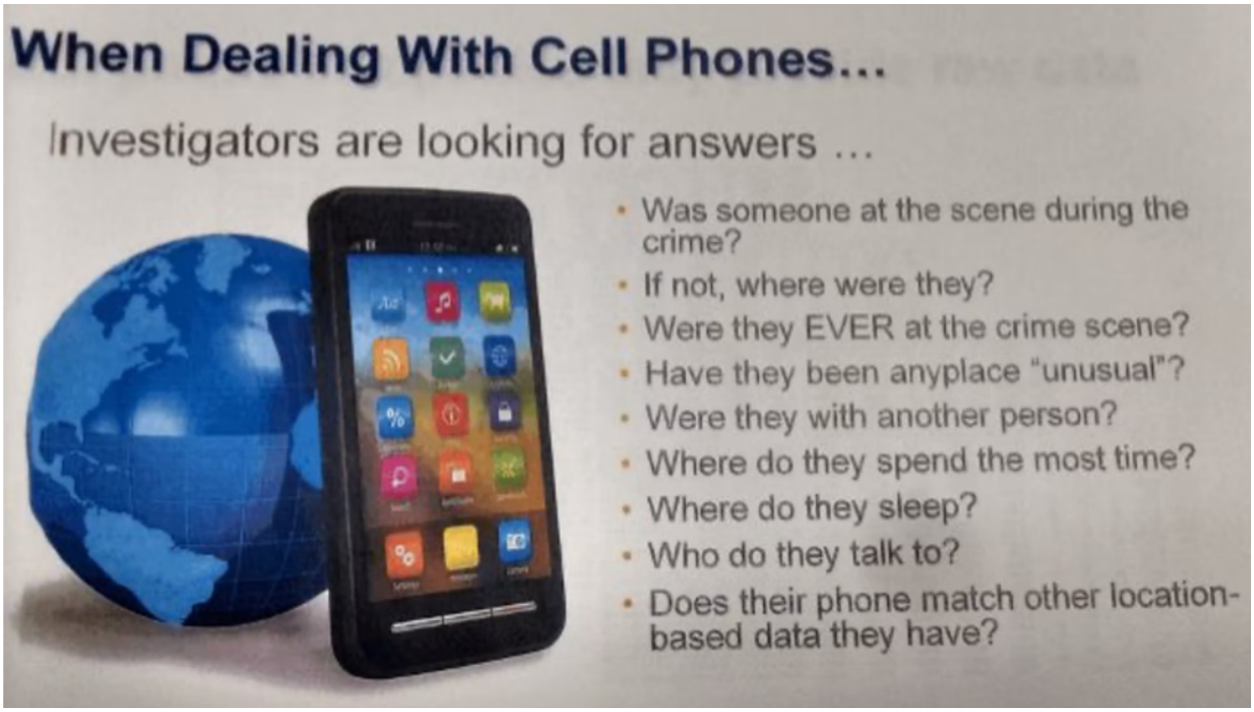
San Jose Police Department encourages undercover officers[79] to engage with suspects like pimps and those who may be paying for sex acts via the chat function on social media or on a dating website like Plenty of Fish and Grindr.

Law enforcement also uses programs like Callyo[80] to anonymously call individuals on phone numbers they have gathered online and from ads. Vacaville's training even includes a period to practice[81] calling phone numbers associated with ads.

Spotlight: CellHawk

CellHawk is a software service offered by Hawk Analytics[82] that allows law enforcement officers to quickly analyze vast amounts of data collected by cell phone towers. CellHawk analyzes huge data dumps from towers, which include GPS location and ridesharing data. It can animate the movements of over 20 phones at once to show how they move in relation to each other.

[78] day-3-afternoon_redacted.pdf
[79] San-jose-police-department-attachment_1-_human_trafficking_docs_redacted.pdf p.19
[80] investigative-tools_redacted.pdf
[81] 2670_21519_outline.pdf p. 3
[82] Hawk Analytics



Screenshot of CellHawk marketing.

CellHawk offers the capability to receive notifications when suspects go to a location or enter an area. It can show when, how often, and from what locations a person called or texted another person.

It isn't clear from CellHawk's promotional presentation whether it only has access to cell tower data gained by a law enforcement agency through a warrant, or whether it has access to this information all of the time. We asked a professor of criminal justice to help us understand: While he was not familiar with CellHawk, he explained that police do not need warrants to look at cell tower data. Once our phones are connected to a public cell tower, we have no legal expectation of privacy.[83] Warrants are needed in most jurisdictions for police to see our live location data.

But Does the Technology Rescue the Children?

ESPLER reviewed charging documents in all federal cases of sex trafficking filed in California between January 2020 and February, 2022. Of 18 cases of trafficking of a minor, two were discovered with the use of Spotlight or TrafficJam–but not by police. In both cases, the National Center for Missing and Exploited Children forwarded advertisements featuring missing youth to the police. Four times as many cases–eight in total–came to light when a victim or family member of a victim initiated a police report, and one when a victim called her trafficker from the

[83] Ping! The Admissibility of Cellular Records to Track Criminal Defendants, *Saint Louis University Public Law Review*

juvenile detention center. This indicates that while databases like Spotlight and TrafficJam can be used to rescue children, they are not used in this way by police. Instead, victims are most commonly discovered through their own reports.

Cases charged under California's pimping and pandering of minors laws were similar: Although we made requests of every district attorney in California, only eight responded, providing a total of 30 cases. Of those, 16 were from Fresno County, and 11 were dismissed or found not guilty. An additional three cases did not seem to involve minors. For 24 of the cases (including the 11 that were dismissed or found not guilty) we could find no case information. Of the remaining six cases, each minor was found due to a report by the victim, victim's family member, or group home staff. None were found through the use of surveillance technology.

How Surveillance Technologies in Commercial Sex Cases are Used to Violate the Fourth Amendment and CalECPA

Cell phones contain a huge amount of personal information. As our collective dependence on them has increased, so has California's and the federal government's response to protecting the information contained in a phone or stored by the cell phone provider. California prohibits any government agency, including law enforcement, from interacting with a citizen's cell phone (or any other electronic device), and prescribes what actions law enforcement must undertake to legally gain private citizens' data from the corporations that collect it.

