Privacy at Great Cost: 
An Argument Against Collecting and Storing DNA and Location Data and Other Mass Surveillance

Mark Tunick

Abstract
Mass surveillance involves the collection and storage of vast amounts of information, such as DNA samples from the general population, or location data from cell phones towers, aerial surveillance, and other sources, to then be used when a future crime occurs. For example, DNA from a crime scene could be checked against the database to identify a suspect; location data could identify suspects who were at the scene of a crime. Mass surveillance implicates important privacy interests, but it would surely reduce crime and therefore has been defended by those who reject “privacy at all costs.” I also reject “privacy at all costs.” However, while agreeing that privacy is a value that must be balanced against competing values, I argue that requiring everyone to provide a sample of their DNA or keeping track of everyone’s movements would limit the autonomy of vast numbers of people who there is no reason to suspect will pose a threat, and though such policies would make society safer, that is not worth the cost to individual autonomy. After explaining why individuals can have a substantial interest in privacy even if they are not guilty of a crime, by linking that interest to the value of individual autonomy, and drawing on a political theory of liberal pluralism to restrict what counts as a legitimate public interest that might justify mass surveillance, I articulate a method of balancing these competing interests that is more feasible than a utilitarian approach.

Keywords: privacy; surveillance; DNA; rights; autonomy; utilitarianism; liberal pluralism; legal moralism

I. Introduction

Recently, a consultant who advises governments and corporations on matters of privacy ethics, Reid Blackman, published an essay in The New York Times warning of the dangers of “privacy at all costs.” Blackman criticizes the technology used in Signal App that allows users to employ end-to-end encryption to send text messages that cannot be read by third parties, including the company that runs Signal App or
the government. The encryption technology prevents the company or the government from even knowing the identity of the app’s users and who is talking to whom. The company is founded on what, to Blackman, is a misguided belief: that state or corporate surveillance undermines an uncompromisable value of privacy, and that privacy must be protected at all costs.\footnote{Blackman focuses on “informational privacy,” or the ability to control who has access to information about oneself.} He does not think criminals should be able to restrict access to information about their crime, such as the fact that they are planning it, or boast about it after the fact. At first glance, Blackman makes a persuasive point. Even though Signal App has many beneficial uses—it enables journalists to communicate with confidential sources, for example—it also enables murderers, child abusers, terrorists, and other criminals to evade detection.

Others have also pointed to the dangers of “privacy at all costs,” and defend surveillance policies that would collect massive data that could be stored and used in the future, when needed to help solve crimes.\footnote{Consider two examples of mass surveillance. First consider the collection and storage of DNA samples. By storing DNA samples from a large population, DNA evidence at a crime scene can be cross-checked against the database of samples to identify suspects. For example, police in Maryland collected a DNA sample from Alonzo King, after he was arrested in 2009 for menacing a group with a shotgun. The DNA sample was used, three months after his arrest, to see if it matched DNA found in connection with an unsolved rape of 2003. It did, and he was convicted of rape. For defenders of a massive DNA database, the larger the collection of samples is the better. Having DNA on file of people charged with a crime would be better than just having DNA samples of convicted criminals; and if our only goal is public safety, we should collect DNA samples of everyone. Not only would it be easier to catch criminals, but potential criminals would be more hesitant to commit crimes. A second example of mass surveillance is the collection and storage of data on people’s location. By drawing on location data from cellphone towers, GPS devices, and ALPR (automatic license plate readers), and video images from aerial surveillance as well as from cameras placed on building exteriors or utility poles or worn by police officers, and on records of whose laptops, tablets and phones connect to Wi-Fi routers or were used to publish posts on apps like Facebook, authorities can determine who is at a crime scene or learn vital details about the crime. Some of the participants in the January 6, 2021 riots at the U.S. Capitol were identified by the fact that they live streamed video on Facebook from the U.S. Capitol at the time of the riots, and a federal court permitted the use of this data to identify them, data that was obtained without a search warrant. More recently, video footage from a SkyCop pole camera and police-body-worn cameras showed that several Memphis police officers savagely beat Tyre Nichols following a traffic stop, though he posed no immediate threat to them: only because of the footage was the prosecutor able to charge the officers with}
homicide. Even more recently, an ALPR was used to identify a car seen leaving the scene of the firebombing of a synagogue in New Jersey, leading to a suspect’s arrest.

