A HOOVER INSTITUTION ESSAY

Facial Recognition as a Less Bad Option

JANE BAMBAUER

Aegis Series Paper No. 2107

This essay does the unthinkable—it defends the police use of facial recognition technology to identify suspects in crime footage or to locate individuals with outstanding warrants. I argue that the perils that flow from facial recognition can be mitigated through sensible limits without banning the technology, and that in any case, the risks of facial recognition are less bad than the options police have *without* its use. In other words, acknowledging the potential costs of police use of facial recognition, I make the case that such use is still warranted.

In broad strokes, my argument goes as follows: (1) to the extent criminal justice reformers have political capital to spend, it should be spent reducing criminal liability and sentences for most crimes while increasing the probability that criminal conduct will be detected so that crime rates stay low; and (2) facial recognition is a valuable tool for increasing the probability of detection because it reduces the discretion that police officers have as compared to other forms of surveillance. Put differently, and all things being equal, it is more efficient *and fairer* for police to run a photograph through facial recognition software to identify candidate suspects than to try to identify the suspect using witnesses or to solve the case without using the image.

The essay unfolds in three sections. Section 1 builds a case for increasing the use of surveillance technologies as part of a grand bargain for criminal justice reform. Those who believe that the American criminal justice system currently relies on excessively harsh punishment to keep crime rates low (a point I will argue for below) should be willing to increase surveillance and criminal detection in exchange for changes in punishment or in the substance of the criminal code. That is, given a choice among potential criminal justice reforms, a responsible policy maker should do whatever possible to dramatically reduce criminal sentencing and the indirect effects of incarceration. Since this can only be accomplished by either increasing the capacity to detect criminal conduct using surveillance tools or allowing the crime rates to creep back up, an honest account of criminal justice reform must confront trade-offs. Much of the political discourse ignores or wishes away the inescapable trilemma between the probability of enforcement, the harshness of punishment, and crime rates. If we acknowledge the trade-offs between surveillance, punishment, and crime, then the prohibitions of new surveillance technologies have an obvious

practical and political cost: they will make decriminalization and sentencing reform more difficult. To put it positively, instead of negatively, I will argue that we should consider embracing new surveillance tools like facial recognition systems so that they can be used as part of a strategic package of reforms that more directly benefit communities harmed by both crime and policing.

Section 2 of this essay argues that facial recognition technologies are more valuable than the average surveillance tool because they rely on only limited amounts of police discretion. Facial recognition is used today in a crime-driven, rather than suspect-driven, manner.[1] Because police start with photographic or video evidence from a crime scene or from an arrest file and use facial recognition to work out toward a suspect, the tool has the potential to decrease bias and arbitrariness that can taint investigations when they start with one or more identified suspects and attempt to build up to probable cause. Facial recognition technologies can also reduce the high stakes of arrest. If a suspect resists arrest but does not seem to present a physical danger to the police or others, a police officer may be less likely to use force against the suspect if he has increased confidence that a facial recognition system will find the suspect again soon. (Likewise, the suspect himself is less likely to resist for the same reason.)

Finally, although the use of facial recognition presents real risk related to the invasion of privacy and racially biased error, these criticisms probably fail the "Compared to what?" test. Thus, the moral calculus of police use of facial recognition is quite complex, notwithstanding the consensus among thought leaders that it should be banned.

I. The Inescapable Trilemma: Crime, Detection, and Punishment

Crime is terrible, and so is its detection and punishment.[2]

In the United States, crime rates are quite low in historical terms. Violent crimes have basically dropped by half since the early 1990s, and property crimes have dropped even more dramatically.[3] And although Black and Hispanic Americans are more likely to become victims of crime than White Americans, homicide rates plummeted for all racial groups between 1993 and 2014 and continues to be fairly low in historical terms.[4] In 1993, one out of every fifteen Black Americans was the victim of a violent crime at some point during the year,[5] but in 2018 the figure was one in eighty.[6] For those of us interested in criminal reform, this is excellent news because there is some buffer—perhaps some room to spare—to experiment with reforms even if they cause temporary increases in crime rates.[7] On the other hand, recent spikes in crime (particularly homicide) during 2020 and 2021 suggest this window of opportunity may close as voters and constituents return to a state of anxiety and put pressure on the criminal justice system to drive crime rates back down.[8]

Economist Gary Becker famously modeled crime with a simple formula determined by the probability of conviction and the severity of punishment.[9] Becker was writing at the height of the rational actor approach to legal design; because it was much easier for the state to ratchet up punishment than to catch more perpetrators, his work persuaded many politicians to manage crime through tough sentencing.[10]

The sparseness of Becker's model for crime rates leaves much to be desired. There is ample evidence that crime has a range of social and economic causes and that there is a limit to the cold rational actor model.[11] Nevertheless, there is little reason to doubt that detection and punishment of crime are important factors that influence the amount of crime in a given community at a given time,[12] and these factors are more directly under the control of a politically accountable mayor, police chief, or state legislature than many of the other social and cultural determinants.