Under the law, protections for the physical cell phone are different from the protections for the data it stores. For example, if a picture is taken on a cell phone, it isn't considered an electronic communication until it is sent out of the device. Data collected by any third-party entity (like social media and cell phone companies) falls under a different legal protection than cell phones and electronically communicated data.

In surveilling sex workers, police officers will typically directly search the content located on a seized device. An officer will open and scroll through the device, using their own camera to take pictures of content as it is displayed on the screen. Police officers also use proprietary technology (e.g., Cellebrite Technologies) to download and review the entire data content of a device. In some cases, law enforcement uses a warrant to obtain electronic data from third-party service providers.

In the next few pages, we'll unpack which (if any) of these routine law enforcement practices are permitted under the law.

California's Electronic Communications Privacy Act (CalECPA)

To protect private electronic communication (data), California passed CalECPA pursuant to Penal Code section 1546. CalECPA prohibits any government agency, including law enforcement, from forcing production or access to data and devices from either private citizens or their service providers–with some exceptions. The statute makes different exceptions for obtaining data from a private citizen versus from a device.

Law enforcement can only force a service provider or a private citizen to give access to data if[84] they have:

1) A warrant pursuant to Penal Code section 1523
2) A wiretap pursuant to Penal Code section 629.50
3) An electronic reader order pursuant to Civil Code Section 1798.90
4) A Pen Register or Trap device pursuant to Penal code Section 630

Law enforcement can only interact with a device to gain data if they have:

1) A warrant pursuant to Penal Code section 1523.
2) A wiretap pursuant to Penal Code section 629.50.
3) A tracking device search warrant Penal Code section 1523.
4) Specific consent from a person who is authorized to possess the device.
5) Specific consent of the owner, only if it has been reported as lost or stolen.
6) If law enforcement believes, in good faith, that an emergency involving danger of death or serious physical injury to any person requires access to the electronic information.
7) If law enforcement believes, in good faith, the device is lost, stolen, or abandoned, they may access the device to identify/verify/contact the owner.
8) If the device is seized from an inmate's possession in a correctional facility OR if the device is found in a correctional facility where inmates have access and it is not otherwise possessed by another non inmate individual or known to belong to a visitor.
9) If the device is seized from anyone on parole or post release community supervision.
10) If the device is seized from anyone on probation, mandatory supervision, or pre-trial release and the person is subject to an unambiguous electronic device search condition.
11) Law enforcement access location and telephone number information to respond to an emergency 911 call from that device.
12) A Pen Register or Trap device pursuant to Penal code Section 630.

[84] There is an exception not listed but it does not pertain to law enforcement investigations or prosecutions of criminal offenses. (Penal Code section 1546.1(b)(4))

Electronic communication information–data–is critical evidence in investigating and prosecuting violations of Penal Code 236.1 (human trafficking). Electronic evidence found on a cell phone often includes, but is not limited to: access to social media accounts, email accounts, usernames, passwords, photos, photos that match online escort services advertisements, receipts of payment for online escort services advertisements, text and other instant messages reflecting negotiations for commercial sex acts, applications to transfer money between individuals, location data history, history of Internet searches, banking information, or phone numbers of other alleged victims or other suspects. Such "cell phone" evidence is critical in being able to learn about other data service providers for further warrants. It is also necessary to prove the crime in the event that the alleged victim does not want to participate in prosecution.

Coerced Consent to Search a Device is Not Consent

When law enforcement detains people involved in commercial sex work, they often characterize the person as a victim of trafficking. This is complicated by the criminalization of sex work; detained sex workers sometimes claim victimhood to avoid being criminalized for engaging in commercial sex acts. Law enforcement routinely seek to locate, seize, and search any electronic devices found in the sex worker's possession for the purpose of investigating charges of 236.1, or pimping or pandering (trafficking). Once a device is located, police officers routinely attempt to coerce consent.

In order to establish the validity of a consent to search, the government must demonstrate that the consent was freely and voluntarily given, and "not a mere submission to an expressed or implied assertion of authority."[85] The validity of consent is based on the full context of the circumstances.[86]

Police routinely detain and threaten to arrest sex workers for engaging in commercial sex acts unless the person detained consents to a search of their phone. Under the law, this would be considered involuntary consent. Further, the arrest itself is unlawful if the police believe the person is a victim of trafficking. Consent following unlawful detention, entry, or arrest are invalid.[87]

Police also routinely threaten to seize the devices of people they detain–unless a person consents to a search of their phone. This alone will not invalidate consent, but would add to the coercive nature of the consent. This context would be considered among other circumstances like the maturity and emotional condition of the person whose consent is being sought–especially if

[85] Florida v. Royer (1983) 460 U.S. 491, 497; People v. James (1977) 19 Cal. 3d 99, 106; Bumper v. North Carolina (1968) 391 U.S. 543.
[86] Schneckloth v. Bustamonte (1973) 412 U.S. 218, 219.
[87] Wilson v. Superior Court (1983) 34 Cal. 3d. 777, 791, People v. James, supra.

access to the phone is necessary for the person's ability to obtain money, food, housing, and transportation.[88]

CalECPA Protections Extend to Electronic Devices Seized By Law Enforcement

If consent to search a phone is not provided, and an officer chooses to seize the phone, they typically put the phone in airplane mode, or power it off, and store it in a Faraday bag.[89] Some officers will access the serial number and or telephone number of the device. It is commonplace that law enforcement seeks to obtain a warrant only after these steps are taken.

Despite this common police practice, there is no 'seize and search later' exception to CalECPA. The statute says, "… a government entity shall not do any of the following… Access electronic device information by means of physical interaction or electronic communication with the electronic device."

In this commonplace practice, however, law enforcement has physically interacted with the device:

- By seizing the phone
- By placing the phone in airport mode
- By powering the phone off
- By placing the phone in a Faraday bag
- Manipulating the phone to access the serial number

There is no exception which allows law enforcement to physically interact with the device before obtaining a warrant. Rather, CalECPA requires that a warrant must be secured in order to physically interact with the device.

CalECPA Protections Extend to Data Obtained Via a Search Warrant

CalECPA's warrant exception still provides significant protections for private citizens when law enforcement executes a warrant pursuant to Penal Code section 1523. Law enforcement must notify the target of the warrant.