Those who defend the collection and storage of massive amounts of such data point to the obvious benefit: mass surveillance helps us catch criminals. They might deflect concerns about privacy by noting that merely collecting and storing data for future use is not the same as disclosing the information to others, let alone widely disseminating it to the public. Defenders of mass surveillance might further claim that gathering and storing information about you does not even constitute surveillance. The stored information about you, such as your DNA, or location and movements, would in theory only be accessed when a query is made to determine whose DNA in the database matches DNA at a crime scene or who was at or near the crime scene at the time of a crime. If the information about you that is stored in the database is not a match, it will be ignored. If you are not a match, you will never be identified and, the argument goes, have not been observed or surveilled.

We should reject the claim that merely collecting and storing DNA or location data for future use is not really surveillance. Collecting and storing the data enables the government to deduce what you do. If you were a suspect, the database could be searched for information about you: for example, face recognition software could be used to find all images of you stored in the database, to track your location over time. If the government lacked a suspect, it could identify who was at or near the crime scene or whose DNA matches DNA found at the crime scene. In either scenario, the government finds out what you do. Even if it uses the data to establish that you were not at a crime scene, it draws conclusions about your activities based on information it collected about you, and that constitutes surveillance.

Those who defend the collection and storage of mass DNA and location data may concede that it constitutes surveillance but deny that legitimate privacy interests are implicated, merely if the government runs a query in which you are not identified as a match. In that case, your identity is never made known, even to the individual running the query. Why should innocent people with no crime to hide care about having their private information stored, if no one ever observes it?

One reason people who have committed no crime should be concerned is that government queries that access the database could call attention to you, even if you are not guilty of a crime: you may have been near the scene of a crime, having nothing to do with it, but do not want attention given to what you were doing there. Or the government might unreasonably expand its conception of what crimes warrant access to the database. It might come to declare that protesting outside of government buildings or assembling to practice a new religion that it regards as a threat are crimes, and could use the database to punish you for acts that should be permitted in a free society. Or it might use predictive policing algorithms on the DNA database to tag individuals it believes are prone to aggressive behavior in order to more closely monitor them, even though these algorithms may be biased and unreliable.
A second reason innocent people who have committed no crime should care is that the database could be hacked into by individuals who could make use of the information to harm them. Even those who are innocent of a crime have interests in keeping information about themselves private, for reasons I discuss below.\textsuperscript{11} The database could also be accessed illegitimately by government employees who use the data for self-interested purposes rather than the public good. In either case, identifiable information could be disseminated that you could legitimately want to keep private.

Defenders of surveillance might reply that we can adopt back-end protections to ensure access to the data is strictly controlled and used only to conduct “crime-out” investigations, which are investigations prompted by the occurrence of a crime needing to be solved. As one defender of such surveillance argues, “Can we turn our backs on the ability to save lives” that a “store-everything world” would provide?\textsuperscript{12} The hope is that with use and disclosure limitations we could trust authorities to ensure that sensitive information it may store, such as DNA evidence revealing someone’s disposition to diseases, will not get into the hands of prospective employers or insurance companies and be used to discriminate against them illegally; or that images obtained of people in compromising positions, such as entering a drug rehabilitation clinic or urinating on a public street, will not get into the hands of publishers of salacious websites and go viral. Even if defenders of data collection and storage were to concede that measures to secure data from illegitimate access and use can fail, they may argue that the costs of any resulting intrusions would be outweighed by the compelling interest in promoting public safety: they reject “privacy at all costs.”

I also reject “privacy at all costs.” The interest we have in privacy must be weighed against competing interests including the interest in public safety. However, I disagree with Blackman that we should prohibit people from using Signal App, and I oppose the indiscriminate collection and storage of DNA and location data for crime-out investigations. How can I concede that privacy is not an absolute right but rather an interest that must be weighed against competing interests, yet oppose the collection and storage of personal data, even if such surveillance would undeniably help society fight crime?