On severity of punishment, the United States stands out with a brutal and grimly indifferent penal system unmatched by any of our political allies. We use incarceration intensively. In France and the United Kingdom, a criminal who punches a person in the nose would probably be sentenced to less than six months in jail.[13] The same conduct in the United States would likely result in a sentence of about three years.[14] Moreover, no outsider would mistake our prisons for institutions of rehabilitation. To the contrary, the entire sentence is usually carried out in a facility that is punishing, with drab quarters, humiliating toilet and bathroom facilities, and rancid food. Once released, the negative consequences continue as the housing and labor markets penalize criminal convicts.

All of this might be justified if the Becker model of criminal forecasting were valid, but it is not. In fact, punishment has a U-shaped relationship to recidivism, where no punishment and significant periods of incarceration both tend to increase the odds that a perpetrator will recidivate. This relationship is due in part to the criminogenic effect that the prison experience has. A recent study by Amanda Agan, Jennifer Doleac, and Anna Harvey provides some of the most compelling proof that exposure to prison increases recidivism rather than decreasing it.[15] In terms of general deterrence, the length of a prison sentence has swiftly diminishing marginal returns on the likelihood that a person who has not yet committed a crime will decide to exercise restraint.[16] On the other hand, crime rates can be reduced through incapacitation rather than deterrence—that is, by imposing very long sentences on first-time convicts.

Thus, punishment reduces crime in two situations: either as part of a system with high probability enforcement (in which case punishment can be mild) or as part of a system that attempts to incapacitate criminals by confining them for as long as society will tolerate (which necessitates that the punishment be harsh).

• • •

This brings us to the second Becker factor—the probability of detection of criminal conduct. On this factor, the United States is in bad shape. Less than half of the violent crimes reported to the police result in an arrest and referral for prosecution and for property crime, the figure is under 20 percent.[17] Moreover, most crime is not even reported. Only about half of violent crimes are ever reported to the police, and about one-third of property crimes. In other words, more than half of victim-based crimes in the United States don't even make it to the denominator in the clearance rates. Together, the low likelihood of reporting and the low clearance rates means that the probability a criminal will be prosecuted for any particular incidence of violence is about 20 percent. (The figure for property crime is 7 percent.)[18] America uses haphazard enforcement: occasional and harsh.[19]

Unlike the severity of punishment, there is abundant evidence that crime rates are very responsive to the probability of enforcement.[20] There is also some weaker evidence that the swiftness of enforcement—the "celerity"—makes a difference. The detection, identification, and arrest of suspects requires surveillance, of course, and the privacy intrusions from surveillance constitute the third leg of the inescapable trilemma.

II. Surveillance as the Least Bad Option

Let's step back and observe the three legs of the miserable trilemma: surveillance, punishment, and crime. Holding all else constant,[21] a policy goal to reduce any one of these will require tolerance of an increase in at least one of the others. So, at the outset, the trilemma illuminates why we should develop a tolerance (perhaps even a desire) to increase surveillance.

Tolerance for surveillance serves two purposes. First, and most importantly, it will be necessary if we want to reduce punishment without a spike in crime rate. This is especially relevant for reformers and lawmakers interested in rapid decarceration and sentencing reductions. Since rising crime rates have already taxed the public's tolerance for crime, the only responsible and politically palatable course is to increase the chance of detection and enforcement of serious crimes, which will require either more intensive use of surveillance technologies that are already available or the development of new surveillance technologies. For the purposes of this section, I will treat both of those options (more use of extant surveillance systems or development of new surveillance tech) under the single concept of increased surveillance.

The clash between American values in privacy and security is most pronounced at the early stages of investigation, before police have probable cause to arrest a particular individual. Norms and the Fourth Amendment offer quite a bit of latitude for

investigation after the police have reached the probable cause threshold. At that point, the police can conduct full-blown searches and collect communications information (within the bounds and limitations of the warrant requirement, of course). But before probable cause is established, police must build cases using information that is acquired outside the scope of the technical definition of a "search." It is the pre–probable cause stage of an investigation where advances in surveillance technologies are most likely to improve detection. But this is also the stage of investigation that is most embroiled in a battle over the scope and future of the Fourth Amendment.

Facial recognition technologies sit right at the center of this clash. With the possible exception of drones, facial recognition is the technology most reviled by progressives and civil libertarians alike.[22] Yet it seems to me that legal bans on facial recognition will be a Pyrrhic victory because poor criminal detection will leave the harsh punishment equilibrium in place.