Under CalECPA, a warrant to obtain cell phone data must "describe with particularity the information to be seized by specifying . . . the time periods covered, the target's person or accounts, the applications or services covered, and the types of information sought…"

---

[88] Schneckloth v. Bustamonte, supra.
[89] Faraday bags are a type of Faraday cage made of flexible metallic fabric. They are typically used to block remote wiping or alteration of wireless devices recovered in criminal investigations.

Further, CalECPA requires law enforcement to notify the suspect/defendant/target of the warrant. This notice requirement must state the nature of the investigation and provide a copy of the warrant, and be done at the same time that the warrant is executed:

"(a)(1) Except as otherwise provided in this section, any government entity that executes a warrant ... shall serve upon, or deliver to by registered or first-class mail, electronic mail, or other means reasonably calculated to be effective, the identified targets of the warrant ... a notice that informs the recipient that information about the recipient has been compelled or obtained, and states with reasonable specificity the nature of the government investigation under which the information is sought. The notice shall include a copy of the warrant ... The notice shall be provided contemporaneously with the execution of a warrant…"

A court can issue an order delaying notification for 90 days based on a sworn affidavit that notifying the suspect would have any of the following "adverse results":

(1) Danger to the life or physical safety of an individual.
(2) Flight from prosecution.
(3) Destruction of or tampering with evidence.
(4) Intimidation of potential witnesses.
(5) Serious jeopardy to an investigation or undue delay of a trial.

However, this exception isn't a catch-all that allows for any delay. The sworn affidavit must include compelling facts with which a Court can determine whether delayed notification is appropriate. Claims that a suspect may be a flight danger (or etc.) based on mere speculation is not sufficient.

CalECPA provides even more limitations for delayed notice, saying that it is "… only for the period of time that the court finds there is reason to believe that the notification may have that adverse result, and not to exceed 90 days."

Under CalECPA, law enforcement must not review or disclose any information that is unrelated to the objective of the warrant. The statute says:

"The warrant shall require that any information obtained through the execution of the warrant that is unrelated to the objective of the warrant shall be sealed and shall not be subject to further review, use ... A court shall issue such an order upon a finding that there is probable cause to believe that the information is relevant to an active investigation, or review, use, or disclosure is required by state or federal law."

When law enforcement obtains a warrant to search a cell phone based on this statute, the warrant must specify the dates or timeframe of the data sought. This requirement is at odds with the commonplace practice of police searching a phone they have seized or downloading the contents of using Cellebrite technology; there is no time frame limitation to such a search. They can literally view anything on the phone.

Case example: During the preliminary hearing of a trafficking prosecution (236.1, pimping/pandering), a detective testified that she reviewed messages on the co-defendant's seized cell phone, which the detective had searched after obtaining a warrant. These messages reflected the co-defendant had been slapped by the defendant. The prosecutor sought to introduce this evidence to prove the defendant had trafficked the co-defendant. However, the messages were written well before the timeframe approved by the warrant. The magistrate sustained defense counsel's objection to the introduction of the evidence. However, the detective then sought a subsequent search warrant to include the timeframe of the messages she already knew existed.

This example illustrates one way law enforcement routinely violates CalECPA. The only reason the detective knew this evidence existed is because of an unlawful search (reviewing messages on a phone outside the scope of the original warrant); she then failed to disclose her violation of CalECPA in seeking a subsequent warrant.

Misusing the 'Emergency' Exception to Obtain Real Time GPS Location Data

CalECPA's exceptions can be different depending on the actions of law enforcement. The law offers more exceptions if police are getting data directly from the device. Exceptions allowing police to compel a private citizen or service provider to release data is significantly more limited.

As we observed in police training materials, law enforcement routinely scrolls online advertisements looking for persons they believe are involved in sex work, which they often characterize as victims of trafficking. Online advertisements often provide cell phone numbers. Using surveillance technology, law enforcement can easily obtain real time location data/GPS information for that cell phone directly from the cell phone service provider. To duck the warrant requirement, law enforcement may claim an "emergency involving danger of death or serious physical injury." However, this "emergency" exception does not exist when obtaining data from a cell phone provider; it only exists when law enforcement obtains data from a device.

Case example: Law enforcement officers conflated trafficking with sex work in an investigation (236.1, pimping/pandering) of a "victim" they believed was performing commercial sex acts in a particular area. The investigating officers based this investigation on an online advertisement indicative of prostitution involving the alleged victim. From that advertisement, they obtained a cell phone number and used it to locate the alleged victim. They called the cell phone provider to

obtain real time GPS location information, claiming the alleged victim was "kidnapped." From that GPS information, the officers located the alleged victim at a hotel, where they went to make observations while surveilling from the parking lot. After this in-person surveillance, they were able to schedule a "date" with the alleged victim. In their subsequent police report, the officers failed to disclose that they sought and obtained GPS data from the cell service provider. Instead, they reported locating the alleged victim through the scheduled "date." This is another classic example of how law enforcement routinely violates CalECPA. They obtained private data from a service provider, without a warrant and no "emergency" exception applied.

CalECPA Protections Extend Even for Emergency Situations

Even under the 'emergency' exception that allows for law enforcement to access data from a cell phone, CalECPA still imposes significant protections to prevent abuse of this exception by law enforcement.

First, the claimed emergency is not just that a crime is being committed, even trafficking (236.1, pimping/pandering). CalECPA requires a "good faith belief" that "death or serious bodily injury[90]" would occur.

Second, there are strict timelines for what law enforcement must do after it obtains data under this exception. Within three court days, law enforcement must file an application or warrant. This application must provide evidence that death or serious bodily injury would occur without the exception. The court must rule promptly about whether it agrees.

Third, if the target of the data's access was not notified, the application must also include a sworn affidavit requesting the delay based on one or more of the "adverse results" reasons explained above.

Fourth, if the court determines the facts did not give rise to a good faith belief in death or serious bodily injury, or rejects the warrant or order application on any other ground, then the court must order the destruction of the data obtained and notify the target immediately.

In the case example above, law enforcement claimed "possible kidnapping" to obtain data from the cell service provider. Kidnapping is not evidence of "serious bodily injury" or death. Law enforcement did not file a subsequent motion with the court, much less in three days, documenting that they obtained data this way. Law enforcement did not notify the target of the investigation nor seek an order delaying the required notice.