Policies of mass surveillance subvert interests in informational privacy, undermining individual autonomy. By individual autonomy, I refer to the ability to make and act on one’s own choices about how to live one’s life. It is important to acknowledge that surveillance does not always undercut individual autonomy. Surveillance helps deter crime, and crime undercuts our ability to act freely, and so surveillance, by reducing crime, promotes individual autonomy as well. This is a compelling reason why privacy must sometimes give way to other interests, and why we should reject “privacy at all costs.” However, we need to set limits to permissible surveillance, even if doing so will let some criminals go undetected. I argue for “privacy at great cost.” I propose a line that prohibits the government from obtaining information about us that we can reasonably expect to be private, unless the government has reasonable suspicion that we pose a substantial threat to others’ autonomy. I argue that since
banning Signal App, requiring that everyone provide a sample of their DNA, or conducting sweeping surveillance of everyone’s movements would limit the autonomy of vast numbers of people whom there is no reason to suspect will pose a threat, such policies, even though they would make society safer, should be rejected, because their benefit in promoting the interest in public safety is not worth the cost to individual autonomy of frustrating legitimate privacy interests.

In Section II, I explain the framework I draw on, according to which there is a right to privacy only if there is an interest in privacy that outweighs competing interests; in Section III, I show that individuals can have a substantial interest in privacy, by linking that interest to the value of individual autonomy. In section IV, I then draw on a theory of liberal pluralism to identify the legitimate public interests that might justify limits on individual autonomy in a society in which people contest what constitutes the public interest; and in Section V, I argue that a balancing of legitimate privacy and public interests leads us to conclude that we should not permit the mass storage of sensitive data or prohibit secure means of communicating.

II. Privacy as an interest that must be balanced against competing interests

While I will argue that privacy should be respected even if the cost of doing so is great, I reject the position that we should have privacy at all costs. In doing so, I regard privacy not as an absolute right, but as an interest that must be weighed against other interests, a position I now explain.13

To say I have an interest in privacy is to say that privacy is not merely something I desire, but that without privacy my welfare would be diminished. Drawing on the work of Joel Feinberg, I distinguish an interest from a desire.14 I may desire—even strongly desire—that my favorite basketball team win tonight’s game. If they lose, and that desire is not fulfilled, I may be disappointed, but my welfare has not been set back. However, if I owned the team or placed a bet that they would win, then I have not merely a desire but an interest that they win. If they lose, my welfare is set back.

Having an interest in privacy is more than merely desiring it and provides a stronger reason for claiming a right to privacy. To see how interests are stronger bases for rights-claims than desires, consider the following example. I may desire that I not be pricked with a needle to receive a Covid-19 vaccine because I am squeamish about needles. But that is not a reason to exempt me from getting vaccinated that has much, if any, weight. However, if according to my sincerely held religious beliefs receiving the vaccine would make me eternally damned, then I have not merely a desire but an interest in not getting vaccinated. My reason for an exemption now has greater weight. Of course, my beliefs may be ill-founded. For one, I may be mistaken that my religion prohibits vaccinations: most religions do not.15 Second, I may be mistaken that there is such a thing as eternal damnation. I leave aside whether in assessing the weight of interests we should use an objective, evidence-based standard of welfare, or defer to one’s subjective assessment. My point is that claiming one has an interest in
something is conceptually distinct from claiming merely that one desires it. Interests
deserve greater consideration than mere desires.

But to say that I have an interest in not being vaccinated is not yet to say I have a
right to refuse a vaccine. For an interest to become a right it must outweigh competing
interests, and there is a compelling public interest in obtaining herd immunity against
Covid-19. If I have a medical condition that makes the vaccine a threat to my health,
alternative means of promoting the public interest might be used, such as requiring
me to wear an effective mask when around others. If I do not, the public interest in
obtaining herd immunity against Covid-19 may outweigh my autonomy interest in not
being vaccinated. Then, according to the framework I draw of rights as interests that
outweigh competing interests, I would have no right not to be vaccinated. Similarly, if
my interest in privacy is outweighed by competing interests, I would have no right to
privacy.

