



 REPORT SURVEILLANCE & PRIVACY

Beyond Sanctuary: Local Strategies for Defending Civil Liberties

MARCH 21, 2018 — KADE CROCKFORD

Federal agencies—and the surveillance technologies that support them—have intruded into cities and states at the hyper-local level, resulting in apprehensions and detainments that have sent shockwaves of fear through communities. Most recently, the federal government under President Donald Trump has become increasingly aggressive in pursuing its immigration and law enforcement agenda.

Federal enforcement efforts rely on existing structures at the state and local levels. As a result, they tend to amplify the inequities of local policing, disparately impacting immigrants, dissidents, Muslims, LGBT people, the poor, and other oppressed groups. Across the nation, the federal government's aggressive detention and deportation approach to immigration enforcement has exacerbated existing discrimination suffered by immigrants of color, who like their U.S. citizen counterparts are many times more likely to be arrested and prosecuted for a variety of minor offenses compared to white people.¹

The policy decisions state and local leaders make in their communities can either facilitate or hinder these attacks on immigrants, communities of color, and other marginalized populations. Local governments that see federal agency actions as aggressive and harmful have the choice to push back.

Governments at the state, county, and municipal level have begun to respond to this federal overreach, with governors, mayors, and members of city councils actively seeking ways to protect their most vulnerable communities from being targeted by overly aggressive federal law enforcement action. Many cities across the country have become “sanctuary” jurisdictions, implementing policies that limit cooperation with federal immigration authorities.

But even in jurisdictions where local governments have opted not to cooperate with detainer requests from the federal government, immigration agents have begun haunting the halls of courthouses, seizing immigrants who appear for their court dates. In New York, for example, courthouse detentions have skyrocketed 900 percent in 2017.² These efforts are harmful, disruptive, counterproductive, and put immigrants of color at grave risk of detention—making them less likely to seek help from the police, appear at court, go to the hospital, or even take their children to school.³

So, in addition to the sanctuary approach, there are a number of lesser-understood and potentially even more powerful policy interventions that can work effectively at the state and local levels to protect civil rights and civil liberties in an increasingly hostile federal climate. These include: changing policing policy and procedures, halting participation in certain federal programs, and bringing community control over police acquisition and deployment of surveillance technologies.

This report looks at five nodes of concern, where local action can help protect vulnerable communities. In particular, it examines (1) policing that results in a large number of low-level arrests, which endangers people of color, including

immigrants; (2) law enforcement's collection, retention, and sharing of information about people who are not suspected of criminal activity; (3) municipal and state police participation in FBI Joint Terrorism Task Force operations; (4) surveillance technology acquisitions; and (5) data hygiene practices at state and local government agencies. In each section, the report recommends state and local policy reforms that can help protect vulnerable communities from overly aggressive and often discriminatory federal enforcement action.

Ending Police Reliance on Low-Level Arrests

The Trump administration has pledged to double down on the war on drugs,⁴ further militarize the border,⁵ bolster systems of surveillance and control,⁶ and ramp up the detention and deportation of undocumented immigrants.⁷ But the administration is not starting from square one in these efforts. Systems established and bureaucracies enhanced by prior administrations have formed a solid foundation for the Trump administration's racist and xenophobic policies targeting black and brown Americans and immigrants.

The first layer of this foundation is constructed in local municipalities and counties across the nation. Despite the federal government's substantial powers, it cannot enforce its will on the American public without substantial cooperation and participation by local authorities, most notably police departments.

Many of these police departments continue to pursue what is known as "broken windows" policing—a strategy that assumes police will be able to prevent serious violence if they crack down hard on minor offenses, such as jumping turnstiles and drug possession. Unfortunately, this strategy of making low-level arrests tends to focus oppressively on poorer neighborhoods of color, feeding our jail systems with a steady flow of black and brown bodies—among them immigrants, and the bulk of them poor.⁸

This section reviews recent history, outlining specific policy decisions that helped create this architecture of oppression, and describes a straightforward policy reform to defend immigrants and other marginalized people. It will recommend that, as cities, counties, and states look for ways to protect their vulnerable communities, they should consider an enhanced sanctuary city approach that contemplates interventions in the detention and deportation process *before* immigrants enter state or local police custody. Such a model must take into account the role that low-level arrests play in immigration enforcement.

Good Immigrant versus Bad Immigrant: The Secure Communities Disaster

Under President Barack Obama, the United States remained the most carceral nation in the world—locking up more

Americans per capita than China, Russia, and Iran.⁹ President Obama deported more people than any prior president in U.S. history.¹⁰ But under Obama's tenure, thanks in part to the actions of U.S. Attorney General Eric Holder, the federal prison population began to decline for the first time since the Carter administration.¹¹ And, despite the mass deportations, Obama took executive action, through the Deferred Action for Childhood Arrivals (DACA) program, to protect hundreds of thousands of undocumented immigrants who came to the United States as children.

The Obama administration used executive authorities to limit the use of mandatory minimums in drug prosecutions at federal prosecutors' offices around the country, to restrict the federal government's use of private prisons, and to protect undocumented youth, but the administration also institutionalized systems of surveillance and control that deepened existing links between the criminal law enforcement and immigration systems.

In 2013, the Obama administration completed full implementation of a controversial Bush-era surveillance program called "Secure Communities" (also known as S-Comm).¹² In most counties and municipalities in the United States, police and sheriff's departments fingerprint anyone they arrest. Historically, local and county departments have shared those fingerprints with the Federal Bureau of Investigation (FBI), so that the FBI can conduct a background check using the fingerprints and send the results back to the locals. That's how a local police department learns, for example, whether someone it has just arrested is wanted for a serious offense in another state, or has used an alias.

S-Comm changed this long standing practice by adding one step in the process. Under the program, after the FBI receives fingerprints of arrestees from local or county departments, it automatically shares the prints with ICE, the Department of Homeland Security (DHS) agency responsible for investigating, detaining, and initiating deportation proceedings against people. By the time S-Comm was fully implemented in 2013, the fundamental character of a local arrest in any county or town in the United States had changed.¹³ Under S-Comm, an arrest isn't just an inroad into the local or state criminal punishment system; it can be a flare shot up into the sky notifying ICE of the presence and location of a person in the United States on a visa or without documentation.

The Obama administration initially defended S-Comm as a commonsense immigration program that sought to get "convicted criminals" off the streets and into deportation proceedings. The program would result in the deportations of "the worst of the worst," states and communities were told.¹⁴ But the system didn't work that way. In 2013, the first year during which S-Comm was fully operational throughout the United States, only a small fraction of the people ICE deported were convicted of what ICE calls "Level 1" offenses, which include homicide, espionage, sexual assault, and other serious felonies, but also certain types of larceny, mail fraud, and drug offenses—including the sale of marijuana,

which nine states and Washington, D.C. now consider a legal activity.¹⁵ Despite the Obama administration's pledges about the true intention of the S-Comm program, nearly half of all deportations in 2013 were of people convicted of immigration and traffic violations.¹⁶

While S-Comm didn't produce the results the Obama administration promised, it did succeed in solidifying the immigration narrative into the damaging "good immigrant/bad immigrant" framework. Now, when the Trump administration says it only wants to deport the "bad hombres," it can point to the groundwork created by the Obama program as historical precedent. Furthermore, S-Comm also engineered one of the largest federal surveillance systems in current use by the U.S. government, sweeping millions of people a year into ICE databases.¹⁷ That system is perfectly primed to assist the Trump administration in its mass deportation efforts; but state and local policymakers can take steps to put a wrench in it.

Trump's Reliance on Local Law Enforcement

In 2017, the Trump administration overhauled the nation's immigration enforcement priorities when it issued two immigration-related executive orders. Among the changes included the granting of *carte blanche* to ICE agents to make determinations about whom to detain and deport, under what circumstances, and for what reasons.¹⁸ Where the Obama administration imposed a system of priorities, the Trump administration promised to get out of the way, to let individual agents decide the fate of persons they captured or set in their sights. Trump's executive order regime reoriented immigration enforcement, prioritizing the detainment and deportation of noncitizens who "have been charged with any criminal offense that has not been resolved" and "have committed acts that constitute a chargeable criminal offense."¹⁹ As Human Rights Watch observes in a 2017 report on the first year of deportations under Trump, the latter could include "crimes" such as jaywalking.

The results of these policy changes were predictable. Just a month after the Trump inauguration, a fifteen-year veteran of ICE told the *New York Times*, "The discretion has come back to us; it's up to us to make decisions in the field. We're trusted again." More than a year into the Trump presidency, we are starting to get a clearer picture of what "taking the shackles off" ICE agents has meant in terms of ICE detention and deportation rates. In the first year of Trump's presidency, ICE detentions inside the United States soared by 42 percent, while detentions of noncitizens with criminal convictions increased by 19 percent. Human Rights Watch's analysis found that the vast majority of these people were convicted of minor offenses:

In the most recent data available, which only covers one month of the Trump administration, strikingly few of the non-citizens arrested by ICE who had criminal convictions had been convicted of crimes of a violent or dangerous nature. One in three “criminal” arrests involved someone whose most serious crime was an immigration offense, almost always the act of entering the country illegally. About 16 percent had been convicted of a drug offense and another 15 percent had a traffic offense as their most serious crime. Fewer than 1 percent had been convicted of a homicide, and the most serious offense of only 19 percent, fewer than one in five, included violent or potentially violent crimes.²⁰

In Trump’s America, immigrants have ample reason to fear that any interaction with the criminal legal system will result in the initiation of deportation proceedings against them.²¹

Trump’s plans to rely on local law enforcement to be the tip of the spear for deportation efforts were not a secret. An April 2017 photograph of top Trump advisor Steve Bannon’s office captures a whiteboard, upon which is written a number of campaign pledges his administration is working to realize. One of the pledges reads: “Issue detainers for all illegal immigrants who are [illegible] for any crime, and they will be placed into [illegible] removal proceedings.” It’s a safe bet that those illegible words are “arrested” and “immediate.” In August 2016, Trump delivered a speech on immigration in which he said his administration “will issue detainers for all illegal immigrants who are arrested for any crime whatsoever, and they will be placed into immediate removal proceedings.”²²

That very framework is coming to gruesome life in American cities. In May 2017, the *Intercept* reported on data from Gwinnett County, Georgia, showing that traffic stops are the main driver of ICE contact with immigrants in the community. Data from a local jail show that, of 500 people flagged by local police to ICE, a full 70 percent were locked up because of traffic violations, the most common being *driving without a license*.

We don’t have comprehensive data to show exactly how many immigrants have been deported as a result of arrests for minor offenses. But in early 2018, the Trump administration released its own analysis of fiscal year 2017 nationwide immigration arrest data from ICE’s Enforcement Removal Operations (ERO) division.²³ The report reveals that 89 percent of the over 143,000 people ICE arrested in fiscal year 2017 had either criminal convictions or faced pending criminal charges at the time of their arrest. The document claims these figures support the conclusion that ICE is “prioritizing its enforcement resources on those who *pose a known threat to national security and public safety*” [emphasis added]. The report’s details suggest otherwise. The bulk of the criminal charges and convictions dealt with minor offenses: 53 percent of those arrested had drug-related offenses on their records, 48 had traffic-related offenses, and 44 percent had immigration-related offenses.²⁴ Thousands of people were also arrested due to pending charges or convictions for the following: public peace violations (8 percent), larceny (14 percent), and a category ICE calls

“obstructing judiciary, congress, legislature, etc.,” which includes parole and probation violations and failure to appear (15 percent).²⁵ The report reveals some curious details, such as a nearly 1,800 percent spike in ICE arrests of Haitians during the Trump administration’s first months in office. While ICE arrested 310 Haitians in fiscal year 2016, the agency arrested 5,578 Haitians the following fiscal year.