[90] Serious bodily injury is defined in California criminal law as "a serious impairment of physical condition, including, but not limited to, the following: loss of consciousness; concussion; *bone fracture;* protracted loss or impairment of function of any bodily member or organ; a wound requiring extensive suturing; and serious disfigurement." (§ 243, subd. (f)(4), italics added.)

CalECPA: In Summary

CalECPA consumer privacy protections are powerful, but so are the technology surveillance tools that law enforcement routinely uses to circumvent these legal protections, violate consumer privacy, gain access to data illegally, and prosecute people using evidence they broke the law to obtain.

Condoms as Evidence

Section 782.1 of California's Evidence Code instructs police and prosecutors that condoms are not to be used as evidence in prostitution cases. However, 67% of the reports provided to us by police departments after Section 782.1 came into effect reported seizing condoms as evidence.

arrived. Moments later, the sex buyer stated he arrived at the hotel and he was then provided with the room number. After a short time, Detectives who were working surveillance observed the sex buyer approach the decoy room. Once the sex buyer knocked on the door, the arrest team contacted the suspect and placed him under arrest without incident. Once in the hotel room, the suspect was identified as [redacted] and the phone number which the undercover Detectives communicated with was matched to [redacted] cellular phone, which was located in his right front pant pocket at the time a search of his person incident to arrest was conducted. $60 was also located within [redacted] left front pant pocket along with a Trojan condom, which were ultimately seized as evidence. [redacted] consented in having his cellular phone imaged by SBSO Detectives and signed a consent form to do so. Upon completion of the cellular phone imaging process, [redacted] was issued a citation for the violation of PC 647(b)(1) - Solicitation of Prostitution and released on scene.

The criminalization of condoms is an extreme public health hazard for street-based sex workers, who fear carrying condoms will cause them to be arrested, and broadly undermines the public health of Californians. For 67% of law enforcement to fail to uphold this important law that protects the health of sex workers and sex trafficking survivors makes it hard to believe the narrative that police only arrest us because they care about us.

Conflating Sex Work, Sex Trafficking, and National Security for More Surveillance: Government Doublethink

As a criminalized activity, prostitution is classified as a misdemeanor. A misdemeanor shouldn't be a high priority for police departments. In most states, police are not allowed to make an arrest for a misdemeanor without a warrant unless they witnessed it themselves.

This means that police shouldn't waste valuable time on the taxpayer dime to technologically surveil, investigate, prosecute, arrest, and house sex workers in overcrowded public jails. A misdemeanor charge is not meant to ruin a life, but these arrests create a permanent record for, disproportionately, low-income queer women of color who, thereafter, face ongoing discrimination in housing, employment, child custody, and banking.

HSI Phoenix assists in multi-agency operation, 18 men arrested on prostitution and other charges

*Attempted Sex Conduct with a Minor; Child Prostitution with a Minor under 15; Money Laundering; Prostitution

MESA, Ariz. — Special agents with U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) joined the East Valley Human Trafficking Taskforce (EVHTTF) on a two-day "Buyer Reduction" or sting operation, which resulted in 18 arrests.

However, through the purposeful and ongoing conflation of sex trafficking and prostitution, prostitution has become a matter of national security. Government officials have used this conflation to justify the expansion of surveillance technology and the use of law enforcement time and funds–even Department of Homeland Security time and funds–on prostitution charges. Prostitution stings are now carried out by DHS on a regular basis under the guise of "national security" to combat "human trafficking", with no accountability mechanisms to ensure that traffickers and not sex workers and our clients are actually targeted.

This level of conflation is the result of decades of work by the anti-prostitution lobby. In 2000, the federal Violence Against Women Act introduced a new definition, not of sex trafficking, but of a victim of sex trafficking. It said that a minor who was engaged in the commercial sex industry was a sex trafficking victim, even if no one had trafficked them. It went even further to say that a minor who traded sex to meet survival needs–like housing, food, or clothes–was a sex trafficking victim. Suddenly, youth shelters weren't just dealing with "bad kids," they were rescuing sex trafficking victims. New research showed that almost all homeless and runaway youth had been sex trafficked![91]

[91] Are 30% of Anchorage's homeless youth being sex trafficked.pdf.pdf

> They perpetuate a constructed class – 'prostitute' – which justifies their actions.
> -Augustin

At the same time, there was a push nationwide to redefine clients of sex workers as sex traffickers. In 2015, the federal Justice for Victims of Trafficking Act expanded the criminal definition of sex trafficking even further, to include those who produce child pornography and clients who agree to pay for sex with a minor. Stings ensued where federal agents pimped out fictitious minors online and charged men who responded to their ads, whether out of concern or with sinister intentions, with sex trafficking. These sting operations would result in news articles declaring that dozens of sex traffickers had been caught.

Nonprofits have also used the conflation of sex work and trafficking to represent themselves as anti-human trafficking organizations, regardless of their provisions to actual trafficking victims. Self-identifying as an anti-human trafficking organization can increase access to government funds and bolster community impact assessments and social capital. Forcing victim labels onto sex workers can make an organization look as though it serves many sex trafficking victims, while actually falsely inflating the numbers that the federal government later uses to justify its own spending on law enforcement and surveillance.

The engagement with this harmful and inaccurate conflation by civil society members reinforces government surveillance and increases policing of marginalized communities–including the massive investment in illegal technological surveillance and privacy infringements of people in and adjacent to the sex trades by law enforcement, for-profit business, and nonprofits seeking anti-trafficking funds.

These methods of falsely inflating the perceived amount of sex trafficking in the United States are used to create an increasing sense of moral and humanitarian crisis. This manufactured wave of crisis is used to justify bad laws and civil rights violations. It distracts from the tragic realities of actual human trafficking and the wanton abuse of sex workers by the state.