Progressive concerns over the inhumanity and inequity in mass incarceration and libertarian concerns about unchecked state power would benefit more directly from decriminalization and from greatly reducing sentences for the crimes that are left on the books. I have argued that legislators or courts should set ceilings that are significantly lower than average sentences today in order to constrain and properly calibrate the state's imposition of punishment on the unlucky minority of criminal actors who are caught.[23] That is, if the state is constrained by law or constitutional interpretation from detaining or imprisoning individuals at all based on minor infractions, or from levying long sentences for anything other than the most serious and violent offenses, then the *threat* of state surveillance is reduced.

Political pressure to ban surveillance tools might make sense as a second-best solution if decriminalization and reduced sentencing is politically infeasible, but the risk is that the strategy can lock out the first-best solution—the low-penalty/high-detection solution. Indeed, as murder rates have risen over the last year and a half, the decriminalization and police reform movements are already more politically controversial than they were a couple years ago. If crime rates continue to rise while detection is capped or suppressed through new legal constraints on technology, politically accountable decision makers are likely to continue to rely on incapacitation (i.e., very long prison sentences) to manage crime.

The second reason to tolerate surveillance more than the other options is that surveillance is likely to be a necessary component for alternatives to criminal justice systems anyway. If we expect the government to handle social problems related to drugs, mental health, or gangs using public health models of intervention, then those, too, will depend on surveillance to gauge risk, monitor compliance, and create positive feedback loops for individuals in nonpunitive treatment programs. Indeed, in the

case of health crises, Americans sometimes want *more* surveillance if the data might improve public health.[24]

To summarize, the least bad approach to criminal justice would involve dramatic reductions in the civil or criminal penalties for misconduct combined with a greatly increased probability of detection. And the best alternatives to a criminal justice system are also likely to require surveillance. On these assumptions, and assuming that the risks of abuse of new surveillance tools can be effectively managed (which requires its own commitment to surveilling and policing the police), there is reason to embrace effective surveillance as part of a first-best or least bad approach to managing crime.

What is much less clear at this point is how we could possibly achieve the first-best solution given the legal and practical constraints we have today. The US Constitution places minimal constraints on crime rates and sentencing length, but it places significant restrictions on surveillance. That is, there is no explicit constitutional duty for the government to keep crime below a particular threshold. The crime leg of the tripod can be as large as circumstances, local government, and the voting public allow it to get. Police rarely have an affirmative duty to respond to crime.[25] The punishment leg is also effectively unconstrained: statutory and constitutional limits on the severity of punishment are so lax that they create no meaningful constraint. The surveillance leg is the only one limited by constitutional and statutory rules, and police often operate up to the bounds of the legal limits. When law enforcement does find a way to expand that leg of the tripod—by adopting a new surveillance technology—the public is often quick to react and demand legal restrictions on its use. Thus, for the foreseeable future, the reformers have only two legs to work with—they can reduce punishment and incarceration (causing a rise in crime rates), or they can reduce crime (by increasing punishment).

So far, I have discussed the benefits of facial recognition as a generic tool of surveillance and detection. But I will go further. Even among possible surveillance tools, facial recognition has some advantages over traditional policing. Facial recognition is no worse and often better than other investigation tools when it comes to criminal justice problems related to privacy, use of force, and bias.

III. Facial Recognition as a Least Bad Form of Surveillance

Police must rely on some form of information-gathering to build an initial case against a suspect or to locate a person with an outstanding warrant. Whatever they do to gather incriminating information will constitute some form of surveillance and will raise the possibility of an intrusive privacy invasion.

In typical accounts of law enforcement surveillance, observations of clear evidence of crime are not in themselves socially harmful. If a police officer observes a person committing a crime, that observation is generally thought to implicate no legally recognized privacy interest.[26] However, whatever surveillance is used will usually collect more information than strictly relevant and necessary for the investigation or prosecution of a crime. When a police officer patrols a public street or enters a home with consent or pursuant to a warrant, whatever evidence of criminality is discovered there is accompanied with the observation of lots of other irrelevant information related to perfectly legal behavior. The revelation of those licit details is the privacy harm. That information can be used later to harass or embarrass an individual, or to pursue a personally or politically motivated investigation. Even if negative consequences never occur, the loss of control over information related to private (and legal) conduct constitutes a dignitary loss.

Facial recognition technologies present privacy risks, but they are modest compared to other forms of investigation (at least, as the technology is typically used today).[27] In the use cases that are most likely to proliferate across police departments, facial recognition is used when police have already collected photographic or video evidence from the scene of the crime, or where the police have already sought and received a warrant based on probable cause from other sources and are pursuing the final step of identifying or locating a suspect. This differs from investigations that involve tailing a suspect for a period of time or talking to confidential sources because the amount of extraneous information gathered by the police is limited. Police will not observe the inside of a suspect's car or home and often will not even know his movement patterns. Other than identity, little is revealed by facial recognition technologies per se. They are privacy-preserving compared to other forms of information-gathering.