The personal cost to immigrants resulting from arrest for minor offenses is extremely high. For example, on May 14, 2017 a Minneapolis transit cop arrested 23-year old Ariel Vences-Lopez on charges of suspicion of committing fare evasion, giving a false name, and obstructing a police officer. On May 15, ICE asked the county jail to hold Mr. Vences-Lopez on an immigration detainer. ICE picked him up from local custody the next day, and he was placed into deportation proceedings. Had the transit police officer not arrested Mr. Vences-Lopez on this minor charge, he would probably still be living in Minneapolis a free man.

Even Americans not at risk of deportation pay a high cost when arrested. Low-level arrests like these typically do not lead to convictions. Prosecutors often drop the charges, or people plead to what’s called, in various states, a continuance without a finding, pretrial probation, or adjournment in contemplation of dismissal, meaning no conviction will appear on their record. But for poor people and people struggling to overcome entanglement with the criminal legal system, even one arrest can cause devastating problems that simply will not go away. Even if an arrest doesn’t lead to a conviction or incarceration, it can have severe consequences for individuals and families.²⁶

If you’re too poor to pay bail, you can sit in jail for weeks or months waiting for prosecutors to call your case—even if you’re innocent of the charges against you. While you’re in jail, you’ll likely lose your job, and maybe even your home and your children. You may also find that an arrest record is used as a proxy for judgments made about you without your knowledge, which can compound economic and racial inequalities.²⁷

For thousands of American citizens, even one arrest can cause irreparable harm. For Mr. Vences-Lopez and so many other immigrants, an arrest for a minor offense can mean life as you know it is abruptly brought to an end.

Low-Level Arrests in the United States Disproportionately Impact People of Color

Mr. Vences-Lopez’ arrest for the minor offense of fare evasion is but one data point among millions like it in the United States each year. While we don’t have comprehensive immigration data to show how enforcement priorities have changed deportation patterns since Trump’s inauguration (apart from the fiscal year 2017 data cited above), we do have large quantities of arrest data confirming racial disparities remain rampant in low-level policing in the United States.

Data from Massachusetts and other states nationwide show that black and brown people are far more likely to be arrested for low-level offenses than their white counterparts. In New York City, for example, 92 percent of people arrested in 2015 for turnstile jumping on the subway were people of color. In the city of Worcester, Massachusetts, black and Latinx people accounted for over 80 percent of arrests for trespassing in the years 2012 to 2016, while these groups together make up just 32 percent of the population.

Massachusetts statewide arrest data obtained by the ACLU of Massachusetts also reveal extreme racial disparities in terms of whom police choose to arrest versus to whom they choose to issue summonses—for the exact same offenses. Statewide arrest data from 2012 to 2016 show that 96 percent of people arrested for drug offenses and identified by police as Hispanic were taken into custody instead of being issued summonses to appear in court. Data for the same years show that police took into custody 90 percent of black people arrested for drug offenses, while only 84 percent of white people arrested for drug offenses were brought in. In other words, white people cited for a drug offense in Massachusetts were allowed to go home with a court date at much higher rates than for blacks and Hispanics. In fact, the vast majority of Latinx people police suspected of drug crimes were taken into custody—and if their fingerprints were taken during the booking process, these were sent to ICE.²⁸

Recent figures show that more than one in every nine arrests in the United States is for drug possession, amounting to a staggering 1.25 million arrests per year. On an average day in the United States, about 137,000 people are locked up on drug possession charges, most of them still awaiting trial. People of color and the poor are disproportionately targeted.²⁹ Federal arrest data from 2010 showed that black Americans were four times more likely to be arrested for marijuana offenses than white Americans, despite the fact that blacks and whites use marijuana at the same rates.³⁰

Recommendations

Sanctuary cities across the country have drawn the unwanted attention of the U.S. Department of Justice under Secretary Jeff Sessions. While there's no single model for designating a town or city a sanctuary, it generally means that (1) local law enforcement do not engage in controversial 287(g) programs, which deputize local police as federal immigration agents; and (2) local law enforcement do not hold people on ICE “detainer” requests after they've been cleared for release from local custody. The Trump administration has pledged to deny federal grant monies to sanctuary cities for following this approach. Those threats may not amount to actual budget cuts for localities, but the threat itself has chilled some mayors and governors.³¹

But there are other ways that local governments can keep their vulnerable residents out of the Trump deportation machine that will also advance long-standing criminal justice policy goals: local and county police departments can stop making arrests for certain categories of offense, and cities and states can decriminalize some of those offenses.

When local police arrest someone and send their prints to the FBI, the FBI shares those fingerprints with ICE. The best way to stop that from happening is, simply, for local police to stop arresting people for minor crimes, including:

- drug offenses;
- traffic violations, including driving without a license, driving with a suspended license, and driving with an expired registration;
- petty larceny;
- disorderly conduct;
- trespassing;
- public drinking and drug use;
- vagrancy; and
- fare evasion.

These types of minor offenses account for the vast majority of arrests in the United States. FBI crime data from 2015 show that, of the nearly 11 million arrests nationwide that year, just over 500,000 were for violent crimes, or about 4.5 percent. Meanwhile, nearly 1.5 million of those arrests were for property crimes, nearly 1.5 million were for drug crimes, and larceny accounted for over 1.1 million arrests.³²

If police really think it necessary, for public safety, to issue a summons for these offenses, doing so in place of arresting someone will have the dual benefit of keeping that person out of ICE's sights, as well as keeping them out of jail.³³

Some municipalities are already taking action to protect immigrants at the local level by changing criminal justice policy. In Colorado, for example, Denver advocates changed local law to reduce the maximum sentence for many municipal crimes. Certain convictions make noncitizens—including green card holders—deportable, but only if they are sentenced to

a year or more of imprisonment. As a result, Denver changed the law to reduce the maximum sentence for various crimes from 365 to 364 days.³⁴

But the best strategy is to push for an end to broken windows style policing, and the low-level arrests that have made the strategy so notorious in communities of color across the United States.³⁵

Limiting Law Enforcement Intelligence Collection and Sharing

Programs like S-Comm tied local law enforcement to federal immigration authorities in new and dangerous ways, turning arrests into opportunities for ICE intervention. But local intelligence collection and sharing policies can be just as harmful as S-Comm, sweeping innocent people into a vast machinery of surveillance and law enforcement. On the other hand, if done right, policies governing the collection and sharing of intelligence and the state and local police level can go a long way towards shielding our local communities and their most vulnerable members from unwanted federal harassment and repression.

The American Surveillance Super-State, from COINTELPRO to 9/11

No study of American domestic surveillance gone wrong would be complete without mention of the horrible example of J. Edgar Hoover's FBI. From the 1950s through the early 1970s, the FBI under Hoover ran a domestic surveillance and espionage program targeting black Americans, suspected communists, Vietnam War resisters, and left-wing dissidents. The FBI called it COINTELPRO, short for counterintelligence program. At its height, the FBI had five thousand informants on its payroll, working in the civil rights and antiwar movements to try to cripple them from within.

An infamous 1970 memo from FBI headquarters urged agents to get more aggressive with their field interrogations of members of radical leftist groups. "It will enhance the paranoia endemic in these circles and will further serve to get the point across there is an FBI agent behind every mailbox," the memo said.³⁶ That memo, along with thousands of other internal FBI documents, was liberated by activists who broke into a Pennsylvania FBI office in 1971 and stole every paper file they could carry out. The activists gave the documents to reporters, who, using the newly enacted Freedom of Information Act, broke open the COINTELPRO scandal.

The COINTELPRO revelations sent shockwaves through Washington, D.C. Congressman Frank Church led a committee to investigate domestic political spying.³⁷ His committee pulled back the curtain to reveal a cancerous growth in the American body politic: a sprawling, repressive domestic surveillance apparatus that, almost entirely in secret, aimed to

limit and manipulate the boundaries of political discourse in the United States. The FBI had even kept intelligence files on Supreme Court Justices, Church's committee found. J. Edgar Hoover was a master at political blackmail, making him an untouchable for decades in D.C. Hoover's disregard for democracy enabled him to act above the law.

In light of these and other disturbing revelations about the activities of U.S. intelligence agencies, Congress formed the intelligence committees as a way to provide an official check on the FBI and CIA. Also, for the first time in U.S. history, the U.S. attorney general established guidelines requiring that FBI agents suspect someone of a crime before digging into their personal life and amassing a file on them. These guidelines were meant to prevent the kind of political surveillance and harassment Church's committee had discovered the FBI was neck deep into. The FBI was supposed to focus on people committing serious, interstate crimes—not people with unpopular political views, or religious or racial minorities. The guidelines aimed to create and enforce a new institutional culture at the FBI, one focused on crime instead of policing dissent.

Those attorney general guidelines generally held for nearly thirty years, until September 11, 2001. After the attacks, everything changed.

First, Congress created the Department of Homeland Security (DHS), which is now the largest non-military federal bureaucracy, overseeing 240,000 employees and dozens of sub-agencies, including the Coast Guard, ICE, the Transportation Security Administration (TSA), Customs and Border Protection (CBP), and the Secret Service. DHS immediately got to work building an infrastructure to connect law enforcement and intelligence agencies, up and down and across government, from the local level all the way up to the National Security Agency (NSA). One of the mechanisms for achieving this connection was the creation of "fusion centers" in states across the country—places where local, state, and federal law enforcement would sit next to representatives from the U.S. military and private industry to share information and intelligence about a host of potential "threats," often including political protesters upset with the status quo.

Another thing the federal government did after 9/11 was to significantly revise the attorney general guidelines, which largely prevented FBI agents from spying on people who were not suspected of criminal activity. That policy change set the tone for a federally integrated state and local law enforcement community, suddenly focused on counterterrorism and newly recognized as intelligence partners in the national effort. From the local level all the way up, the wall between intelligence and criminal matters came down, the gloves came off, and the consequences have been devastating. The institutional culture, once reformed, had swung back in the direction of limitless state power. These were changes for the worse—both for civil liberties *and* public safety. The institutional table was set to repeat the worst excesses of the Hoover

era, but this time, the federal intelligence bureaucracy had two powerful new tools: advanced information sharing systems integrating state and local police with the federal intelligence architecture, and digital technologies that facilitate mass surveillance and data overload.

Suspicionless Spying: Bad for Safety, Bad for Civil Liberties

Among the post-9/11 intelligence sharing programs pushed on state and local governments was “See Something, Say Something,” also known as the Suspicious Activity Reporting (SARs) program. The theory behind the SARs program is that “pre-operational” terrorist attack planning may look like innocent activity, such as photographing public buildings or asking questions about security procedures, and so goes unnoticed. To ferret out such planning, the program gives absurd advice to the public, for example, asking ordinary people to be on the lookout for “The Eight Signs of Terrorism,” which include taking notes, collecting money for donations, and cash withdrawals.³⁸ If state and local police keep detailed records of such incidents, and pass on leads about them to the FBI, the theory goes, law enforcement and intelligence agents may be able to stop the next big attack. But this overly broad approach to suspicious activity reporting has not, in practice, worked to deter terrorism—even as it has caused real discriminatory harm.³⁹

The “See Something, Say Something” program has netted a lot of useless information, wasting law enforcement time and resources chasing down bad leads, typically targeting people perceived to be Arab, Middle Eastern, Muslim, or South Asian. While it has been well documented that the SARs program has resulted in racial profiling and discrimination,⁴⁰ there’s no publicly available information to suggest it has been useful in stopping terrorism.