> I want an explanation for, how much violence against "prostitutes" have we made acceptable? The police run-ins, the police denying help, the police abuse—all this shapes the context in which the sting, and the video of it, form a complete pursuit of what we are to understand as justice, which in this case is limited to some form of punishment, of acceptable violence.
> - Grant, *Playing the Whore*

Using human trafficking narratives to justify increased surveillance and policing has impacted not only advocates for sex workers but labor rights activists at large. Funding for agencies that hold corporations and employers accountable for worker treatment (like the Department of Labor) is dwindling, and as these protections recede, corporations have justified

increasing harmful surveillance of their own workers through the lens of human trafficking identification.[92] Even technology intended for workers to report abuses themselves has raised concerns about repercussions for workers, workplace safety, and violations by corporations through large-scale data collections.[93]

Despite these issues, advances in technology are often presented as steps forward by the anti-trafficking movement, rather than expressing concern at increased opportunities for the state and for corporations to use data to target and further oppress marginalized communities.[94]

After the events of September 11th, government-generated reports identified that lack of communication between law enforcement agencies, and lack of identification of those who engage in "non-criminal suspicious activity" was a data gap that needed to be addressed. In response, the Suspicious Activity Reporting Initiative was developed. Each U.S. state now has its own Fusion Center that serves as a clearinghouse for reports about "observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity." Since prostitution is now a matter of national security, we wondered if sex workers and our clients were in this national database. In response to our records request, we were told that there were thousands of records containing the sex work related words we'd requested. Since our request, the California State Threat Assessment Center has invoked two extensions and now says that it will give us some of the requested data on the date that the report you are reading is scheduled for release.

Wolves in Sheepdog Clothing: The Stanislaus DA is Very Worried about What the Cops do to Vulnerable Women

In 2010, Sacramento Deputy Eric Cephus[95] was off duty working as a security officer when he came into contact with two runaway girls, aged 12 and 13. He brought the 12-year-old to CPS but took the 13-year-old to a hotel where he offered her a place to stay and clothes in exchange for sex. In 2009, Dallas Vice Officer Jose Luis Bedoy[96] met "Victim 1" during a strip club raid. He began a relationship with her and, for five years,

> How, exactly, is someone who is most used to having the police threaten them, or demand sex with them in exchange for not being arrested, then supposed to trust the police in any way, let alone to connect them to services which are already freely available? When we construct help in this way we use the same eye with which we build and fill prisons. This isn't compassion. This isn't charity. This is control.
> - Grant, *Playing The Whore*

[92] Outlays of the US Department of Labor Since 2000
[93] Addressing Exploitations in Supply Chains, *Anti-Trafficking Review*
[94] New Report Highlights the Potential of Technologies to Uncover Patterns of Labour Exploitation - United Nations University Institute in Macau
[95] 18-year prison sentence for Sheriff's Deputy - Roseville Today
[96] Former Dallas Police Department Vice Detective Sentenced On Obstruction Convictions

warned her when there would be raids. In 2008, an NYPD detective and his girlfriend trafficked a 13-year-old runaway to 20+ customers; the detective was sentenced to just 3½ years for his crime. In 2011, LAPD Officer Oris Pace[97] was investigated for doing "inspections" on massage parlors where he forced women to undress and fondled them. Orlando Vice Supervisor Riggi[98] had a relationship with a woman referred to as "victim 1" and she gave him money twice a month. All of these stories appear in The Academy's slideshow on ethics in human trafficking investigations. On one slide, they explain that a woman who reported an officer was "not a charged victim," but there is no discussion of the ethics of charging victims.

Stanislaus County District Attorney Tony Colacito is direct with his concerns: "What are DAs not wanting to see? You having too much fun." The slide goes on to explain that if they have "too much fun" during prostitution stings where they "rescue" sex trafficking victims by arresting them, it could be considered "outrageous governmental conduct" and the case could be dismissed, or "your agency could be embarrassed."

By "having too much fun," Mr. Colacito is referring to the police practice of tricking sex workers and sex trafficking survivors into engaging in sex acts with them before arresting them. When stings are done under the guise of rescuing sex trafficking survivors or minors, these tactics are especially disturbing.

> Sexual violence is a tool by which certain peoples become marked as inherently 'rapable.' These peoples then are violated, not only through direct or sexual assault, but through a wide variety of state policies, ranging from environmental racism to sterilization abuse.
> -Smith, *Conquest: Sexual Violence and American Indian Genocide*

Mr. Colacito's concerns about police engaging in these "fun" investigatory tactics while "rescuing" alleged sex trafficking victims by arresting them do not seem to be unfounded. Prostitution charging documents in California generally state the law that they are accusing the defendant of violating, and then what acts the defendant took "in furtherance" of the crime. While most charging documents only alleged that the defendant went to a location to meet the undercover officer, or brought a condom, or accepted money, we found several that listed the "act of furtherance" as sex.

> On or about January 29, 2020, in the County of Santa Barbara, the crime of AGREEING TO ENGAGE IN ACTS OF PROSTITUTION, with an UNDERCOVER OFFICER in violation of **PENAL CODE SECTION 647(b)**, a Misdemeanor, was committed by [redacted], and that defendant did in furtherance of such agreement, the act of, SEX.

[97] LAPD Officer Gets 180 Days in Jail for On-Duty Assaults of Massage Parlor Women – NBC Los Angeles
[98] Internal affairs documents detail relationship between OPD cop and prostitute – Orlando Sentinel

On or about June 16, 2020, [redacted] did unlawfully solicit, engage in, and agree t engage in an act of prostitution with the intent to receive compensation, money and anything of value from another person, and did some act within this state in furtherance of an act of prostitution, to wit: sexual intercourse

On or about January 31, 2020, [redacted] did unlawfully solicit, engage in, and agree to engage in an act of prostitution with the intent to receive compensation, money and anything of value from another person, and did some act within this state in furtherance of an act of prostitution, to wit: sexual intercourse with a condom

These officers had "too much fun" "rescuing" these "trafficking victims."

[redacted], did commit a misdemeanor, namely: a violation of Section 647(b) of the Penal Code of the State of California, in that said defendant did unlawfully engage in and agree to engage in an act of prostitution and did some act within this state in furtherance of an act of prostitution, to wit, did drive to meet at the Carl's Jr parking lot.

An example of an act of furtherance that doesn't involve sex.