Of course, licit details will be revealed anytime facial recognition falsely identifies a suspect who is then subjected to an arrest or probable cause-based search. Much like the drug-sniffing dog,[28] facial recognition is far from infallible, and the false match error will lead to privacy invasions. But no investigation tool is free from error, and facial recognition outperforms the accuracy rates of eyewitnesses and PC-based warranted searches by a large margin.[29] The same is true for racial differences in error rates: while some facial recognition technologies are more likely to produce false matches for photographs of Black faces,[30] the gap in false match error is likely to be reduced over time, and in any event may already be less bad than the difference in false match error from human systems of suspect identification.[31] Moreover, unlike traditional policing methods, facial recognition technology can be calibrated to only produce a match when the risk of a false match is below a certain threshold (ensuring equal false positive rates across race).[32]

Facial recognition surveillance also differs in important respects from suspect-driven investigations. In suspect-driven investigations, police have developed suspicion (or a hunch) around a particular individual and focus their observations on the suspect in order to develop a case. Suspect-driven investigations are propelled by the theories of police officers and proceed at their discretion. By contrast, police have less control over the results of facial recognition investigations that stem from evidence at a crime scene.[33] If facial recognition identifies a wealthy or politically connected individual as the suspect of a crime, it will be much more difficult for police to fail to pursue that lead than in a case where the police use informants or witnesses as the main source of identification. Like geofencing techniques (where GPS data is used to identify who was at the scene of a crime at the appropriate time), police cannot exert control over which individuals will wind up within the scope of suspicion. Techniques that involve starting from the facts of a crime and working toward an identity are sometimes criticized for failing to limit the number of people who wind up in the ambit of potential suspicion,[34] but at a conceptual level, it's hard to fault investigative techniques that begin from the facts of a crime.

None of this is meant to suggest that facial recognition is free from bias or abuse. First, police will decide which crime scene images should be subjected to facial recognition. They will have to decide, for example, whether to pursue arrest and prosecution of violent or destructive rioters at a Black Lives Matter protest or at a pro-Trump rally; this decision is subject to justified criticism if the standards between the two differ. Likewise, in the case of locating identified individuals with outstanding search warrants, police departments will decide which public and online spaces to monitor for potential matches. Still, these types of enforcement decisions about which crimes to investigate and where to look for outstanding suspects will have to be made regardless of the form of surveillance used to carry out the investigation.

In fact, there is reason to believe that such an effective technology as facial recognition would reduce, rather than increase, the chance that police will focus enforcement on underprivileged communities. The role of discretion in decision-making related to which types of crimes to prosecute or which parts of a town to monitor are themselves a product of limited capacity to detect crime. A police department's limited resources give it the power and excuse to pick and choose between different law enforcement missions and different locations of scrutiny. If cheap, privacy-preserving surveillance tools were readily available, there would be no reason to use it for some crime footage and not for others, or to scan for people with outstanding arrest warrants in some neighborhoods and not others. The decision to concentrate the tool on minority neighborhoods would be highly suspect (even if the neighborhoods have higher crime rates) if there is no significant cost to deploying them everywhere, or in locations where more people congregate. Thus, while a marginally useful surveillance tool might exacerbate racial disparities in criminal investigation and enforcement rates,

a cheap and highly efficacious criminal detection tool can reduce them (by increasing detection across the board).

Facial recognition can also help reduce the stakes during police encounters and seizures. Police will not need to use force to stop a suspect who is resisting arrest and attempting to flee if they are confident that the suspect will be located again very soon using facial recognition.[35] (And for the same reasons, the suspect is also less likely to flee.)

Finally, tools like facial recognition can be calibrated to report an alert only for particular types of crime. If a police department sets up facial recognition at a crowded sports stadium, they could program the app to alert on individuals who have outstanding warrants for only a subset of serious crimes. If there are doubts that the police would constrain their use in this way, courts or lawmakers could restrict use to solving serious crimes rather than banning the technology outright.[36]

Some fear the government will begin to combine facial recognition with a network of surveillance camera footage to record and store the location and movement history of law-abiding individuals in identified form indefinitely, and for unlimited purposes. But Fourth Amendment cases like *Carpenter v. United States* and possibly *United States v. Jones* seem to effectively foreclose that scenario.[37] The city of Baltimore, for example, has already had a police program dismantled on Fourth Amendment grounds because the city was keeping aerial surveillance footage of the whole city for up to six months.[38] And law enforcement use of automated license plate reading technologies have been approved by courts only when their use is limited to short amounts of time or to cars that are not owned by the target.[39] Persistent monitoring of movement using facial recognition would presumably be struck down for the same reasons. In any case, the network of surveillance cameras and indefinite storage of their footage rather than facial recognition technology would be the most proximate cause of risk if a stockpile of this sort of data were to be created.[40]

Conclusion: The Least Bad among Bad Options

As a society, we value freedom from government surveillance as well as freedom from crime victimization. Since law enforcement operates in the unavoidable clash between these two goals, all options are bad.