But the SARs program is hardly unique in at least one core sense: law enforcement officials across the country have long engaged in racially discriminatory surveillance programs targeting people not suspected of crimes, through both gang databases and the notorious tactic of stopping, frisking, and questioning people on the street. In the post-9/11 age, communities that have long been targets of enhanced law enforcement attention are facing increasingly severe consequences in the new information sharing environment.⁴¹

Post-9/11 developments in Massachusetts are exemplary of a national trend. In the years since 9/11, the state has received nearly \$1 billion in DHS grants for “counterterrorism” operations.⁴² Millions of those dollars have gone to the two state fusion centers: the Boston Police Department’s Boston Regional Intelligence Center (BRIC), and the Commonwealth Fusion Center run by the state police. State and local enforcement officials at these fusion centers sit side-by-side with their federal counterparts, including agents from the FBI and ICE, and share intelligence. Just as at the federal level in the post-9/11 era, the Boston Police Department’s privacy and civil liberties policy allows analysts and officers to collect, retain, and share information about people who are not suspected of engaging in criminal activity.⁴³

In Massachusetts, as in states across the country, the post-9/11 focus on “counterterrorism” intelligence collection and sharing, merged with a much more deeply entrenched system of categorizing and tracking young men of color through the architecture of the local fusion center. The BRIC serves as a representative case study of what happens when a local police department with a history of racially disparate enforcement and surveillance is transformed into an arm of the federal government’s intelligence and immigration system. The results are predictably bad—particularly for black and brown youth.

One recent case in Boston illustrates precisely the harms that can come to youth of color when the perfect storm of federal-local intelligence sharing, disparate enforcement and surveillance against people of color, and suspicionless monitoring is unleashed on a community. In that case, documented by the *Intercept*, a teenaged El Salvadoran immigrant was at his high school in the predominately Latinx neighborhood of East Boston when an argument broke out near him in the cafeteria. Despite the fact that no physical violence occurred, Boston School Police later looked at video surveillance footage of the incident and documented the student as a suspected gang member in an incident report. The report was then forwarded to the BRIC. According to the student’s lawyer, a disastrous chain of events unfolded after the Boston police shared the report with ICE.

First, an agent from ICE’s Homeland Security Investigations unit examined the student’s Facebook page, where he found images of the teenager wearing red, blue, and white clothing. This was enough for the Feds to decide he was indeed in a gang—despite the fact that “one of those photographs was taken on the day of a Salvadoran parade in Boston when [he] was wearing blue and white, the colors of El Salvador’s flag.” ICE then seized him and initiated deportation proceedings against him.

The student’s lawyer told *Intercept* reporter Ali Winston what anyone who pays close attention to law enforcement and intelligence practices already knows: this likely wouldn’t have happened had her client not been Hispanic. “My client was going to school full-time and working at a restaurant from 5 p.m. to midnight—he didn’t have time to be a gang member,” attorney Sarah Sherman-Stokes told Winston. “What has happened is that every behavior problem of a young brown person has become a gang problem. I sincerely doubt that a lunchroom dispute would result in this information being sent to BRIC were they not poor kids of color.”

In November 2017, an ICE agent told CBS News the agency relies on gang determinations, often made by state and local police departments without establishing a nexus to criminal activity, in order to prevent detained immigrants from being released at bond hearings. “The purpose of classifying him as a gang member or a gang associate,” the agent said, “is because once he goes in front of an immigration judge, we don’t want him to get bail.”

The Boston Police Department's gang policy allows officers to list people as gang members even if the police have no reason to believe the persons are suspected of criminal activity. As in other cities nationwide, inclusion in Boston's database is predicated on a points system. "Reasonable suspicion" of criminal involvement is reached when officers have amassed criteria adding up to ten points—even if none of those criteria relate to criminal activity. For example, someone could be listed in the Boston police gang database if an outside law enforcement agency told BPD the person is a gang member (8 points) and a BPD officer observed the person in a "group related photograph" (2 points). Alternatively, someone could be identified as a gang member by BPD if police officers conducting social media surveillance saw a photograph of someone wearing a certain color (4 points), using a certain nickname (4 points), and standing next to someone who is already included in the database (2 points).

Once the information about the young man in Boston was sent to the regional fusion center, the BRIC, it ended up in the hands of federal agents. This story shows why it's so important for governments to implement sensible information collection and sharing policies at the state and local level. These policies should bar the collection, retention, and sharing of information that is not directly linked to well-founded suspicion of specific criminal acts.

In the United States, law enforcement officials shouldn't be keeping tabs on anyone or creating an intelligence file on their activities if there is no suspicion of criminal activity. But due to gang databases, street-level surveillance mostly targeting black and brown youth, enhanced information sharing and relaxed local rules after 9/11, and billions of dollars of funding for intelligence systems for state and local law enforcement across the country, this troublesome surveillance is not only happening—it's resulting in catastrophic material consequences for some of the most vulnerable people in the country.

Recommendations

Police departments and fusion centers should institute policies mandating a criminal predicate requirement for intelligence collection, retention, and sharing. Doing so will go a long way toward preventing scenarios like the one that unfolded in East Boston that led to an innocent student landing in immigration detention, fighting a deportation order. Better intelligence policy will also protect young people of color who are citizens from law enforcement harassment and even incarceration due to often arbitrary and secretive inclusion in gang databases.⁴⁴

Specifically, policies should require that law enforcement officials have reasonable suspicion to believe someone is involved in criminal activity before collecting, maintaining, or sharing information about that person—with specific, clearly delineated exceptions, for example in missing persons cases. If the matter involves First Amendment protected

activity or association, policy should dictate that law enforcement may only collect, maintain, or share information that specifically relates to the suspected criminal activity.⁴⁵ Finally, policies should ban the use of race, religion, ethnicity, and national origin as a factor to any degree in determining reasonable suspicion.

Some police departments and cities have already taken steps to align their information gathering with civil liberties and racial justice. In June, 2017, the Providence, Rhode Island mayor signed a far-reaching police oversight ordinance into law. The ordinance bars Providence police from considering race, political views, ethnicity, language, and housing status when determining whether they have reasonable suspicion to believe someone has engaged in—or will soon engage in—criminal activity. And in September 2017, concerns about the racially disparate impact of the Portland, Oregon police department's gang database led officials to shutter it.⁴⁶

Withdrawing Local Police from the FBI's Joint Terrorism Task Force Operations

The Joint Terrorism Task Force (JTTF)—a partnership between federal, state, and local agencies—had about thirty or so operations scattered around the country before 9/11, the first created in New York City in 1980. Now, there are more than 180 JTTFs nationwide,⁴⁷ comprised of state and local law enforcement, FBI agents, ICE agents, TSA officers, members of the military, and representatives from dozens of other federal agencies. The Boston JTTF, for example, includes officers from—at minimum—the following state and local departments and agencies: Springfield PD, Worcester PD, Essex County Sheriff, Lowell PD, Pittsfield PD, Providence PD (RI), Chicopee PD, West Springfield PD, Massachusetts Department of Corrections, Rhode Island State Police, Portland PD (ME), Manchester PD (NH), MBTA PD, Boston PD, New Hampshire State Police, Holyoke PD, and the Massachusetts State Police.

When state and local law enforcement officers work on JTTFs, they are deputized as federal agents. Memoranda of understanding (MOUs) obtained by the ACLU through public records requests show that when local departments and agencies assign officers to work on the task forces, those state and local employees follow federal rules for intelligence gathering and surveillance.⁴⁸ In most cases, these federal rules are less stringent than local or state law. For example, in California and other states, state and local police are required to obtain warrants to track cell phones. Federal agents operating in California, and those local police officers deputized as federal agents on JTTFs, are not necessarily required to do so—even if state law requires it.⁴⁹

Partnerships on JTTFs may also enable local and state police to conduct activities in secret, under cover of federal law protecting “classified information,” where their activities would otherwise be subject to public scrutiny through state open records laws. Sometimes, local officers deputized to work as federal agents on JTTFs aren't even subject to ordinary

chain-of-command requirements, for example, if their local commanding officer doesn't have security clearance to access information held by the JTTF member. These frameworks make it impossible to hold local and state law enforcement officials accountable for their work on JTTFs.

Making matters worse, federal law and Department of Justice rules established in 2008 allow FBI officials to conduct suspicionless investigations called "assessments," during which the FBI claims the authority to conduct a range of invasive surveillance and intelligence-gathering techniques, including the use of covert informants.⁵⁰ When tasked to the JTTF and deputized as federal agents, state and local officers can do the same.

Under existing Department of Justice and FBI rules, JTTF officers can:

- infiltrate, monitor, and even direct the activities of religious and political groups;⁵¹
- use biased racial and religious profiling;⁵²
- open an investigation into someone even if they don't suspect that person of involvement in any crimes; and
- obtain huge quantities of sensitive, personal information about people without any suspicion of criminal activity.

Local and state police assigned to JTTFs and deputized as federal agents may even have access to information collected by the CIA, NSA, or foreign intelligence agencies,⁵³ as their FBI counterparts do.⁵⁴ Indeed, FBI guidelines allow agents to ask the CIA and NSA for information on people agents are investigating during an assessment. Again, agents and task force members do not even need to suspect someone of involvement in criminal activity before opening such an assessment. Local police assigned to the JTTF may therefore have access to information about Americans that was collected by the NSA without any judicial process, even if the targets of the spying aren't suspected of any crime—let alone a serious offense connected to terrorism.

At the same time, while JTTF members get all the privileges and powers of federal agents, the agency MOUs establishing JTTF relationships with the FBI put the burden of paying the local officers' salaries on the local department. So, while a local community pays, the local officer is allowed to use more permissible federal rules regarding surveillance, and his or her local community members may be in the dark about what that local officer is actually doing with those local dollars. And worse still, if the local officer is sued as a result of his work with a JTTF, the local department is required, under the terms of the MOU, to pay out any adverse settlements or judgments.

The FBI calls JTTFs “our nation’s front line on terrorism: small cells of highly trained, locally based, passionately committed investigators, analysts, linguists, SWAT experts, and other specialists from dozens of U.S. law enforcement and intelligence agencies.”

But communities and individuals who have been monitored, harassed, or threatened by JTTF operations or their task force officers may see their role differently. To those groups, the JTTFs likely appear more interested in solidifying and expanding the power of their own bureaucracy, and protecting the political, social, and economic status quo—often at the expense and on the backs of marginalized communities. And despite the FBI’s claim that the JTTFs are the nation’s “front line on terrorism,” the FBI doesn’t have much to show, in terms of benefits to public safety, for the vast expenditures of public funds poured into them.⁵⁵

So what have the JTTFs done with all the money and power they’ve amassed over the past fifteen years? On the one hand, they’ve pursued controversial “terrorism” investigations of Muslims, leading to prosecutions oftentimes predicated on informant-driven, FBI-manufactured terrorism plots. Other times, their operations have been even more nakedly political, involving the harassment, intimidation, and monitoring of dissidents. In both types of cases recounted below, public trust in the FBI suffers—particularly among Muslim, immigrant, and dissident populations—with no demonstrable benefit to public safety.