Before we can even say that I have an interest in privacy, we must be able to
establish that I can reasonably expect privacy. Suppose a public school bus driver
sees that a student on the bus is bullying another student, so he stops the bus, walks
over to the bully and, in a fit of rage, slaps him in clear violation of laws against
the use of physical force against children. When some of the students on the bus
who witnessed the scene tell the authorities what happened, and the driver faces
disciplinary proceedings, the driver cannot object that when others report what he
did, they violated his privacy. He was in plain view of them when he slapped the
bully and could not reasonably expect that they would not reveal what he did to the
authorities. Nor could the Memphis police officers who beat Tyre Nichols claim they
had a legitimate interest in privacy that was violated by the recording of footage taken
from police-body-worn cameras. Even if we think people should not be video recorded
without their consent even when they are in a public place, the officers consented to
being recorded by police-body-worn cameras as a condition of their job.16

But now, suppose you are in an automobile accident and are rushed to a hospital
in an ambulance. If the paramedic working on you in the ambulance were to record
you as you writhe in pain and say “I just want to die” and provide the recording
to a television station for broadcast as part of a human interest story on emergency
response teams at work, they do implicate a legitimate interest you have in privacy:
while you were in plain view of others, you were not in plain view of someone who can
legitimately share that information with others given that there is a socially-recognized
expectation of privacy between patient and medical care provider.17

We can have an interest in keeping information about ourselves private, if that
information is not in plain view of, or readily accessible to, others who use legitimate
means to observe us, and if release of that information could set back our welfare.
Before we can say we have a right to keep this information private, however, we must
weigh our interest in privacy against competing interests.

What competing interests must be weighed against our interest in informational
privacy? There can be several possessed by distinct entities. The government has an interest in exposing information that identifies threats to public safety, but private citizens also can have an interest in accessing information. For example, parents considering me as a babysitter have an interest in knowing if I have a prior criminal record or view child pornography. Prospective business partners can have an interest in knowing whether I am trustworthy or have sufficient financial resources. Friends and significant others can have an interest in knowing whether I am virtuous or prone to violence. Gilberto Valle, a police officer at the time, shared deeply disturbing chats with anonymous strangers in which they fantasized about abducting, killing, and eating women, and in some chats Valle discussed doing this to his wife. His wife had an interest in knowing this dark side of her husband, and when she found out by searching through their shared laptop, she called the FBI and promptly left him. If, as he claimed, and the evidence indicated, Valle—who became known as “Cannibal Cop”—was merely fantasizing and did not have a crystallized intent actually to commit a crime, then while his wife can still have a substantial interest in knowing about his inner darkness, the government may not. However, if Valle’s chatroom exchanges were indicative of a propensity to commit a crime, then the government’s interest in accessing his communications to ensure public safety could be substantial enough to outweigh Valle’s privacy interest.\(^\text{18}\)

III. The interest in privacy, which is connected to autonomy, is substantial

To support the position that we should protect privacy even at great cost—that we should permit individuals to communicate in ways that can evade detection and not create massive databases of everyone’s DNA or location information—I must explain why the interest in privacy is so substantial that it might outweigh the competing interest in catching criminals. The first step in doing so is to ask why informational privacy is important. There is a rich literature on this question; for brevity’s sake, I summarize some leading reasons theorists have articulated, reasons that lead us to conclude that mass surveillance could threaten interests in privacy that are substantial.\(^\text{19}\)

Informational privacy is important to individual autonomy in several ways. Without it, we are vulnerable to reputational harm. Suppose you lose your temper and do something in the heat of the moment that you immediately regret. If what you did was captured on video and widely shared, people may judge you based on that snippet, which does not reflect who you really are. The consequences to your reputation could be severe. Privacy enables us to do things without being misjudged on the basis of snippets\(^\text{20}\) and protects us from excessive or undeserved punishment.\(^\text{21}\)

The ability to keep private important personal information such as our social security number, passwords to access our online bank accounts, or the times when we are not at home, can protect us from identity theft, burglary, and other economic and psychological harms, even blackmail. A lack of informational privacy can undermine our autonomy in other ways, too, that may seem less alarming but can also have dire consequences. Without the ability to share thoughts in confidence with those whose
advice we value, we may be hampered in our ability to make important life choices. If we are always under observation, we cannot selectively reveal private information to our friends or loved ones. Charles Fried argues that without this ability we may be unable to form and maintain intimate relationships of friendship, love, and mutual trust.\(^{22}\)