Reducing harsh criminal penalties and keeping crime rates low are, or should be, the greatest goals for American policy makers who want to reform the criminal justice system. Keeping surveillance capacities stuck at twentieth-century standards is the least important criminal justice reform goal. In other words, surveillance is the more manageable option in an unavoidable trilemma.

Among surveillance tools, compared to surveillance that gathers and retains licit details about individuals or that relies on the discretion of police, investigations that use facial recognition to match a known crime to an unidentified suspect is the best among bad options.

ACKNOWLEDGMENTS

I am very grateful to the excellent feedback on early drafts from Barry Friedman, Jack Goldsmith, Farhang Heydari, Elizabeth Joh, Orin Kerr, Jennifer Lynch, Christopher Slobogin, Mark Verstraete, Andrew Woods, and the participants of the Hoover Institution roundtable on "The Private Market and Public Surveillance." I am also indebted to the support of the University of Arizona College of Law library staff who helped me track down statistics and provided other research support.

NOTES

1 *See* Shirin Ghaffary, *How to Avoid a Dystopian Future of Facial Recognition in Law Enforcement*, Vox (Dec. 10, 2019), https://www.vox.com/recode/2019/12/10/20996085/ai-facial-recognition-police-law-enforcement-regulation (describing current law enforcement uses).

2 *See, e.g.*, David A. Anderson, *The Aggregate Burden of Crime*, 42 J.L. & Econ. 611 (1999); Aaron Chalfin & Justin McCrary, *Are U.S. Cities Under-Policed? Theory and Evidence* (National Bureau of Economic Research. Working Paper No. 18815, 2013); Kathryn E. McCollister et al., *The Cost of Crime to Society: New Crime-Specific Estimates for Policy and Program Evaluation*, 108 Drug & Alcohol Depend. 98 (2010).

3 John Gramlich, *What the Data Says (and Doesn't Say) about Crime in the United States*, Pew Rsch. Ctr. (Nov. 20, 2020), https://www.pewresearch.org/fact-tank/2020/11/20/facts-about-crime-in-the-u-s [hereinafter Gramlich 2020]; Rachel E. Morgan & Barbara A. Oudekerk, U.S. Dept. of Just., NCJ-253043, Criminal Victimization, 2018 (2019). Although crimes of all sorts (and particularly murder) have skyrocketed during the COVID-19 pandemic, the pandemic-related stress on social and economic well-being make the recent data difficult to interpret. *Compare* Paul G. Cassell, *Explaining the Recent Homicide Spikes in U.S. Cities: The "Minneapolis Effect" and the Decline in Proactive Policing*, 33 Fed. Sent'g Rep. 83 (2020), *with* Jeffrey Fagan & Daniel Richman, *Understanding Recent Spikes and Longer Trends in American Murders*, 117 Colum. L. Rev. 1235 (2017), *and* German Lopez, *The Rise in Murders in the US, Explained*, Vox (Dec. 2, 2020), https://www.vox.com/2020/8/3/21334149/murders-crime-shootings-protests-riots-trump-biden.

4 Federal Bureau of Investigation, Crime Data Explorer, https://crime-data-explorer.app.cloud.gov/pages/explorer/crime/shr (last visited Oct. 20, 2021) (focusing on "Expanded Homicide Data" from 1985 to 2020).

5 Craig A. Perkins et al., U.S. Dept. of Just., NCJ-151657, Criminal Victimization in the United States, 1993, at v (1996).

6 U.S. Dept. of Just., *supra* note 3, at 16.

7 I should note, though, that there may not be much political appetite even when crime rates are dropping since the United States, even in its lowest crime period, is still far more crime-ridden than other developed

nations. For example, 5.4 out of every 100,000 Americans were killed by homicide in 2016, whereas in France the rate was 1.4 out of every 100,000. *Victims of Intentional Homicide, 1990–2018*, United Nations Off. on Drugs & Crime, https://dataunodc.un.org/content/data/homicide/homicide-rate.

8 *See* Jeff Asher, *Murder Rose by Almost 30% in 2020. It's Rising at a Slower Rate in 2021*, N.Y. Times (Sept. 22, 2021), https://www.nytimes.com/2021/09/22/upshot/murder-rise-2020.html; Domenico Montanaro, *Rising Violent Crime Is Likely to Present a Political Challenge for Democrats in 2022*, NPR (July 22, 2021), https://www.npr.org/2021/07/22/1018996709/rising-violent-crime-is-likely-to-present-a-political-challenge-for-democrats-in.