Targeting Islam: FBI, JTTF, and Other Operations in Muslim Communities

According to an *Intercept* study, after 9/11, “most of the 806 terrorism defendants prosecuted by the U.S. Department of Justice have been charged with material support for terrorism, criminal conspiracy, immigration violations, or making false statements—vague, nonviolent offenses that give prosecutors wide latitude for scoring quick convictions or plea bargains.”⁵⁶ The *Intercept*’s data show that large numbers of these cases were predicated on FBI informant-driven investigations—cases in which paid FBI assets, often working closely with FBI agents, devised, funded, and facilitated fake terror plots to be “discovered” by the FBI, and any unwitting co-conspirators arrested.

Of the 801 people convicted of terrorism-related offenses and sentenced to prison since 9/11, 418 have been released from incarceration, usually with no parole conditions requiring enhanced monitoring. As the *Intercept* observes, this astonishing fact suggests “that the government does not regard them as imminent threats” to the United States.

But while the government may not actually view these people it has convicted of terrorism offenses as threats to the United States, its officials nonetheless marshal those prosecutions as supposed evidence of an existential threat requiring billions of dollars in annual expenditures and nearly limitless authority for law enforcement and intelligence agencies.

As you might expect, Muslims in the United States—like their coreligionists in foreign countries under attack by U.S. weapons—bear the burden of shouldering this destructive paradigm.

People in the United States are far more likely to die from routine gun violence than from acts of political terror, but the FBI and its top officials routinely describe Muslim terrorism as the greatest domestic security threat facing the United States.⁵⁷ In fact, terrorism poses such an infinitesimally small risk to people in the United States that our televisions are more likely to kill us than are terrorists of any political or religious stripe.⁵⁸ Toddlers kill more people in the United States every year than do Muslims.⁵⁹ Over the past nine years, white supremacists and other right-wing terrorists have committed twice as many domestic terrorist attacks than have Muslims.⁶⁰ And for American women, the greatest violent threat comes not from terrorists or other strangers, but rather from their own husbands, partners, and boyfriends.⁶¹

Despite those facts, the substantial number of FBI investigations targeting Muslims conducted each year is used to justify ever-expanding FBI budgets and surveillance powers. So, while Muslims do not pose a significant threat, the FBI's targeting of Muslims has an enormously important strategic value to the bureau. As former FBI assistant director Thomas Fuentes said:

*“If you’re submitting budget proposals for a law enforcement agency, for an intelligence agency, you’re not going to submit the proposal that ‘We won the war on terror and everything’s great,’ because the first thing that’s going to happen is your budget’s going to be cut in half. You know, it’s my opposite of Jesse Jackson’s ‘Keep Hope Alive’—it’s ‘Keep Fear Alive.’ Keep it alive.”*⁶²

- THOMAS FUENTES

The FBI budget would not be as flush if it were waging a global war against television sets, toddlers, the right-wing, or heterosexuality, nor would it be granted the sweeping powers it now holds. Muslims in America are a much easier and more politically useful target.

As a result, many if not most of the FBI's 15,000 informants target Muslims and Muslim communities,⁶³ racking up huge numbers of terrorism prosecutions in dubious cases such as those tallied by the *Intercept*. Reports suggest the FBI is riddled with institutional bias against Muslims and Islam. In 2011, reporter Spencer Ackerman discovered the FBI was training its agents to believe “mainstream” Muslims are “violent and radical.”⁶⁴ The climate of hostility toward Islam at the bureau is so bad that even Muslim FBI agents aren't exempt from it, and instead are subject to a culture of fear and suspicion. “It's a cancer,” one of them told Ackerman in 2017.⁶⁵

The FBI has worked to develop a network of unpaid informants throughout all reaches of U.S. society, with its sights sharply focused on Muslim communities and their houses of worship.⁶⁶ In at least two cases, FBI programs the bureau described as “community outreach” were later found to be principally intelligence-gathering operations, targeting Somali immigrant communities in Minneapolis and American Muslims in San Francisco.⁶⁷ The FBI has even used immigration status as a coercive instrument to try to force people to inform for the bureau.⁶⁸ But when the FBI dangles citizenship in exchange for cooperation, it doesn't always work out well;⁶⁹ and when it's done using the informants, the FBI can help get them deported.⁷⁰

These surveillance efforts by the FBI and other law enforcement agencies were made even worse by an Obama-era Department of Justice program, “Countering Violent Extremism” (CVE), which aimed to fold social service providers, public health workers, and education professionals into the “national security” net by offering training on how to spot so-called “radicalization” among youth, and even asking these providers to inform on young people to law enforcement.⁷¹ A CVE-related FBI operation, “Don't Be a Puppet,” asked teachers to use a video game simulation in classrooms to help indoctrinate youth against terrorist radicalization. The American Federation of Teachers fired off an angry letter in response, saying the video game “created this broad based suspicion of people based upon their heritage or ethnicity.”⁷² The Obama administration said these programs weren't aimed at Muslims, although Muslim and civil rights and civil liberties groups—and even unions like the AFT—contested those claims from the outset.⁷³

Under the Obama administration, the FBI's focus on Muslim communities, as well as its institutional culture and operational orientation, remained largely unchanged from the Bush administration, but the public rhetoric didn't reflect the “war of civilizations” approach preferable to those on the far right. Under the current administration, there's no sign the underlying programs will shift focus or targets, but the rhetoric already has become far worse.

As promised on the campaign trail, President Trump has taken to using the phrase “radical Islam” to describe the “threat” facing the United States. In the Trump era, Obama's so-called “counter-radicalization” effort, which asks teachers to look for things like criticisms of U.S. foreign policy as possible signs of terrorist sympathy,⁷⁴ is now explicitly focused

on Muslims.⁷⁵ The fig leaf maintained by the Obama administration—that the CVE program was an equal-opportunity government surveillance effort—has withered and died.

There's significant reason to believe the Trump administration's xenophobic and Islamophobic rhetoric will exacerbate existing problems with anti-Muslim bias at the FBI. And there's no reason to believe this will change under FBI director, Christopher Wray. During his confirmation hearings in July 2017, Wray was twice given the opportunity to state on the record that he would not go along with Donald Trump's campaign pledge to monitor mosques, even if he had no reason to believe there was any criminal activity occurring in them; both times, Wray refused to do so.⁷⁶

Targeting Dissent: JTTFs as Political Police Units

Muslims aren't the only target of unwarranted FBI surveillance. The dismissal of the 1970s U.S. attorney general's guidelines, which had been implemented after the public learned about J. Edgar Hoover's war on dissidents, opened up the floodgates once again to extensive FBI surveillance of First Amendment protected speech and activity. To some extent, these surveillance efforts predate the 9/11 attacks. But in the War on Terror era, the degree and intensity of JTTF spying on dissidents increased exponentially, fueled by new powers, resources, relationships, and technologies.

In 2015, a police officer in St. Paul, Minnesota, assigned to the local JTTF tracked participants in the Black Lives Matter movement.⁷⁷ The FBI has also said that PETA supports "eco-terrorism," and has investigated PETA as a possible domestic terrorist organization.⁷⁸ In 2010, just days after the Department of Justice inspector general released a report condemning FBI surveillance of Greenpeace, PETA, and Thomas Merton Center (a social justice and peace organization in Pittsburgh, named after a Trappist monk), the FBI raided the homes and offices of peace activists in Chicago and the Twin Cities.⁷⁹

These and other FBI surveillance operations targeting activists prompted civil liberties groups, in March 2016, to write leaders of the House and Senate Judiciary Committees asking for hearings to investigate the FBI's conduct. The groups were particularly concerned about the FBI's marshaling of "anti-terrorism" resources to target First Amendment-protected activity and speech:

“The FBI in particular has a well-documented history of abuse of First Amendment rights. In recent years that abuse has continued, including sending undercover agents and informants to infiltrate peaceful social justice groups, as well as surveillance of, documenting, and reporting on lawful political activity under counterterrorism authorities. Among the groups and movements recently targeted are the School of the Americas Watch (SOAW), Occupy Wall Street, Black Lives Matter, and anti-Keystone XL Pipeline activists.”⁸⁰

As recently as February 2017, the *Guardian* reported that the JTTFs were investigating Standing Rock water protectors. In at least three cases, according to civil rights lawyer Lauren Regan, JTTF members approached Standing Rock advocates in what are called “knock and talks,” without warrants or subpoenas, seeking information about their dissident activities. One of those officers was Andrew Creed, a Boston Police Department detective assigned to the Boston JTTF.⁸¹ What Creed was doing trying to interview Standing Rock water protectors, under cover of “counterterrorism” authority, and so far from Massachusetts, is unclear. What is clear is that the FBI and its JTTFs too often conflate activism that challenges powerful corporations and the government with terrorism.

Recommendations

No state or local police department should collaborate with a federal agency that has done what the JTTFs have done. Communities of color, immigrants, Muslims, and dissidents already have good reason not to trust the FBI. Those concerns predate the Trump administration, but its outright hostility towards Muslims, immigrants, and dissidents makes this divorce from federal agencies all the more urgent.

Some localities are already moving in this direction. In 2008 in San Francisco, advocates and local policy makers worked together to change the police department’s policy so that it prohibited law enforcement from collecting information about First Amendment–protected activity, unless officers have “articulable and reasonable suspicion to believe” that a target is planning to engage or is engaging in serious criminal activity.⁸² That change in policy set the stage for a more dramatic operational shift, when the SFPD formally removed its officers from the FBI’s JTTF.⁸³

On February 1, 2017, San Francisco Police Chief William Scott announced that, given the sea change in federal leadership, his officers could no longer in good faith participate on the JTTF. “When that confidence is shaken,” the Scott said, “we have to slow down for a minute and make sure that the public sees us as an organization that they can trust.”

Cities across the country should follow San Francisco’s lead: first, by establishing privacy-protective policies at the local department level (policies as described in section two of this report); and second, by cutting ties with federal agencies and programs such as the JTTFs when they do not follow similar civil liberties guidelines. Furthermore, state and local officials should mandate that if any of their police officers are deputized as federal agents to work on federal task force operations must abide by state and local law, not federal law, when the former is more protective of civil rights and privacy. Our state and local police departments should not facilitate deportation, the use of immigration status as a coercive tool to force cooperation with law enforcement, unconstitutional surveillance, or racial or religious profiling. Unfortunately, partnerships with federal agencies like the JTTFs enable all of those things.

Implementing Local Checks against the Expansion of the Techno-Surveillance State

Information-sharing policies and federal task force operations aren’t the only means by which state and local police have been integrated into the national security architecture. The acquisition of cutting-edge surveillance technology at the state and local level, frequently assisted by federal grant programs, has allowed federal agencies a deeper and more penetrating view into life in our cities and towns than ever before.

There are only about 35,000 FBI employees nationwide,⁸⁴ but there are nearly one million police officers.⁸⁵ When the federal government equips state and local law enforcement with biometric data collection and other surveillance tools, it exponentially expands its reach into our communities.

Simple, common sense policy solutions at the city and county level can ensure the types of surveillance technologies that facilitate this expansion of federal power are only adopted after rigorous public debate, and with democratic oversight and strict transparency requirements in place to regulate their use. In many cases, when communities have a full and open debate about the costs and benefits of adopting new surveillance technologies, elected officials will vote to pass on their adoption. In others, communities will be able to implement policies restricting data collection and sharing, to protect vulnerable community members from federal overreach.

So far, in most of the country, the opposite is happening.