Surveillance Technologies and Anti-Prostitution Laws are Racist and Transphobic

> By the latter half of the nineteenth century, the analogy between erotic deviance and racial deviance emerged as a necessary element in the formation of the modern European imagination. The invention of racial fetishism became central to the regime of sexual surveillance, while the policing of "degenerate sexuality" became central to the policing of the "dangerous classes": the working class, the colonized, prostitutes, the Irish, Jews, gays and lesbians, criminals, alcoholics, and the insane. Erotic "deviants" were figured as racial "deviants," atavistic throwbacks to a racially "primitive" moment in human prehistory, surviving ominously in the heart of the imperial metropolis. At the same time, colonized peoples were figured as sexual deviants, the living embodiments of a primordial erotic promiscuity and excess.
>
> - Ann McClintock

Police surveillance has historically been used primarily against Black people, from people escaping enslavement to the FBI's COINTELPRO program aimed at Martin Luther King and other Black civil rights activists in the 1960s. Contemporary big data surveillance tools build on that history.[99] In a report for The Brookings Institute, researchers Lee and Chin[100] explain:

> In December 2020, the New York Times reported that Nijeer Parks, Robert Williams, and Michael Oliver—all Black men—were wrongfully arrested due to erroneous matches by facial recognition programs.[36] Recent studies demonstrate that these technical inaccuracies are systemic: in February 2018, MIT and then-Microsoft researchers Joy Buolamwini and Timnit Gebru published an analysis of three commercial algorithms developed by Microsoft, Face++, and IBM, finding that images of women with darker skin had misclassification rates of 20.8%-34.7%, compared to error rates of 0.0%-0.8% for men with lighter skin.[37] Buolamwini and Gebru also discovered bias in training datasets: 53.6%, 79.6%, and 86.2% of the images in the Adience, IJB-A, and PBB datasets respectively contained lighter-skinned individuals. In December 2019, the National Institute of Standards and Technology (NIST) published a study of 189 commercial facial recognition programs, finding that algorithms developed in the United States were significantly more likely to return false positives or negatives for Black, Asian, and Native American individuals compared to white individuals.[38] When disparate accuracy rates in facial recognition technology intersect with the effects of bias in certain policing practices, Black and other people of color are at greater risk of misidentification for a crime that they have no affiliation with.

Some have argued that big data surveillance is by nature objective and not racist, but research has repeatedly found that surveillance technologies serve to institutionalize and increase the effectiveness of racist laws and policing practices.[101] Anti-prostitution laws, including pimping and pandering laws, are clearly racist, sexist, and classist at their core. In *Helping Women Who Sell Sex:The Construction Of Benevolent Identities,*[102] Laura Agustin explains the development of European prostitution policy in the 1700s and 1800s when middle class women created occupations for themselves outside the

[99] The Snitch in the Silver Hearse - The Intercept
[100] Police surveillance and facial recognition: Why data privacy is imperative for communities of color
[101] Predict and Surveil: Data, Discretion, and the Future of Policing: Brayne, Sarah: 9780190684099: Amazon.com
[102] Helping Women Who Sell Sex: The Construction of Benevolent Identities

home by "rescuing" working class women into domestic servitude and moral instruction. In the United States, anti-prostitution policy was born of anti-Black and anti-Asian hate through the Mann Act of 1910, which made it a felony to transport a woman across state lines for immoral purposes–which included interracial relationships.[103]

California's current prostitution, pimping, pandering, and sex trafficking laws are enforced in ways that are as racist as the laws that preceded them. One of the only police departments that provided information on the race of those they arrested for prostitution, the Los Angeles Police Department, reported arresting 2,428 Black people, 2,271 Hispanic people, and only 621 white people. According to census.gov,[104] the City of Los Angeles' population is 45% white and only 9% Black.

On January 1, 2021, the Racial Justice Act went into effect in California. The RJA allows defendants to make the case that criminal laws are being applied to them in a manner inconsistent with how they are applied to people of other races. In one RJA filing, the Contra Costa Public Defenders Office wrote:

> On June 2, 2022, defense counsel, Kira Klement, solicited data from both the Alternate Defender's office and the Public Defender's Office in Contra Costa County regarding whether any attorneys have represented male clients charged with either Human Trafficking, Pimping, or Pandering… Multiple attorneys responded and reported a total of 22 male clients the combined offices have represented. Of those 22 male clients, **21 of them are Black.**

And:

> Deputy District Attorney, Dana Filkowski, who was the lead attorney of the Human Trafficking Unit for some time, exhibited clear racial bias in her examination of an expert witness. In November of 2021, Ms. Filkowski was the attorney who filed charges in Mr. Davis's case. On August 30, 2019, during a Preliminary Hearing, Ms. Filkowski asked a police officer, Officer Alexis Bartley, who was designated as an expert in human trafficking, pimping and pandering the following: "Would there be a particular significance to a black male adult being on 23rd Street wearing that hat?" …Officer Bartley responded: "Yes." (Id.) Mis. Filkowski then asked "What would that be?" (Id.) Officer Bartley responded "Just the intention of pimping or that he is in the area to pimp." (Id.) Ms. Filkowski specifically identified race as a factor in the expert's opinion that the black defendant in that case was a pimp… Such a question amounts not simply to implicit bias, but explicit bias.

[103] Mann Act | Wex | US Law | LII / Legal Information Institute
[104] U.S. Census Bureau QuickFacts: Los Angeles city, California

In an article called Black Pimps Matter: Racially Selective Identification and Prosecution of Sex Trafficking in the United States, the authors used various means to determine the percentage of people charged with sex trafficking who are Black:

> For example, we used bop.gov, the federal inmate locator, to determine the race of the convicted felon or felons named in an extensive review of randomly encountered articles, judicial opinions, media stories, and tallied the percentages of blacks. No matter how many random searches were conducted, ranges were 75 to 95% black males. The one time it dropped to around 70%, it was because of numerous white codefendants in one Gambino family FBI roundup. We did the same type of random searching at FBI.gov with Boolean searches for 18 USC1591, 18 USC 2423, and other sex trafficking terms. FBI press releases of arrests, convictions, and sentences were analyzed by checking with bop.gov, online mugshots, or news media photos to determine the race of the defendant or convict. The lowest figure found in any official report is from April 2011, when the Department of Justice generated a report stating that, between January 2008 and June 2010, federally funded task forces aimed at targeting human trafficking identified 2515 incidents of suspected human trafficking. That same report showed that, of the suspects identified in federal nationwide sex trafficking cases, 62% were black (Banks and Kycklehahn 2011). However, these counted "suspected" human traffickers, which means a lot of non-blacks were not convicted. We estimated 90% black when counting convicted human traffickers. Dr. Paul Hofer kindly provided us with national database analysis, which corroborated preliminary federal and state felony racial findings. Our Oregon findings were also corroborated by data analysis by Dr. Hofer, showing that 18 USC §1591 convictions of Oregon defendants between 2009 and 2014 were 84.2% black. Our findings were also corroborated in a recent study of Portland sex trafficking probationers where the sample revealed that 89% of those probationers were black (Gotch 2016). Importantly, despite analyzing her sample for criminogenic characteristics, Gotch surmised that the overrepresentation of blacks was due to policing practices. The statistics for the most punitive Oregon sex trafficking state charges, "Compelling Prostitution" between 2004 and 2016 for the State of Oregon shows 17 blacks compared to six non-blacks (Caucasian, Hispanic or Other) which is 74% black compared to the general state population of 1.8% black. Multnomah County for the same period, with approximately a 5% black population, shows 15 blacks and one non-black, (93.75% black) convicted for Compelling Prostitution.

Several state prostitution laws[105] have been overturned or changed because they targeted only women, not male sex workers, or in the case of manifesting prostitution laws, they targeted transgender women. Although laws have been rewritten to apply equally to male and female sex

[105] Coyote v. Roberts, 502 F. Supp. 1342 (D.R.I. 1980) :: Justia

workers, enforcement continues to be focused on both cisgender and transgender women. In 2023, many in law enforcement still believe that sex is inherently harmful to women, but not to men. Prosecutors refer to women selling sex as selling "themselves." None of these strange ideas seem to be applied to men who sell sex.

> Men are routinely expected to encounter and overcome trouble, but women may be irreparably damaged by it.
> - Agustin

Increasing big data policing or police use of surveillance technologies may increase prostitution related arrests, but these arrests are racist, sexist, and classist by nature.

Prostitution and Immigration Issues

Sex workers, including legal sex workers, are regularly denied entry to the USA and other countries. In a recent case reported on by VICE,[106] a virtual reality sex worker named Hex received a letter notifying her that she was permanently ineligible for admission to the USA because of "prostitution". Presumably, one of the databases that crawls the sex work side of the Internet captured her face at some point. The United States has a moral turpitude law that makes people who've committed "crimes of moral turpitude" ineligible for admission to the USA.[107]

In a Riverside case ESPLER was provided in its records search, defendant "Juan"'s attorney pleaded with the judge to sentence him to a diversion program rather than give him a conviction that would result in his deportation. "Your honor, the defense asks for mercy on this case," his attorney wrote. "[Juan]'s conviction on this charge will have immigration consequences. He will be placed in removal proceedings. The collateral consequences will be devastating, not only to him but to his family as well. He is the breadwinner in his home. His home has been America for 20 years. He is asking for one last chance." Juan was convicted.

Homeland Security has painted itself as an agency that "rescues" trafficking victims in the name of national security, but when Homeland Security's ICE officers raid Asian massage parlors, few sex workers meet the requirements to avoid deportation.

What Next: Unanswered Questions

We are left with more questions than answers. Many agencies did not provide the records we requested, or only provided partial records. Some of the things we are left wondering are:

[106] A Virtual Reality Sex Worker Was Denied Entry to the U.S. for 'Prostitution'
[107] What is a Crime of Moral Turpitude? | U.S. Immigration | Nolo

- What are the phone apps that sell our data to database companies like Clearview?
- Do cell phone companies provide tower data to CellHawk and similar companies without warrants?
- Are California police departments keeping databases of sex workers and/or our clients? If so, are they collaborating or do they have separate databases?
- Are sex workers and our clients reported to the Suspicious Activity Reporting Initiative? Are sex worker activists in the FBI's gang member database?

Given time and funding, future ESPLER investigations will report on answers to these questions.

What Next: Policy Recommendations

"It's time to pass bipartisan legislation to stop Big Tech from collecting personal data on kids and teenagers online, ban targeted advertising to children, and impose stricter limits on the personal data these companies collect on all of us." - President Joe Biden, February 7, 2023[108]

The problems explored in this report may seem sprawling and complex, but their solutions are simple:

1. **Ban commercial surveillance.** The Federal Trade Commission defines commercial surveillance as "the business of collecting, analyzing, and profiting from information about people." This includes companies that sell your information to police or advertisers as well as companies who sell information about individuals online to anyone who will pay. The United States is a world leader in technology, yet we are virtually alone in our lack of protections. A federal law is needed to ban commercial surveillance.
2. **Regulate police databases.** Oversight and regulation are needed to redirect police towards solving crimes against people rather than forcing sex workers to disrobe for photos of all their tattoos and building databases of sex workers–or databases of transgender people, as recently happened in Texas.[109] When databases are used, care needs to be taken that police agencies don't blur definitions, as they have with the Suspicious Activity Reporting Initiative and the FBI's gang member definition.
3. **Police, prosecutors, and courts should protect sex workers' and our clients' identities**. Publishing our names and arrests in newspapers and online subjects us to public hostility, discrimination in housing, employment, and social media, and at times, violence.
4. **We need government accountability and integrity laws** to prevent the conflation of things like prostitution and terrorism. When government bodies gaslight the public in this

[108] Remarks of President Joe Biden – State of the Union Address as Prepared for Delivery - The White House
[109] LGBTQ+ community 'terrified' after Texas attorney general sought data on trans Texans

way, and do so for profit, at the expense of the rights and liberties of citizens, disaster ensues.

5. **The California Public Records Act, California's Electronic Communications Privacy Act (CalECPA), the Racial Justice Act, and California Evidentiary Code 782.1 should be expanded to include direct meaningful consequences of the civil and criminal variety for agencies and personnel that violate them.**
6. **Police engaging in sex acts as an investigatory tactic should be criminalized.** We need our policy makers to take a strong leadership role in drawing this line in the sand and saying this is not okay, this is criminal behavior.
7. **Individuals should be notified by police about where their data, including photos, are being stored, how they are being used, and who can access them.**
8. **Police who steal sex workers' photos in order to catfish and arrest our clients should be held accountable.** No one should use our erotic photos without permission, but when the government does so under the guise of "rescuing" us, it is particularly reprehensible and contributes directly to public distrust.
9. **Remove prostitution from the federal moral turpitude statues** that are so vague as to be arbitrarily used to bar legally working sex workers like cam workers from entering the United States.
10. **Prostitution arrests should never be a means to deport sex workers, sex trafficking survivors, or our clients.**
11. **We call for a complete overhaul of prostitution and sex trafficking training for law enforcement to ensure that policing practices are aligned with the Racial Justice Act.**
12. **All aspects of consensual adult prostitution need to be decriminalized** to prevent the surveillance, public stigmatization of, and discrimination against sex workers and our clients.