Autonomy includes the ability to control, within reason, how one appears to or is defined by others. It includes the ability to project different images of yourself to different audiences. While having informational privacy sometimes means being able to keep personal information from the entire world, it often means being able to keep information about oneself secret from some circles while sharing it with others. Oliver Sipple was content having his friends and neighbors in San Francisco know he was gay, and so he was willing to march in gay parades, frequent gay bars, and have his association with prominent gay figures reported in niche magazines in the San Francisco Bay Area. But he did not want his parents and siblings in Michigan to know; and so when the *San Francisco Chronicle* published stories that outed Sipple as gay, after he heroically prevented a woman from shooting President Ford in San Francisco’s Union Square, Sipple sued for invasion of privacy. Sipple’s suit was rejected because the Court did not feel his sexual orientation was a private fact; the Court failed to recognize the important interest we have in sharing information with some people while keeping it from others.\(^ {23}\) Without this control, Sipple was not able to lead the life that was worth living to him: he died alone at the age of 47, alienated from his family. Being able to control who has access to information about ourselves lets us compartmentalize our lives, which may be essential to our well-being and happiness. It can also enable occasional, harmless escapes from the constraints of social conventions.

The reasons so far given for valuing privacy appeal to the beneficial consequences privacy can have to our reputation and well-being. Several philosophers have defended privacy on non-consequentialist grounds, instead arguing that privacy should be valued because of the demand that human beings be treated with respect and dignity.\(^ {24}\) This argument draws on Kant’s moral philosophy. Kant argues that human beings, insofar as they are rational agents, are entitled to equal respect as persons and that it would be wrong to treat them merely as means to your own ends. Persons should be treated with dignity, which means respecting them as ends-in-themselves, not as objects we can use to advance our own interests.\(^ {25}\) On this view, the need for informational privacy is a distinctly human requirement that we have as moral persons with a right to pursue our own aims and correlative duty to respect other persons’ rights to pursue their own aims.\(^ {26}\) Apart from the consequences to our reputation, relationships, and economic and psychological well-being of having our secrets exposed, merely being under surveillance can be an indignity. Stanley Benn argues that even if an individual is unaware they are being observed, whoever secretly observes them takes liberties that individual does not consent to, thereby failing to respect them as a person: “he is wrong[ed] because the significance to him of his enterprise, assumed unobserved, is
deliberately falsified... He may be in a fool’s paradise or a fool’s hell: either way [he is being made a fool of].”

Scott Sundby articulates a sense in which intrusions upon privacy by government, in particular, fail to show respect: the government treats the citizens it surveils as if they are undeserving of trust, eroding the mutual trust that must underpin a democratic society.

So far, I have reviewed some general reasons for thinking the interest in informational privacy is substantial. I now consider how these reasons might come into play if we adopted policies of mass surveillance or banned Signal App.

Why is it important that people be able to text with one another in private? Signal App lets me convey sensitive information to individuals in positions of trust, such as an attorney, banker, employer, doctor, family member—information which, if it gets into the wrong hands, could be used to harm me or tarnish my reputation. I might want to text someone I trust to relate my doubts about whether to enter into or break off relationships with friends, loved ones, or employers, or whether to pursue projects and other investments of my time and resources; if my concerns were exposed, it might sabotage those relationships and projects. Signal App also lets us secretly share thoughts with others that we would never want our intimate partners to know about, and this ability may sometimes be necessary to maintain a relationship or preserve our own sense of self.

If data about our location and movements were available, again our ability to pursue our aims in life may be hampered. Tracking my movements over time might deter me from going places I need to go, keeping me from pursuing aims that are important to me. Inferences can be drawn from my whereabouts about my activities, medical conditions, religious views, sexual preferences, or political ideology. In an intolerant, politically and ideologically divisive society, access to information about my religion, or political or sexual leanings, might expose me to physical dangers. Following my movements can amount to stalking me, which can cause me to suffer anxiety, fear, and other psychological harm.