Usually in secret, law enforcement agencies across the country have spent the past fifteen or so years arming themselves as if they were miniature military intelligence outfits. Federal grant programs from the Department of Homeland Security and the Department of Justice have funded, to the tune of billions of dollars, state and local acquisitions of surveillance tools such as license plate readers, biometric fingerprint readers, cell phone tracking devices, surveillance cameras, listening devices, and even proprietary “predictive policing” software. Many of these technologies collect information never before available to state and local cops, and sometimes in an indiscriminate and dragnet fashion. Too often, a failure to require basic privacy policies to govern the use of these tools and the data they produce has left the door open to federal agents rummaging around in the private comings and goings of residents of cities and towns across the country—even when there’s no reason to believe the persons monitored are suspected of crimes.

For example, license plate readers allow law enforcement to collect huge quantities of location information showing where drivers have been, and when.⁸⁶ These data are collected without any targeted criminal suspicion, and without any judicial oversight. Many local license plate reader databases are accessible by federal agencies. In Vermont, for example, license plate readers owned by state and local law enforcement send data to a centralized, statewide database. Over an eighteen-month period in 2012–13, sixty-one license plate readers operating in the state captured nearly eight million scans of drivers’ whereabouts.⁸⁷ At least once during that time period, information from this database was shared with U.S. Border Patrol.⁸⁸ A privacy impact assessment from the Northern California fusion center states that its license plate reader database may be accessed by law enforcement agencies with “authorized law enforcement and public safety purposes,” leaving the door open to sharing with ICE and the FBI.⁸⁹

Electronic fingerprint and iris scanning readers also facilitate the transfer of sensitive personal information from state and local law enforcement to federal authorities. In 2014, the NYPD announced it would spend \$160 million to buy 35,000 handheld electronic fingerprint readers and 6,000 tablets enabling “fingerprint scanning, as well as enhanced data collection in the field.”⁹⁰ In 2012, the NYPD faced criticism for delaying the processing of arrestees who refused iris scans as part of the booking process.⁹¹ The NYPD is notoriously secretive about its internal surveillance operations, but there’s no reason to believe the department won’t make its biometric data available to the FBI upon request, or even on an ongoing, automatic basis.⁹²

Local department acquisitions of technologies such as license plate, iris scanning, and fingerprint readers often fly under the radar unless groups such as the ACLU or journalists dig around and investigate what’s happening behind the scenes. But sometimes, efforts to keep surveillance technology acquisitions secret are orchestrated, conspiracy-style, by the federal government. In 2015, for example, it became known that the FBI forced police departments to sign nondisclosure agreements before acquiring cell phone tracking “Stingray” devices.⁹³ These NDAs barred local law enforcement from

telling the public, including officers of the court, about the existence of the technology. In at least one case, in Baltimore, this secrecy agreement forced a local prosecutor to drop key evidence in a criminal prosecution because it came from a Stingray, the use and existence of which the FBI didn't want to acknowledge in open court.⁹⁴

When state and local police departments acquire surveillance technologies in secret, civil liberties violations are inevitable. In Baltimore, the police bought a Stingray device in total secrecy, without even informing the city council. Acting in secret, the department used the technology thousands of times in criminal investigations. It wasn't until the department's widespread use of the technology became public that a defense attorney was able to challenge the practice in court, leading to a Maryland appellate court ruling requiring probable cause warrants for cell phone tracking.⁹⁵ Had the existence of the device remained secret, as the FBI had planned, the local department likely would have continued using it without warrants in criminal investigations, in violation of the Fourth Amendment rights of thousands of Baltimore residents.

Recommendations

Local governments can fight back against the transfer of huge quantities of information about residents from the local to the federal level—and the corrosive secrecy that enables this violation of privacy—by instituting local laws and policies requiring democratic transparency, oversight, and accountability over the surveillance technology acquisition process.

In 2016, officials in Santa Clara County, California, working with advocates including the ACLU, instituted such an ordinance. The Northern California ACLU describes what that ordinance requires:

1. **Informed Public Debate & Board Approval at Earliest Stage of the Process**—Public notice, production and distribution of an easy-to-understand Surveillance Impact Report and opportunity for meaningful public input prior to seeking funding or otherwise moving forward with surveillance technology proposals;
2. **Determination by Board That Benefits Outweigh Cost and Concerns**—The Board expressly consider costs (fiscal and civil rights) and determines whether surveillance technology is appropriate before moving forward;
3. **Robust Surveillance Use Policy Approved by Board**—Board approval of a Surveillance Use Policy with robust civil rights, civil liberties, and security safeguards for all existing and new surveillance technology; and
4. **Ongoing Oversight & Accountability**—Proper oversight of surveillance technology use and accountability through annual reporting and public review by the Board.⁹⁶

In August 2017, the City of Seattle passed a similar law, beefing up an existing ordinance on the books since 2013.⁹⁷ Organizers in more than fifty cities across the country, including Oakland, California, New York City, and Cambridge, Massachusetts, are working to pass similar local laws. The ACLU has a model ordinance and resources available online that elected officials at the local level across the country can use to implement similar policy reforms.⁹⁸

Transparency isn't just important for its own sake, as a necessary prerequisite for democratic decision-making; it also often leads to better decisions. When communities find out police departments intend to buy surveillance technologies, they can take part in a public dialogue about the wisdom of adopting the specific tools. Oftentimes that transparency directly results in a change of direction at police departments.

In Boston, for example, when the public learned about the Boston Police Department's plan to buy a social media surveillance system for \$1.4 million, people were outraged. An ACLU-driven local advocacy campaign ultimately succeeded in stopping the department's plans. In January 2017, the police commissioner announced he would scrap the request for proposals for the controversial system.⁹⁹

The best way to prevent unlawful surveillance and the integration of state and local law enforcement into the federal intelligence architecture is to stop the secrecy surrounding the acquisition of new surveillance tools. And the best way to ensure transparency and accountability to local demands is to require it through local law.

Instituting Fair Information Practices at State and Local Government Agencies

During his campaign and after his electoral victory, Donald Trump promised to create a national registry of Muslims.¹⁰⁰ The federal government's deportation machine is in high gear, threatening sanctuary cities with aggressive immigration enforcement operations targeting undocumented people and mixed-status families.¹⁰¹ In the face of these and other threats from the federal government, the national surveillance and data-sharing apparatus left behind by the Obama administration presents numerous challenges for cities and states seeking to defend the most vulnerable at the local level. In many circumstances, the federal government relies on information collected by state and local governments. That's a good thing, when the federal government aims to provide services or funding to people in the states. But information sharing can also cause substantial harm to the personal liberty and even safety of people who are targeted by repressive federal government measures.

Recent state policy decisions pertaining to registry of motor vehicle databases provide a good example of how state government initially can err—and then correct their mistakes—when it comes to instituting fair information practices.

In June 2016, a Government Accountability Office report revealed that the FBI had agreements with at least sixteen states to access drivers' license images stored in state registry of motor vehicles databases.¹⁰² The purpose of these agreements is to grant the FBI the ability to use these databases as facial recognition lineups. According to the 2016 GAO report, at least eighteen other states were in negotiations with the FBI to establish similar agreements.

The increasing use of facial recognition technology by federal agencies relying on state and local databases is a crisis states must immediately address. As Jake Laperruque of The Constitution Project has observed, "the FBI's Next Generation Biometric Identification Database and its facial recognition unit, FACE Services, can already search for and identify nearly 64 million Americans, from its own databases or via its access to state DMV databases of photo IDs." The end result of this information sharing could very well be the end of privacy and anonymity in public. As Laperruque writes, soon the "government will be able to find out who you are, where you've been and when, and who you've associated with simply by putting your name into a search bar."¹⁰³ In signing agreements to share drivers' license images with the FBI, states are enabling one of the most troubling and far-reaching surveillance programs in the history of the country.

In Vermont, as it turned out, the agreement the state made to grant the FBI access to its state drivers' license database violated state law. When the ACLU became aware of it, advocates pushed state policymakers to reverse course and end FBI access to the massive data trove of Vermonters' facial images. But across the country, even if they don't expressly violate state laws, these agreements with the FBI violate fair information practices guidelines cautioning against using information collected for one purpose for a totally different purpose. In this case, information collected for the purpose of providing drivers with licenses is being used in the equivalent of a massive, federal mug-shot lineup. When people sign up for a drivers' license, they do not consent to or knowingly submit to inclusion in such a line-up.¹⁰⁴

In some cases, local governments can prevent the misuse of information about populations at higher risk for federal government repression, such as undocumented persons, by creating alternative information practices. In New York City, for example, immigrants rights advocates long fought for municipal identification cards, partially as a means of assisting undocumented people in their daily lives. The advocates said these cards would enable New Yorkers—documented and not—to access city services and to obtain library cards, open bank accounts, and visit their children in school. The New York Civil Liberties Union urged the city to attach benefits to the municipal identification cards, to encourage a diverse range of New Yorkers to apply for them. That way, if citizens and undocumented people sought the IDs, the cards wouldn't be a proxy for someone's citizenship status.

Unfortunately, when legislation authorizing the municipal ID system came up for a vote in July 2014, the New York affiliate of the ACLU couldn't support it. As the NYCLU wrote, the bill

“provides for the city to copy and store people’s most sensitive documentation, like pay stubs, social security numbers, and even their children’s educational records. In this bill, the city has not done enough to protect those documents from being used by law enforcement. The NYPD, FBI, DHS and others can request these documents without having to show probable cause. . . . While the NYC ID will bring benefits to many people, we are disappointed that the city is inviting New Yorkers to gamble with the stakes as high as prosecution or even deportation.”¹⁰⁵

Government agencies as a matter of course must collect, maintain, and share information in order to fulfill their missions. But how they do that matters—not only for protecting individual security, but also for ensuring civil rights and liberties.

One often overlooked thing state and local governments can do to protect vulnerable communities is to follow fair information practices. That may sound dull, but its implications for protecting civil rights and civil liberties—particularly after a crisis like 9/11 or a drastic change in political leadership—are enormous.

Fair information practices can play a critical role at times like this, ensuring that information collected for one purpose won’t be used for another, and mandating that individuals have the power to access and correct information about themselves. In an age of “big data” and algorithmic decision-making, rules such as these and other fair information practices and principles are central to keeping our communities safe from federal government overreach.¹⁰⁶

Recommendations

City and state agencies should review their existing data protection policies and procedures, and where necessary, make changes to align them with fair information privacy practices. The Organization for Economic Cooperation and Development’s (OECD) landmark information privacy guidelines are an important touchstone that should serve as the basis for all data privacy policies and regulations. These rules, formally called the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,¹⁰⁷ known as the OECD Fair Information Practices, require the following:

1. **Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject
2. **Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
3. **Purpose Specification Principle:** The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. **Use Limitation Principle:** Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [section 3] except a) with the consent of the data subject; or b) by the authority of law.
5. **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
6. **Openness Principle:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. **Individual Participation Principle:** An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
8. **Accountability Principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.

State, county, and municipal government agencies across the United States collect extremely sensitive information about hundreds of millions of people in the course of their daily business. Fair information practices should guide how these agencies collect, store, share, and purge these sensitive data.

A 2017 report from Harvard's Berkman-Klein Center for Internet and Society provides even more detailed advice for local governments, using a risk and benefit model.¹⁰⁸ Governments should use both the OECD's guidelines and the Berkman report as resources in establishing sensible, privacy-protective policies that will enable agencies to fulfill their missions while doing the utmost to protect local residents from federal overreach.

Additionally, as NYCLU maintained in the case of NYC ID, state, county, and municipal agencies must implement policies requiring judicial search warrants before disclosing information to law enforcement. Too often, agencies use vague language enabling the disclosure of information to law enforcement without warrants. When governments collect sensitive information about their residents, they must ensure this information is walled off from law enforcement search and seizure absent a showing of probable cause. Doing so will protect both citizens and undocumented people from government fishing expeditions predicated on someone's race, religion, or First Amendment protected speech or association.