9 Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. Polit. Econ. 169 (1968); *see also* A. Mitchell Polinsky & Steven Shavell, *The Theory of Public Enforcement of Law, in* Handbook of Law & Economics 421 (2007).

10 *See* Cass R. Sunstein et al., *Do People Want Optimal Deterrence?*, 29 J. Legal Stud. 237 (2000).

11 *See, e.g.*, Cesare Lombroso, Criminal Man (Mary Gibson & Nicole Rafter, trans., 2006) (1876) (discussing genetic theories of crime); S. J. Schoenthaler & I. D. Bier, *The Effect of Vitamin-Mineral Supplementation on Juvenile Delinquency among American Schoolchildren: A Randomized, Double-Blind Placebo-Controlled Trial*, 6 J. Alt. & Complementary Med. 7 (2000) (discussing malnutrition as a factor in crime); Civic Research Institute, The Science, Treatment, and Prevention of Antisocial Behaviors (Diana H. Fishbein ed., 1999) (reviewing evidence of the impact of alcoholism, drug use, sexual abuse, cognitive and genetic factors, and family/gender role factors); Clifford R. Shaw & Henry D. McKay, Juvenile Delinquency and Urban Areas (1942) (exploring the effect of weakened or disorganized social institutions on crime and including the roots of what would become the "broken windows" theory).

12 *See* Exec. Off. of the President, Economic Perspectives on Incarceration and the Criminal Justice System 36–40 (2016) (citing to the empirical literature finding that increased incarceration reduces crime, but less effectively than equivalent increased spending on police); Andrew von Hirsch, Doing Justice: The Choice of Punishments 61–65 (1976); Raymond Paternoster, *The Deterrent Effect of the Perceived Certainty and Severity of Punishment: A Review of the Evidence and Issues*, 42 Just. Q. 173 (1987).

13 House of Commons Library, CBP 7218, Comparative Prison Sentences in the EU, 2010 (2015), https://commonslibrary.parliament.uk/research-briefings/cbp-7218.

14 U.S. Sent'g Comm'n, *Table 15, Sentence Imposed by Type of Crime, Fiscal Year 2020, in* Sourcebook of Federal Sentencing Statistics (2020), https://www.ussc.gov/research. Note, though, that the differences for nonviolent offenses like theft appear to be smaller (<6 months in the United Kingdom compared to a median of eight months in the United States). It should also be noted that the US data is drawn from 2020 while the European data relates to 2010; however, data from the United States in 2010 leads to similar results. U.S. Sent'g Comm'n, *Table 13, Sentence Length in Each Primary Offense Category, Fiscal Year 2010, in* Sourcebook of Federal Sentencing Statistics (2010), https://www.ussc.gov/research.

15 Amanda Y. Agan et al., *Misdemeanor Prosecution* (National Bureau of Economic Research. Working Paper No. 28600, 2021).

16 Von Hirsch, *supra* note 12, at 61–65.

17 John Gramlich, *Most Violent and Property Crimes in the U.S. Go Unsolved*, Pew Rsch. Ctr. (Mar. 1, 2017), https://www.pewresearch.org/fact-tank/2017/03/01/most-violent-and-property-crimes-in-the-u-s-go-unsolved [hereinafter Gramlich 2017]; Gramlich 2020, *supra* note 3. These statistics deal with clearance rates that measure the annual number of reported cases that result in an arrest and referral for prosecution but do not take into account reported cases that are cleared in subsequent years.

18 *See* Gramlich 2017, *supra* note 17; Gramlich 2020, *supra* note 3.

19 This critique, it should be noted, dates back to the eighteenth-century work of Jeremy Bentham and Cesare Beccaria. *See* Raymond Paternoster, *How Much Do We Really Know about Criminal Deterrence?*, 100 J. Crim. L. & Criminology 765, 767–73 (2010).

20 Reviews of empirical literature consistently find that harsh sentences cannot be justified on deterrence grounds because while crime rates are highly sensitive to the probability of enforcement, the severity of punishment has no consistent effect. *See, e.g.*, Aaron Chalfin & Justin McCrary, *Criminal Deterrence: A Review of the Literature*, 55 J. Econ. Literature 5, 13–15, 23–29 (2017); Steven N. Durlauf & Daniel S. Nagin, *Imprisonment and Crime: Can Both Be Reduced?*, 10 Criminology & Pub. Pol'y 13, 17 (2011); Daniel S. Nagin, *Deterrence in the Twenty-First Century*, 42 Crime & Just. 199 (2013); Daniel S. Nagin, *Deterrence: A Review of the Evidence by a Criminologist for Economists*, 5 Ann. Rev. Econ. 83 (2013); Jeffrey Grogger, *Certainty vs. Severity of Punishment*, 29 Econ. Inquiry 297 (1991).