Collecting and storing our DNA could also undermine our autonomy. Adopted children could identify their biological parents who want to remain anonymous. Depending on what DNA profile is stored, health insurers and prospective employers might learn of a person’s probability of suffering a genetic disease and refuse them coverage or employment. My location and activities could be inferred by identifying me from DNA I unknowingly leave behind. DNA databases also present a unique and frightening concern apart from their threat to informational privacy: a corrupt police officer, or someone who is out to get me, could frame me for a crime I did not commit by placing items with my DNA at crime scenes.

Apart from these consequentialist reasons why mass surveillance can set back our welfare, there is, as I noted earlier, the consideration that merely keeping track of us, even if the data are never accessed by anyone, disrespects us as persons and fails to treat us with dignity. Collecting our DNA or denying us the ability to text someone in
secrecy also shows a lack of trust of all citizens, not just of those citizens there are good reasons not to trust.

IV. The government’s legitimate interest in limiting individual autonomy

Privacy is valuable in protecting individuals from threats to their autonomy and helping them pursue their aims in life, but privacy’s relation to autonomy is ambivalent. Privacy might enable harmful and destructive acts that undermine our autonomy. This is a key reason that Blackman and others reject “privacy at all costs.”

In deciding whether government surveillance policies violate a right of privacy we need to weigh the interest in privacy against competing public interests to determine if the privacy interest is substantial enough to be regarded as a right. However, first we must identify the relevant public interests to be weighed. Since the mass surveillance policies we are considering would be designed so that only the government could access the information, we should consider the government’s legitimate interest in public safety but not the interest of private actors or businesses in accessing the information. Friends and loved ones (like Cannibal Cop’s wife) may have an interest in knowing the secrets of those they care about, including whom they are texting, and insurance companies have an interest in accessing DNA samples of those they might insure. However, those interests are not relevant in assessing the legitimate public interest in surveillance. The government properly uses its monopoly of legitimate coercive power only to enforce laws that promote public safety and welfare and not to enable private individuals and corporations to learn secrets that can advance their own private interests. The possibility that the information leaks out or is accessed and used without authorization is relevant in assessing the weight of privacy interests that could be set back, although that weight would be reduced given the presumably low (though nonzero) probability that there would be unauthorized access and use. If we were considering a policy that gave open access to everyone of whatever information is collected and stored by the government, the weight of privacy interests at risk would increase exponentially. But instead, we are considering a policy where the aim is to give access to data only to the government for its legitimate interests. Therefore, if there were a leak that enabled individuals or corporations to advance their own interests in knowing the secrets of others, we should regard those interests as illegitimate.

What constitutes a legitimate public interest that could justify state restrictions on individual autonomy? The answer will depend on our political theory of the appropriate scope of the state’s powers. Liberal political theories defend decisional autonomy, or the right of individuals to decide how to live their life free of undue coercive restrictions, but at the same time they set limits to individual autonomy. We should be free to act as we please—which means being free to conform to traditions and customs, if that is what we choose, but also free not to—but only to the extent that we leave a similar liberty to others. Conservative political theorists, in contrast, do not value individual autonomy to the same degree and do not think each of us should be free to simply reject traditions and shared community values as we please.
Whereas liberals, drawing on the theory of liberal pluralism, recognize that there are a plurality of legitimate conceptions of the aims an individual can pursue to live a worthwhile life and are unwilling to impose a particular conception of the common good on everyone, some conservatives assume there is a correct conception of the common good, the defense of which justifies restrictions on individual autonomy, and that the state may use its coercive powers to uphold a common morality.\textsuperscript{33}

An example of the conservative position follows. Many Puritans in early colonial New England believed that the common good was promoted by requiring members of the community to attend church and prohibiting them from living alone, swearing, drinking alcohol, or dressing ostentatiously, as none of these activities were thought compatible with a life worth living. Some Puritan leaders wanted means of surveillance to ensure these requirements were met. Privacy that would enable rule-violators to evade detection would threaten the common good.