In Massachusetts, the introduction of all electronic tolling on the MassPike presented an opportunity for activists to push for the adoption of fair information practices to the sensitive location information collected by the state's Department of Transportation, MassDOT. While the final MassDOT data policy didn't explicitly require that law enforcement obtain warrants to get access to stored location data, the department included, for the first time ever, a data retention schedule, requiring that information be deleted when it's no longer needed for tolling purposes. These types of policies are critical interventions state and local governments can make to ensure they aren't inadvertently putting their residents at risk by amassing enormous and sensitive data troves about them. If the data don't exist, they can't be exploited or misused by the federal government or anyone else.

Conclusion

Across the United States, cities and towns large and small are struggling to protect low-income people, people of color, and immigrants from a federal actions that seem to grow crueler and more vicious by the day. But inspiring progressive rhetoric about "resistance" from well-meaning politicians isn't enough. Those elected officials must match deed to word. This report provides a roadmap that, if followed, will align constituents' desires at the state and local level with concrete policy reforms to make real the promise of freedom and civil rights for all.

Policymakers across the country will find vocal support for these reforms among their constituencies. In New York City, activists formed the Coalition to End Broken Windows to demand the city stop “quality of life” policing, divest from police, and invest in communities of color. The coalition uses a mix of public education, protest, and direct advocacy to raise awareness about and demand changes to policing in New York City. In June 2017, the coalition co-sponsored a Town Hall event in Brooklyn, where elected officials were held to account for the actions of the NYPD. Among attendees was Brooklyn District Attorney Eric Gonzalez. The coalition also organizes #SwipeItForward, a public education and advocacy campaign to encourage New Yorkers to share their Metrocards with other riders. Every time New Yorkers swipe it forward, they make sure a low-income person doesn’t face the threat of arrest for jumping a turnstile—and they learn about the extreme racial disparities in arrest rates for turnstile jumping in the city.¹⁰⁹

Likewise, in Boston, activists are organizing to demand that the Boston Police Department change its policy to forbid the collection and sharing of information about people who are not suspected of criminal activity. A coalition comprised of immigrants’ rights, religious, civil rights, and community groups has united to demand the Boston police stop sharing information with federal agencies about people who aren’t suspected of crimes, because the information sharing puts Boston residents at grave risk of deportation or harassment.¹¹⁰ The activists are also calling for the Boston police to withdraw from the FBI’s Joint Terrorism Task Force. One of the tactics the coalition is using is to highlight the distance between rhetoric and policy in the city. The Mayor and police commissioner have publicly spoken in defense of the city’s immigrant population, but those nice words ring hollow if police policy allows law enforcement to share information about Boston residents that can put them in harm’s way.¹¹¹

Organizers from Cambridge, Massachusetts to Berkeley, California are fighting for local laws to require a transparent, democratic public process before law enforcement can buy new surveillance technologies. Those efforts have borne fruit in places such as Santa Clara County, California and Seattle, Washington, where local elected officials worked with advocates to institute bold, progressive, local law reform to rein in secret surveillance operations.

For people who care about civil rights and civil liberties, these are challenging times. But despite the bluster and regressive policy coming from the White House, people across the country have substantial power to shape the present and the future from the ground up. The federal government has a lot of influence, but that influence has limits. And particularly in the criminal justice context, laws and policies at the state and local level are often more important than their federal counterparts. As this report demonstrates, state and local officials can strategically throw sand in the gears to protect their communities from a malicious federal administration. Doing so will have the benefit of strengthening civil rights and civil liberties for all people for generations, no matter who is in power at the federal level.

Rhetoric alone won't protect vulnerable residents from the excesses of federal agencies. It's time for state and local policy makers to step up and protect their constituencies by working with impacted communities to institute the bold policy reforms laid out in this report.

The ACLU of Massachusetts

This report is co-published in partnership with with the ACLU of Massachusetts.

The ACLU of Massachusetts—a private, nonpartisan organization with more than 72,000 supporters across the Commonwealth and over 100,000 online activists—is a state affiliate of the national ACLU. We defend the principles enshrined in the Massachusetts Declaration of Rights as well as the U.S. Constitution and Bill of Rights. Learn more about the history of the ACLU of Massachusetts, the range of issues we cover, and the national ACLU's work and history.

Notes

1. Brad Heath, "Racial gap in US arrest rates: 'Staggering disparity,'" *USA Today*, November 18, 2014, <https://www.usatoday.com/story/news/nation/2014/11/18/ferguson-black-arrest-rates/19043207/>.
2. Esther Yu Hsi Lee, "Immigration arrests at New York courthouses up 900 percent, advocates say," *Think Progress*, November 15, 2017, <https://thinkprogress.org/courthouse-arrests-immigrants-900-percent-b15d5155d5bf/>.
3. "Arresting immigrants at schools, hospitals and courthouses isn't just cold-hearted, it's counterproductive," editorial, *Los Angeles Times*, March 16, 2017, <http://www.latimes.com/opinion/editorials/la-ed-trump-ice-courts-20170316-story.html>. Tom Dart, "Fearing deportation, undocumented immigrants weary of reporting crime," *Guardian*, March 23, 2017, <https://www.theguardian.com/us-news/2017/mar/23/undocumented-immigrants-wary-report-crimes-deportation>. Elisha Waldman, "Immigration fears are preventing children from getting medical care," *Washington Post*, June 30, 2017, https://www.washingtonpost.com/opinions/immigration-fears-are-preventing-children-from-getting-medical-care/2017/06/30/66f92d76-4c8f-11e7-9669-250d0b15f83b_story.html. Jonathan Blitzer, "After an immigration raid, a city's students vanish," *New Yorker*, March 23, 2017, <https://www.newyorker.com/news/news-desk/after-an-immigration-raid-a-citys-students-vanish>.
4. Sari Horwitz, "How Jeff Sessions wants to bring back the war on drugs," *Washington Post*, April 8, 2017, https://www.washingtonpost.com/world/national-security/how-jeff-sessions-wants-to-bring-back-the-war-on-drugs/2017/04/08/414ce6be-132b-11e7-ada0-1489b735b3a3_story.html?utm_term=.0e9e816c8696.
5. "Statement on Trump's Border Militarization Proposal," National Immigration Law Center, January 5, 2018, <https://www.nilc.org/2018/01/05/trump-border-militarization-proposal/>.
6. Jamiles Lartey, "Sessions slams visa lottery: 'It tells us nothing about who is entering this country,'" *Guardian*, November 2, 2017, <https://www.theguardian.com/us-news/2017/nov/02/sessions-slams-visa-lottery-it-tells-us-nothing->

about-who-is-entering-this-country.

7. Laurel Wamsley, "As It Makes More Arrests, ICE Looks for More Detention Centers," *NPR News*, October 26, 2017, <https://www.npr.org/sections/thetwo-way/2017/10/26/560257834/as-it-makes-more-arrests-ice-looks-for-more-detention-centers>.
8. See: "The War on Marijuana in Black and White," ACLU, June 2013 <https://www.aclu.org/issues/mass-incarceration/smart-justice/war-marijuana-black-and-white>. The Prison Policy Initiative's 2017 "whole pie" analysis of U.S. incarceration shows local jails, state prisons, and federal prisons incarcerate large numbers of people for low-level offenses such as public order, drug, and property crimes. Racial disparities persist in incarceration rates across jurisdictions. See: Peter Wagner and Bernadette Rabuy, "Mass Incarceration: The Whole Pie," Prison Policy Initiative, March 14, 2017, <https://www.prisonpolicy.org/reports/pie2017.html>. See also: German Lopez, "These maps show the war on drugs is mostly fought in poor neighborhoods," *Vox*, April 16, 2015, <https://www.vox.com/2015/4/16/8431283/drug-war-poverty>.
9. Michelle Ye Hee Lee, "Yes, U.S. locks up people at a higher rate than any other country," *Washington Post*, July 7, 2015, https://www.washingtonpost.com/news/fact-checker/wp/2015/07/07/yes-u-s-locks-people-up-at-a-higher-rate-than-any-other-country/?utm_term=.8a831a43fbdc.
10. Serena Marshall, "Obama Has Deported More People Than Any Other President," *ABC News*, August 29, 2016, <http://abcnews.go.com/Politics/obamas-deportation-policy-numbers/story?id=41715661>. It is worth noting, however, unlike previous administrations, Obama started counting people apprehended at the border as "deportations," thus inflating the numbers quite a bit. See Brian Bennett, "High deportation figures are misleading," *Los Angeles Times*, April 1, 2014, <http://www.latimes.com/nation/la-na-obama-deportations-20140402-story.html>.
11. John Gramlich, "Federal prison population fell during Obama's term, reversing recent trend," January 5, 2017, Pew Research. <http://www.pewresearch.org/fact-tank/2017/01/05/federal-prison-population-fell-during-obamas-term-reversing-recent-trend>.
12. "Secure Communities" page, ICE, Department of Homeland Security website accessed August 3, 2017, <https://www.ice.gov/secure-communities>.
13. Another part of S-Comm involved equipping state and local police and sheriffs departments with electronic finger print readers, to facilitate the expedited transfer of these data. Learn more about federal assistance for state and local surveillance technologies in section four of this report.
14. Gretchen Gavett, "Why Three Governors Challenged Secure Communities," *PBS Frontline*, October 18, 2011, <http://www.pbs.org/wgbh/frontline/article/why-three-governors-challenged-secure-communities/>.
15. "Secure Communities and ICE Deportation: A Failed Program?" TRAC Immigration, <http://trac.syr.edu/immigration/reports/349/>.
16. Ibid.
17. FBI crime statistics, 2015, https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/persons-arrested/arrestmain_final.pdf.
18. Nicholas Kulish et al., "Immigration Agents Discover New Freedom to Deport under Trump," *New York Times*, February