21 Even if we do not hold all else constant—if, for example, social disruption causes crime to increase, or if nutritional improvements cause crime to decrease—unless the change causes a dramatic shift in crime, the trade-offs between the three factors in the trilemma will still have to be made under conditions similar to those that we have today.

22 *See, e.g.*, Press Release, *Ban Dangerous Facial Recognition Technology That Amplifies Racist Policing*, Amnesty International (Jan. 26, 2021), https://www.amnesty.org/en/latest/press-release/2021/01/ban-dangerous-facial-recognition-technology-that-amplifies-racist-policing ("Facial recognition risks being weaponized by law enforcement against marginalized communities around the world . . . [T]his invasive technology turns our identities against us and undermines human rights."); *The Fight to Stop Face Recognition Technology*, Am. Civ. Liberties Union (July 15, 2021), https://www.aclu.org/news/topic/stopping-face-recognition-surveillance/ ("Face recognition surveillance presents an unprecedented threat to our privacy and civil liberties."); Press Release, *Pressley, Clarke, Tlaib Reintroduce Bill to Ban Facial Recognition Technology in Public Housing*, U.S. Congresswoman Ayanna Pressley (July 7, 2021), https://pressley.house.gov/media/press-releases/pressley-clarke-tlaib-reintroduce-bill-ban-facial-recognition-technology-public.

23 Jane Bambauer & Andrea Roth, *From Damage Caps to Decarceration: Extending Tort Law Safeguards to Criminal Sentencing*, 101 B.U. L. Rev. (forthcoming 2021).

24 Cason Schmit et al., *U.S. Privacy Laws Go against Public Preferences and Impede Public Health and Research: Survey Study*, 23 J. Med. Internet Rsch. (2021).

25 *See, e.g.*, DeShaney v. Winnebago County, 489 U.S. 189 (1989) (no constitutional duty to protect a young child from domestic abuse); Castle Rock v. Gonzales, 545 U.S. 748 (2005) (same); Riss v. City of New York, 22 N.Y.2d 579 (N.Y. 1968) (denying tort recovery to the victim of an attack who had requested police assistance multiple times). However, some state Riot Act statutes allow state and local government to be sued for failure to respond and protect others in the course of a riot. *See* Susan Glassberg, *Liability for Urban Riot Damage*, 1971 Urban L. J. 193 (1971).

26 Unless, of course, the substance of the criminal law is flawed or the penalties are too harsh. The implicit threat from surveillance is that it can lead to the enforcement of civil or criminal laws that many believe are substantively flawed (e.g., drug or immigration enforcement) or that are overpenalized (e.g., most nonviolent crimes) is a concern of high importance to me. However, faults in the substance or punishment of criminal law exist regardless of the type of surveillance used and are better addressed through decriminalization and reduction in sentences than through haphazard reductions in detection.

27 By contrast, programs that use facial recognition as part of a mass surveillance or suspect-driven investigation do not have the benefits that I describe here. As I describe below, such programs would face a constitutional challenge in the wake of *Carpenter v. United States*. Perhaps more concerning is the risk that a surveillance tool could be used by police officers in violation of internal protocols in order to harass

or exploit another person. The rogue use of police equipment is always a risk, but in the case of facial recognition software, the technology is readily available to private actors anyway. *See* Kashmir Hill, *Activists Turn Facial Recognition Tools against the Police*, N.Y. Times (Aug. 1, 2021), https://www.nytimes.com/2020/10/21/technology/facial-recognition-police.html. Thus, an officer's access to official law enforcement systems may not greatly increase the risk that a rogue agent will make inappropriate use of the tool since he may be able to use the same technology outside of work. That said, the legitimacy of the use of this and any surveillance system depends on law enforcement's willingness to hold its own agents to high standards and to avoid corruption and abuse.

28 Illinois v. Caballes, 543 U.S. 405, 411 (2005) (Souter, J., dissenting) ("The infallible dog, however, is a creature of legal fiction.").

29 False match error rates for facial recognition algorithms are now under 1 percent in ideal conditions and under 10 percent when used in the field, and one facial recognition vendor recommends law enforcement use a threshold of 95 percent confidence. William Crumpler, *How Accurate Are Facial Recognition Systems—and Why Does It Matter?*, Ctr. for Strat. & Int'l Stud. (Apr. 14, 2020), https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter. By comparison, eyewitness identification during a lineup has error rates of 20 percent or more. Gary L. Wells & John W. Turtle, *Eyewitness Identification: The Importance of Lineup Models*, 99 Psych. Bull. 320, 323 (1986).

30 Tom Simonite, *The Best Algorithms Struggle to Recognize Black Faces Equally*, Wired (July 22, 2019), https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally.