Appendices:

Appendix A: County Fact Sheets

To view all county fact sheets in one PDF document, click here.

Individual county fact sheets with technologies, costs, and arrests are linked below:

Alameda County → Provided Partial Records

Alpine County ⓧ Did NOT Provide Records

Amador County → Provided Partial Records

Butte County ⓧ Did NOT Provide Records

Calaveras County → Provided Partial Records

Colusa County ⓧ Did NOT Provide Records

Contra Costa County → Provided Partial Records

Del Norte County ⓧ Did NOT Provide Records

Fresno County → Provided Partial Records

Humboldt County → Provided Partial Records

Imperial County ⓧ Did NOT Provide Records

Inyo County ⓧ Did NOT Provide Records

Kern County → Provided Partial Records

Kings County → Provided Partial Records

Lake County → Provided Partial Records

Lassen County ⓧ Did NOT Provide Records

Los Angeles County → Provided Partial Records

Madera County ⓧ Did NOT Provide Records

Marin County → Provided Partial Records

Mariposa County ⓧ Did NOT Provide Records

Mendocino County → Provided Partial Records

Merced County → Provided Partial Records

Modoc County ⓧ Did NOT Provide Records

Mono County ⓧ Did NOT Provide Records

Monterey County → Provided Partial Records

Napa County ⓧ Did NOT Provide Records

Nevada County ⓧ Did NOT Provide Records

Orange County → Provided Partial Records

Placer County → Provided Partial Records

Plumas County ⓧ Did NOT Provide Records

Riverside County → Provided Partial Records

Sacramento County → Provided Partial Records

San Benito County ⓧ Did NOT Provide Records

San Bernardino County → Provided Partial Records

San Diego County → Provided Partial Records

San Francisco County → Provided Partial Records

San Joaquin County → Provided Partial Records

San Luis Obispo County ⓧ Did NOT Provide Records

San Mateo County → Provided Partial Records

Santa Barbara County → Provided Partial Records

Santa Clara County → Provided Partial Records

Santa Cruz County → Provided Partial Records

Shasta County → Provided Partial Records

Sierra County ⓧ Did NOT Provide Records

Siskiyou County ⓧ Did NOT Provide Records

Solano County → Provided Partial Records

Sonoma County → Provided Partial Records

Stanislaus County → Provided Partial Records

Sutter County ⓧ Did NOT Provide Records

Tehama County ⓧ Did NOT Provide Records

Trinity County ⓧ Did NOT Provide Records

Tulare County → Provided Partial Records

Tuolumne County ⓧ Did NOT Provide Records

Ventura County → Provided Partial Records

Yolo County ⓧ Did NOT Provide Records

Yuba County ⓧ Did NOT Provide Records

ACKNOWLEDGEMENTS

Every step of producing this report took diligence, patience, and persistence, from dealing with uncooperative law enforcement agencies to advocating for fundamental human rights and civil liberties for sex workers and all Californians.

ESPLER would like to acknowledge the efforts of Maxine Doogan, Tara Burns, Allie Benz, Paden McNiff, Gill Sperlein, Megan Hobza, and Helena Eddy-Mizer. This report is the result of your insight and analysis.

Additionally, Electronic Frontier Foundation researchers Beryl Lipton, Dave Maass, and Paul Tepper contributed research to this report.

ESPLER deeply appreciates the team's commitment to holding law enforcement accountable and upholding the right to privacy, bodily autonomy, and freedom from government intimidation.

CONTRIBUTOR BIOS

Maxine Doogan is an American prostitute, social justice, and politics expert and advocate, documentarian, artist, author, and media personality. For 33 years, Maxine has regularly traveled across the U.S. and abroad advocating for the expanded rights and protected working conditions of sex workers. Her advocacy has successfully reformed prostitution laws in Alaska and California. Doogan is the Executive Director of the ESPLER Project, Inc.

Gill Sperlein is a Baltimore native who graduated summa cum laude from American University's Washington College of Law School before moving to San Francisco in 1994. Sperlein's law practice focuses on free speech and other First Amendment rights. In the past, he served on the Board of Free Speech Coalition and he currently serves as Vice President of the First Amendment Lawyers Association.

Tara Burns is a career sex worker, trafficking survivor, and writer/researcher who received her Interdisciplinary Masters in Social Justice from the University of Alaska Fairbanks. Her research at the intersections of lived experiences and public records have covered things like the lived experiences and policy recommendations of people in Alaska's sex trade and two decades of prostitution and prostitution related charges in Rhode Island. She has lobbied successfully to change Alaska's prostitution and sex trafficking laws. Burns is a board member of the Community United for Safety and Protection and Research Director of Call Off Your Old Tired Ethics Rhode Island (COYOTE RI).

Megan Hobza is a nonprofits strategist and grant writer who has worked with ESPLER since 2016. She specializes in consulting for grassroots nonprofits, serving clients in education,

advocacy, environment, health, and the arts. Her work as a community-building catalyst has included founding roles in the Whole Place of Whittier and Sustainable City nonprofits.

Allie Benz is a data analyst who received her Masters in International Human Rights from the Josef Korbel School of International Studies. Her work focuses on equity and people-centered data. She has previously worked on sex worker advocacy projects for COYOTE RI.

Helena Eddy-Mizer is a young digital artist. As someone with a parent who has worked in erotic services, freedom and the right to privacy is very important to her. She is proud to have been able to participate in this important project knowing firsthand what is at stake.

Paden McNiff is a California-based consultant and designer with a focus on digital marketing and content creation for progressive organizations, electoral candidates, and nonprofits.

Madelyn Roderigues is an Indigent Defence Attorney.