- 25, 2017, <https://www.nytimes.com/2017/02/25/us/ice-immigrant-deportations-trump.html?mcubz=1>.
19. “The Deported: Immigrants Uprooted from the Country They Call Home,” Human Rights Watch, December 5, 2017, <https://www.hrw.org/report/2017/12/05/deported/immigrants-uprooted-country-they-call-home>.
20. Ibid.
21. As described in section two, people needn’t even be arrested in order for local police to endanger them by entangling them in the deportation matrix.
22. “Fact Check: Donald Trump’s Speech on Immigration,” NPR, August 31, 2016, <http://www.npr.org/2016/08/31/492096565/fact-check-donald-trumps-speech-on-immigration>.
23. Immigration Customs Enforcement, “Fiscal Year 2017 ICE Enforcement and Removal Operations Report,” February 2018, Department of Homeland Security. <https://www.ice.gov/sites/default/files/documents/Report/2017/iceEndOfYearFY2017.pdf>.
24. This category includes offenses like illegal entry, illegal reentry, and false claim to US citizenship.
25. These numbers don’t add up to 100 percent because some people faced charges for or were convicted of multiple crimes.
26. Shaila Dewan, “The Collateral Victims of Criminal Justice,” *New York Times*, September 5, 2015, https://www.nytimes.com/2015/09/06/sunday-review/the-collateral-victims-of-criminal-justice.html?_r=0.
27. In a 2004 study, men who told employers they had a drug conviction were 50 percent less likely to get a callback from a potential employer. The researcher concluded that employers used the convictions as “a proxy for reliability and trustworthiness and a broader range of concerns beyond simply whether they would be aggressive.” See: Binyamin Appelbaum, “Out of Trouble, but Criminal Records Keep Men Out of Work,” *New York Times*, February 28, 2015, https://www.nytimes.com/2015/03/01/business/out-of-trouble-but-criminal-records-keep-men-out-of-work.html?mcubz=1&_r=0.
28. Data from ACLU public records request to Massachusetts Executive Office of Public Safety and Security.
29. “Every 25 Seconds: The Human Toll of Criminalizing Drug Use in the United States,” ACLU and Human Rights Watch, 2016, https://www.hrw.org/sites/default/files/report_pdf/usdrug1016_web.pdf.
30. Ian Urbina, “Blacks are singled out for marijuana arrests, study finds,” *New York Times*, June 3, 2013, <http://www.nytimes.com/2013/06/04/us/marijuana-arrests-four-times-as-likely-for-blacks.html>.
31. Others have fought back. The Cities of Chicago and San Francisco and the state of California have filed lawsuits against the DOJ to challenge Trump’s executive order on sanctuary cities.
32. FBI crime statistics, 2015, https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/persons-arrested/arrestmain_final.pdf.
33. Nationwide, approximately 64 percent of the jail population is awaiting trial. In other words, most people in jail in the United States haven’t been convicted of a crime. Incarcerating people pretrial costs the United States about \$17 billion per year. See: Christopher Ingram, “Why we spend billions to keep half a million unconvicted people behind bars,” *Washington Post*, June 11, 2015, https://www.washingtonpost.com/news/wonk/wp/2015/06/11/why-we-spend-billions-to-keep-half-a-million-unconvicted-people-behind-bars/?utm_term=.ba63cf491ba1.

34. Samantha Schmidt, "Denver fights back against Trump's deportation crackdown with surprisingly simple change in law," *Washington Post*, May 24, 2017, https://www.washingtonpost.com/news/morning-mix/wp/2017/05/24/denver-fights-back-against-trumps-deportation-crackdown-with-surprisingly-simple-change-in-law/?utm_term=.96160f87614e.

35. The "broken windows" policing strategy assumes that by arresting people for low-level offenses like breaking windows, police will interrupt violence before it breaks out. The theory says that by making arrests for small offenses, police will be able to prevent more serious crimes. See: Sarah Childress, "The Problem with 'Broken Windows' Policing," *PBS Frontline*, June 28, 2016, <https://www.pbs.org/wgbh/frontline/article/the-problem-with-broken-windows-policing/>, <http://www.pbs.org/wgbh/frontline/article/the-problem-with-broken-windows-policing/>.

36. Mark Mazetti, "Burglars Who Took on FBI Abandon Shadows," *New York Times*, January 7, 2014, <https://www.nytimes.com/2014/01/07/us/burglars-who-took-on-fbi-abandon-shadows.html>.

37. The Church Committee produced a voluminous report to document its findings. The Church Committee's full report is available in a searchable archive at the Mary Ferrell Foundation website, <https://www.maryferrell.org/php/showlist.php?docset=1014>.

38. "The Eight Signs of Terrorism," Colorado Department of Homeland Security and Emergency Management, site accessed July 15, 2017, <https://www.colorado.gov/pacific/dhsem/eight-signs-terrorism>.

39. ACLU, "ACLU Eye on the FBI: Documents reveal lack of privacy safeguards and guidance in government's 'Suspicious Activity Report' systems." <https://www.aclu.org/other/aclu-eye-fbi-documents-reveal-lack-privacy-safeguards-and-guidance-governments-suspicious-0?redirect=national-security/aclu-eye-fbi-documents-reveal-lack-privacy-safeguards-and-guidance-governments>.

40. Zwerdling, Daniel, et al, "Under Suspicion At The Mall Of America," September 7, 2011, *NPR News*. <http://www.npr.org/2011/09/07/140234451/under-suspicion-at-the-mall-of-america>.

41. See, for example, Barton Gellman and Sam Adler-Bell, "The Disparate Impact of Surveillance," The Century Foundation, December 21, 2017, <https://tcf.org/content/report/disparate-impact-surveillance/>.

42. Statement of FEMA deputy administrator Richard Serino, "Lessons Learned from the Boston Marathon Bombings: Preparing for and Responding to the Attack," Committee on Homeland Security and Government Affairs, July 10, 2013, https://www.fema.gov/media-library-data/20130726-1923-25045-1176/lessons_learned_from_the_boston_marathon_bombings_preparing_for_and_responding_to_the_attack.pdf.

43. One predictable result of this policy is law enforcement surveillance of and intelligence collection on First Amendment protected dissident activity. In 2012, the ACLU of Massachusetts and the National Lawyers Guild, Massachusetts Chapter, published a report based on so-called "intelligence reports" from the BRIC. These reports showed that BRIC officers and analysts had spent significant time infiltrating, monitoring, and documenting the perfectly legal protest activities of antiwar groups throughout the Greater Boston area, labeling them as homeland security threats and "extremists."

44. See Ali Winston, "You may be in California's gang database and not even know it," *Reveal news*, March 23, 2016, <https://www.revealnews.org/article/you-may-be-in-californias-gang-database-and-not-even-know-it/> and Meredith Broussard, "When Cops Check Facebook," *Atlantic*, April 19, 2015, <https://www.theatlantic.com/politics/archive/2015/04/when-cops-check-facebook/390882/>

- <https://www.theatlantic.com/politics/archive/2015/04/when-cops-check-facebook/390882/>.
45. Dan McGowan, "Mayor Elorza signs Providence police reform ordinance into law," June 8, 2017, WPRI, <http://wpri.com/2017/06/08/mayor-elorza-signs-providence-police-reform-ordinance-into-law/>.
46. Maxine Bernstein, "Portland police to halt, purge all gang designations," *Oregonian*, September 8, 2017, http://www.oregonlive.com/portland/index.ssf/2017/09/portland_police_to_halt_purge.html.
47. FBI Budget Request for Fiscal Year 2018. <https://www.fbi.gov/news/testimony/fbi-budget-request-for-fiscal-year-2018>.
48. Joint Terrorism Task Force Memorandum of Understanding between the FBI and Boston Police Department, 2007, <https://www.documentcloud.org/documents/238313-boston.html>.
49. Cyrus Farivar, "FBI didn't need warrant for stingray in attempted murder case, DOJ says," *Ars Technica*, July 12, 2017, <https://arstechnica.com/tech-policy/2017/07/fbi-didnt-need-warrant-for-stingray-in-attempted-murder-case-doj-says/>.
50. Brennan Center for Justice, "Just What Is An FBI Investigation? A Fact Sheet," New York University School of Law, May 20, 2013, <https://www.brennancenter.org/analysis/just-what-fbi-investigation-fact-sheet>.
51. Cora Currier, "Hidden loopholes allow FBI agents to infiltrate political and religious groups," *Intercept*, January 31, 2017, <https://theintercept.com/2017/01/31/hidden-loopholes-allow-fbi-agents-to-infiltrate-political-and-religious-groups/>.
52. Cora Currier, "Despite anti-profiling rules, the FBI uses race and religion when deciding who to target," *Intercept*, January 31, 2017, <https://theintercept.com/2017/01/31/despite-anti-profiling-rules-the-fbi-uses-race-and-religion-when-deciding-who-to-target/>.
53. Dia Kayyali, "Newly Revealed NSA Program ICREACH Extends the NSA's Reach Even Further," Electronic Frontier Foundation, September 3, 2014, <https://www.eff.org/deeplinks/2014/09/newly-revealed-nsa-program-icreach-extends-nsas-reach-even-further>.
54. Cora Currier, "CIA and NSA Dossiers Are Available to the FBI in the Absence of Any Crime, Raising Privacy Questions," *Intercept*, January 31, 2017, <https://theintercept.com/document/2017/01/31/domestic-investigations-and-operations-guide/fbi-can-pull-cia-and-nsa-dossiers-in-absence-of-any-crime-raising-privacy-questions/#page-1>.
55. In at least two cases, with Tamerlan Tsarnaev and Omar Mateen, men who committed terrorist attacks had been previously investigated by JTTFs. Some experts, including former FBI agent Mike German, say part of the problem is that the FBI allows its agents to investigate people who aren't suspected of criminal activity—leading to wasted resources and a failure to focus on men who may be truly dangerous, like Mateen and Tsarnaev, both of whom had been arrested for domestic violence prior to their attacks. In other words, if FBI agents are free to harass Muslims simply because they are Muslim, and to monitor police reform activists who've never been connected to any kind of violence, they are unable to effectively identify people who may be true threats. See: Michael German, "Former FBI Agent: Our Terrorism Strategy Isn't Working," *TIME*, July 5, 2016, <http://time.com/4389947/fbi-national-security/>.
56. "Trial and Terror," *Intercept*, September 3, 2017, <https://trial-and-terror.theintercept.com/>.
57. Allen Cone, "FBI director warns of 'terrorist diaspora' after Islamic State crushed," UPI, September 27, 2016, http://www.upi.com/Top_News/US/2016/09/27/FBI-director-warns-of-terrorist-diaspora-after-Islamic-State-crushed/6791474995369/.
58. Andrew Shaver, "You're more likely to be fatally crushed by furniture than killed by a terrorist," *Washington Post*,

November 23, 2015, <https://www.washingtonpost.com/news/monkey-cage/wp/2015/11/23/youre-more-likely-to-be-fatally-crushed-by-furniture-than-killed-by-a-terrorist/>.

59. Gary Younge, "Trump fears terrorists, but more Americans are shot dead by toddlers," *Guardian*, February 8, 2017, <https://www.theguardian.com/commentisfree/2017/feb/08/trump-muslim-terrorists-gun-violence-america-deaths>.

60. Mirren Gidda, "Most terrorists in the US are right-wing, not Muslim: report," *Newsweek*, June 22, 2017, <http://www.newsweek.com/right-wing-extremism-islamist-terrorism-donald-trump-steve-bannon-628381>.

61. Melissa Jeltsen, "Who Is Killing American Women? Their Husbands and Boyfriends, CDC Confirms," *Huffington Post*, July 21, 2017, http://www.huffingtonpost.com/entry/most-murders-of-american-women-involve-domestic-violence_us_5971fcf6e4b09e5f6ccea87.

62. Kade Crockford, "Former assistant FBI director: to keep budgets high we must keep fear alive," Privacy Matters, ACLU of Massachusetts, January 28, 2015, <https://privacysos.org/blog/former-fbi-assistant-director-to-keep-budgets-high-we-must-keep-fear-alive/>.

63. Trevor Aaronson, "The Informants," *Mother Jones*, September 2011, <http://www.motherjones.com/politics/2011/07/fbi-terrorist-informants/>.

64. Spencer Ackerman, "FBI teaches agents: 'mainstream' Muslims are 'violent, radical,'" *Wired*, September 14, 2011, <https://www.wired.com/2011/09/fbi-muslims-radical/>.

65. Spencer Ackerman, "Muslims inside FBI describe culture of suspicion and fear: 'It is cancer,'" March 22, 2017, the *Guardian*. <https://www.theguardian.com/us-news/2017/mar/22/fbi-muslim-employees-discrimination-religion-middle-east-travel>.

66. David Morgan, "Review: How East Germans spied on themselves, in 'Karl Marx City,'" April 1, 2017 *CBS News*. <http://www.cbsnews.com/news/review-how-east-germans-spied-on-themselves-in-karl-marx-city/>.