31 Race bias compared to eyewitness identification.

32 Crumpler, *supra* note 29; Simonite, *supra* note 30. The *Wired* article claims that changing the threshold in this way might violate the equal protection clause, *id.*, but given that the chance of a false match would be equalized, I have my doubts. Setting the false match rate to be equal is equivalent to ensuring that "probable cause" for Black suspects means the same thing it does for whites.

33 I have called these "crime-out" investigations. Jane Bambauer, *Other People's Papers*, 94 Tex. L. Rev. 205 (2015). Christopher Slobogin calls these "event-driven" investigations. Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. Chi. L. Rev. 317, 331, 338–40 (2008); Christopher Slobogin, *Policing, Databases, and Surveillance*, 18 Criminology, Crim. Just., L. & Soc. 70 (2017).

34 *See, e.g.*, Tim Cushing, *Government's "Reverse" Warrant Rejected by Two Consecutive Federal Judges*, Techdirt (Sept. 8, 2020), https://www.techdirt.com/articles/20200902/11565245234/governments-reverse-warrant-rejected-two-consecutive-federal-judges.shtml.

35 This is all the more true if police, too, are under greater surveillance through body-worn cameras. *See* Morgan C. Williams Jr. et al., *Body-Worn Cameras in Policing: Benefits and Costs* (National Bureau of Economic Research. Working Paper No. 28622, 2021).

36 Jeffrey Bellin has suggested that Fourth Amendment jurisprudence should mediate rules related to searches based on the severity of a crime. Jeffrey Bellin, *Crime-Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World*, 97 Iowa L. Rev. 1 (2011).

37 Carpenter v. United States, 138 S. Ct. 2206 (2018); United States v. Jones, 565 U.S. 400, 418 (2012) (Alito, J., concurring). These cases suggest tracking individuals' whereabouts for long periods of time is an intrusion on reasonable expectations of privacy under *Katz v. United States* and would not ordinarily be permissible without a warrant. Note that it is the geolocation information that is most critical. In *Maryland v. King*, the Court has suggested that analyzing data solely for the purpose of identification is not intrusive enough on its own to constitute a violation of reasonable privacy expectations (though the application to individuals who have not been arrested is not entirely clear). 133 S. Ct. 1958, 1979–80 (2013).

38 Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330 (4th Cir. 2021) (en banc).

39 *See* U.S. v. Yang, 958 F.3d 851 (9th Cir. 2020); Commonwealth v. McCarthy, 142 N.E.3d 1090 (Mass. 2020); *Commonwealth v. McCarthy: Massachusetts Supreme Judicial Court Holds That Use of Automated License Plate Readers May Constitute a Search*, 134 Harv. L. Rev. 2887 (2021) (case comment).

40 A much more likely scenario, and one which I would defend (but not here), is a system where footage is stored for a period *without* identification and used in combination with facial recognition only after probable cause has been established with respect to a targeted suspect.

The views expressed in this essay are entirely those of the author and do not necessarily reflect the views of the staff, officers, or Board of Overseers of the Hoover Institution.

hoover.org

27 26 25 24 23 22 21 7 6 5 4 3 2 1

The preferred citation for this publication is Jane Bambauer, *Facial Recognition as a Less Bad Option*, Hoover Working Group on National Security, Technology, and Law, Aegis Series Paper No. 2107 (November 4, 2021), available at https://www.lawfareblog.com/facial-recognition-less-bad-option.

About the Author

University of Arizona
James E. Rogers College of Law

JANE BAMBAUER

Jane Bambauer is a professor of law at the University of Arizona. Her research assesses the social costs and benefits of Big Data and questions the wisdom of many well-intentioned privacy laws. Her work has been published in leading legal journals.

The Jean Perkins Foundation Working Group on National Security, Technology, and Law

The Jean Perkins Foundation Working Group on National Security, Technology, and Law brings together national and international specialists with broad interdisciplinary expertise to analyze how technology affects national security and national security law and how governments can use that technology to defend themselves, consistent with constitutional values and the rule of law.

The group focuses on a broad range of interests, from surveillance to counterterrorism to the dramatic impact that rapid technological change—digitalization, computerization, miniaturization, and automaticity—are having on national security and national security law. Topics include cybersecurity, the rise of drones and autonomous weapons systems, and the need for—and dangers of—state surveillance. The group's output will also be published on the *Lawfare* blog, which covers the merits of the underlying legal and policy debates of actions taken or contemplated to protect the nation and the nation's laws and legal institutions.

Jack Goldsmith is the chair of the National Security, Technology, and Law Working Group.

For more information about this Hoover Institution Working Group, visit us online at http://www.hoover.org/research-teams /national-security-technology-law-working-group.

Hoover Institution, Stanford University
434 Galvez Mall
Stanford, CA 94305-6003
650-723-1754

Hoover Institution in Washington
1399 New York Avenue NW, Suite 500
Washington, DC 20005
202-760-3200

HOOVER INSTITUTION