67. Cora Currier, "Spies among us: How community outreach programs to Muslims blur lines between outreach and intelligence," *Intercept*, January 21, 2015, <https://theintercept.com/2015/01/21/spies-among-us-community-outreach-programs-muslims-blur-lines-outreach-intelligence/>; "FOIA documents show FBI using 'mosque outreach' for intelligence gathering," ACLU, March 27, 2012, <https://www.aclu.org/news/foia-documents-show-fbi-using-mosque-outreach-intelligence-gathering>.

68. Cora Currier, "Revealed: The FBI's secret methods for recruiting informants at the border," *Intercept*, October 5, 2016, <https://theintercept.com/2016/10/05/fbi-secret-methods-for-recruiting-informants-at-the-border/>.

69. Recent reporting suggests Boston marathon bomber Tamerlan Tsarnaev may have been motivated by frustration with the FBI. Boston based reporter Michelle McPhee's latest book raises the following hypothesis about Tsarnaev's radicalization: He worked with the FBI as an informant, in part because the bureau promised him expedited citizenship approval in exchange for his collaboration. But when those promises stalled, Tsarnaev became enraged and began plotting his attack. See: Jamie Bologna and Meghna Chakrabarti, "Unanswered questions about Tamerlan Tsarnaev," *WBUR*, June 15, 2017, <http://www.wbur.org/radioboston/2017/06/15/tsarnaev-mcphee-fbi>.

70. Trevor Aaronson, "When informants are no longer useful, the FBI can help deport them," *Intercept*, January 31, 2017, <https://theintercept.com/2017/01/31/when-informants-are-no-longer-useful-the-fbi-can-help-deport-them/>.

71. Brennan Center for Justice, "Countering Violent Extremism (CVE): A Resource Page," New York University School of Law, July 13, 2017, <https://www.brennancenter.org/analysis/cve-programs-resource-page>.
72. Mazin Sidahmed, "FBI's Don't Be a Puppet game targets Muslim youth, teachers' union says," *Guardian*, August 26, 2016, <https://www.theguardian.com/us-news/2016/aug/26/fbi-dont-be-a-puppet-terrorism-muslim-teachers>.
73. Jaweed Kaleem, "Obama's Anti-Extremist Strategy Criticized As Wrongly Singling Out Muslims," *Huffington Post*, February 13, 2015, http://www.huffingtonpost.com/2015/02/13/muslims-white-house-summit-extremism_n_6680952.html.
74. Naureen Shah, "Terrorist or ... Teenager?" *Slate*, November 12, 2014, http://www.slate.com/articles/news_and_politics/politics/2014/11/justice_department_s_countering_violent_extremism_progr.
75. Julia Edwards Ainsley, Dustin Volz and Kristina Cooke, "Exclusive: Trump to focus counter-extremism program solely on Islam - sources," *Reuters*, February 1, 2017, <https://www.reuters.com/article/us-usa-trump-extremists-program-exclusiv-idUSKBN15G5VO>.
76. Neema Singh Guliani, "The Man Likely to Be the New FBI Director Won't Commit to Not Spying on Mosques and Muslim Leaders in America," ACLU, July 21, 2017, <https://www.aclu.org/blog/washington-markup/man-likely-be-new-fbi-director-wont-commit-not-spying-mosques-and-muslim>.
77. Lee Fang, "Why was an FBI Joint Terrorism Task Force tracking a Black Lives Matter protest?" *Intercept*, March 12, 2015, <https://theintercept.com/2015/03/12/fbi-appeared-use-informant-track-black-lives-matter-protest/>.
78. "FBI/JTTF Spying," ACLU, <https://www.aclu.org/other/fbi-jttf-spying>.
79. Amy Goodman, "FBI Raids and the Criminalization of Dissent," *Truth Dig*, September 29, 2010, http://www.truthdig.com/report/item/fbi_raids_and_the_criminalization_of_dissent_20100928.
80. Bill of Rights Defense Committee et al letter to Judiciary Committee Chairs, March 8, 2016, https://drive.google.com/file/d/0B_3GXBIfLVB8OUpoOGYyUzdROFk/view.
81. Sam Levin, "Revealed: FBI terrorism taskforce investigating Standing Rock activists," *Guardian*, February 10, 2017, <https://www.theguardian.com/us-news/2017/feb/10/standing-rock-fbi-investigation-dakota-access>.
82. San Francisco Police Department, General Order 8.10, <http://sanfranciscopolice.org/sites/default/files/FileCenter/Documents/24722-DGO%208.10%20100108%20police%20commission%20members.pdf>.
83. Stephen McNeil, "End Your Cities' Participation in the FBI's Joint Terrorism Task Force Now!" American Friends Service Committee, April 5, 2017, <https://www.afsc.org/story/end-your-cities%E2%80%99-participation-fbi%E2%80%99s-joint-terrorism-task-force-now>.
84. Frequently Asked Questions, FBI, <https://www.fbi.gov/about/faqs>.
85. FBI crime statistics, 2013, <https://ucr.fbi.gov/crime-in-the-u.s/2013/crime-in-the-u.s.-2013/tables/table-74>.
86. Catherine Crump, et al, "You Are Being Tracked," ACLU, July 2013 <https://www.aclu.org/feature/you-are-being-tracked>.
87. Taylor Dobbs, "License Plate Scanners Raise Privacy Concerns, But Do They Help Police?" *VPR*, September 24, 2014, <http://digital.vpr.net/post/license-plate-scanners-raise-privacy-concerns-do-they-help-police#stream/0>.
88. "2013 LPR Release of Information," *VPR*, July 2014, <http://mediad.publicbroadcasting.net/p/vpr/files/201409/2013->

ALPR-releases-vermont-vpr.pdf.

89. "Initial Privacy Impact Assessment for Automated License Plate Reader Technology," Northern California Regional Intelligence Center, undated, <https://ncric.org/html/NCRIC%20ALPR%20PIA.PDF>.
90. Yoav Gonen, Kevin Fasick, Larry Celona and Bruce Golding, "NYPD to get \$160M mobile fingerprint device," *New York Post*, October 23, 2014, <https://nypost.com/2014/10/23/nypd-to-get-160m-mobile-fingerprint-device/>.
91. Colin Moynihan, "Some Who Decline an Optional Iris Photo Are Kept Longer in Jail, Critics Say," *New York Times*, February 12, 2012, <http://www.nytimes.com/2012/02/13/nyregion/new-objections-to-nypds-iris-photographing-program.html>.
92. The FBI's "Next Generation Identification" biometric database aims to collect fingerprints, face scans, iris scans, scent, gait, and other biometric data on as many people as possible, worldwide. The database contains information submitted by state and local law enforcement agencies, as well as by the State Department, Department of Homeland Security, and U.S. military. See: Jennifer Lynch, "The FBI's Next Generation Identification: Bigger and Faster but Much Worse for Privacy," Electronic Frontier Foundation, July 8, 2011, <https://www.eff.org/deeplinks/2011/07/fbis-next-generation-identification-database>.
93. Jessica Glenza and Nicky Woolf, "Stingray spying: FBI's secret deal with police hides phone dragnet from courts," *Guardian*, April 10, 2015, <https://www.theguardian.com/us-news/2015/apr/10/stingray-spying-fbi-phone-drag-net-police>.
94. Cyrus Farivar, "Prosecutors drop key evidence at trial to avoid explaining "stingray" use," *Ars Technica*, November 18, 2014, <https://arstechnica.com/tech-policy/2014/11/prosecutors-drop-key-evidence-at-trial-to-avoid-explaining-stingray-use/>.
95. Justin Fenton, "Maryland appellate court: warrant required for 'stingray' phone tracking," *Baltimore Sun*, March 31, 2016, <http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-stingray-court-decision-20160331-story.html>.
96. Nicole Ozer, "Santa Clara County Passes Landmark Law to Shut Down Secret Surveillance," ACLU of Northern California, June 8, 2016, <https://www.aclunc.org/blog/santa-clara-county-passes-landmark-law-shut-down-secret-surveillance>.
97. "Seattle adopts nation's strongest regulations for surveillance technology," ACLU of Washington, August 8, 2017, <https://www.aclu-wa.org/news/seattle-adopts-nation%E2%80%99s-strongest-regulations-surveillance-technology>.
98. "Community Control over Police Surveillance," ACLU, <https://www.aclu.org/feature/community-control-over-police-surveillance>.
99. Travis Andersen, "Boston police will think twice about monitoring social media," *Boston Globe*, January 14, 2017, <https://www.bostonglobe.com/metro/2017/01/14/boston-police-scrap-plans-buy-social-media-monitoring-software-for-now/rIzAn4e5oQJJSwM4BSkt5H/story.html>.
100. Abby Phillip and Abigail Hauslohner, "Trump on the future of proposed Muslim ban, registry: 'You know my plans,'" *Washington Post*, December 22, 2016, https://www.washingtonpost.com/news/post-politics/wp/2016/12/21/trump-on-the-future-of-proposed-muslim-ban-registry-you-know-my-plans/?utm_term=.d4d5587b3bb1.
101. Mallory Simon and Alex Marquardt, "This is the face of deportation: A dad with no criminal record, an American wife and two kids," CNN, July 27, 2017, <https://amp.cnn.com/cnn/2017/07/27/politics/connecticut-family-deportations/index.html>.

102. Kade Crockford, "Getting a new drivers license? Brace yourself for FBI facial recognition analysis," *Privacy Matters*, ACLU of Massachusetts, June 21, 2016, <https://privacysos.org/blog/getting-a-new-driver/>.
103. Jake Laperruque, "Preserving the Right to Obscurity in the Age of Facial Recognition," The Century Foundation, October 20, 2017, <https://tcf.org/content/report/preserving-right-obscurity-age-facial-recognition/>.
104. For more information about the threat posed by unregulated facial recognition technology, see: Jake Laperruque, "Preserving the Right to Obscurity in the Age of Facial Recognition," The Century Foundation, October 20, 2017, <https://tcf.org/content/report/preserving-right-obscurity-age-facial-recognition/>.
105. NYCLU statement on the NYC municipal ID bill," New York Civil Liberties Union, July 9, 2014, <https://www.nyclu.org/en/publications/statement-nyclu-regarding-new-york-city-municipal-id-bill>.
106. Fair information practices also protect us from other threats to our security and privacy, like internal agency data abuses, data breaches, ransom ware, and other forms of malicious hacking.
107. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," Organisation for Economic Cooperation and Development, 2013, <https://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>.
108. Ben Green, Gabe Cunningham, Ariel Ekblaw, Paul Kominers, Andrew Linzer, and Susan Crawford, "Open Data Privacy Playbook," Berkman Klein Center for Internet and Society, Harvard University, February 27, 2017, <https://cyber.harvard.edu/publications/2017/02/opendataprivacyplaybook>.
109. Coalition to End Broken Windows website, <https://endbrokenwindows.org/video>.
110. Disclosure: The ACLU and the author of this report are involved in this organizing campaign.
111. Kade Crockford, "From Gang Allegations to Deportation: How Boston Is Putting Its Immigrant Youth in Harm's Way," *In Justice Today*, Fair Punishment Project, Harvard Law School, January 18, 2018, <https://injusticetoday.com/from-gang-allegations-to-deportation-how-boston-is-putting-its-immigrant-youth-in-harms-way-de3b0edc9327>.



Kade Crockford, Contributor

Kade Crockford is director of the Technology for Liberty Program at the ACLU of Massachusetts. In 2017, Kade was named an MIT Media Lab Director's Fellow.