In contrast, liberals believe individuals should have the liberty to settle on their own conception of the life worth living even if the majority disagree with it. In John Stuart Mill’s version of liberalism, there are a plurality of conceptions of the aims it is worthwhile for individuals to pursue, and each of us should be free to pursue our own conception so long as we do not harm others.\textsuperscript{34} Liberals reject “legal moralism,” which is the view that the state may punish immoral but harmless self-regarding activity.\textsuperscript{35} I will assume, without argument, that the liberal view that there are a plurality of legitimate ways to pursue one’s life and that people should not be forced to comply with one particular conception is correct; and for simplicity’s sake, I will focus on Mill’s “harm principle” as an appropriate restriction on autonomy, even though some variations may be more attractive.\textsuperscript{36}

According to the harm principle, the government may legitimately coerce individuals only for the limited purpose of preventing them from harming others.\textsuperscript{37} The government’s legitimate public interest is to ensure public safety and not to enforce a particular conception of morality, even if it is widely shared by the majority. For example, Cannibal Cop should be free to have appalling thoughts and share them so long as those thoughts will not lead to harm to others. This does not mean his wife should not leave him when she discovers his dark fantasies, but it does mean the state should not imprison him for his fantasies so long as there was no plausible indication that he would act upon them.

Another example also illustrates the liberal position. Companies are developing sex robots that have humanoid form. While they can engage in sex acts with humans, the robots do not feel pain, lack consciousness, and are not moral agents, and so they cannot be harmed. Should the state permit purchase and use of such robots by individuals who want to use the robot to simulate acts of rape or child sexual abuse? Only someone with a corrupt moral character would engage in such conduct. However, since the robots cannot be harmed, then according to the harm principle the government should not coercively prohibit this behavior, unless it plausibly would lead to future acts that would harm others.\textsuperscript{38} For many people this conclusion will be
Privacy at Great Cost

To meet its legitimate objective of preventing individuals from harming others, a government may need to limit informational privacy. However, it should not frustrate substantial interests in privacy solely to judge or punish individuals for having a bad moral character or to enforce a particular conception of morality that has no bearing on public safety and the prevention of harm. On the liberal theory I defend, the state may intrude upon privacy if necessary to catch murderers, but not to catch an adulterer or marijuana user, even where there are laws prohibiting adultery or marijuana use, because neither of these lawbreakers harms others. There are costs when the government conducts surveillance: in addition to reputational and other harms associated with reduced informational privacy, surveillance breeds mistrust and resentment. Preventing harm may sometimes be worth the cost, but blaming and punishing harmless moral wrongdoers may not be.

Even in colonial New England’s Puritan societies, it was eventually recognized that the benefit to the common good of enforcing morality was not worth the cost of losing privacy. Historian David Flaherty notes how privacy was respected even in this highly regimented society. The English common law that carried over to New England recognized privacy in the relation between husbands and wives; they were not expected to inform authorities when their spouse violated community standards of decency. While there was pressure to report lawbreakers to uphold community values and prevent harmful acts like theft, this pressure was “counteracted by the need to protect the intimacy of a family.” Massachusetts, while encouraging and even obliging persons to report stolen goods, made an exception if “[t]he Fact be private, or committed by some Member of his own Family.” Flaherty argues that over time, colonial law enforcers such as night watchmen, tithingmen, grand juries, constables, and informers became increasingly less than diligent in enforcing Puritan morality, out of respect for privacy.

To summarize the argument so far: we can have a right to privacy when our interest in privacy outweighs competing interests. When we calculate whether our interest in privacy outweighs competing public interests, we should draw on liberal political theory to circumscribe the legitimate public interests that could justify coercive interference from the state. In assessing government policies of mass surveillance, we should limit the government interest that we balance against privacy interests to the interest in preventing harm. The final step in the argument is to consider how we weigh the legitimate public interest in public safety that various forms of surveillance
could advance against legitimate privacy interests.

V. Balancing the competing interests: an alternative to utilitarianism

One might argue that infringements on the right to informational privacy should not be permitted simply because to have a right to privacy means one cannot infringe that right. One might think that mass surveillance fails to respect the dignity of individuals and that we cannot put a price on human dignity. But I have rejected that conclusion. It is unconvincing to say that privacy is automatically more important than competing interests. If it is more important, we should have a right to privacy. However, we must first determine that it is by weighing the interest in privacy against competing interests.

How are we to weigh the competing legitimate interests at stake? One approach to balancing interests is the one taken by utilitarians. Drawing on a prominent version of utilitarian theory, we would decide whether we should adopt a policy by calculating the benefits or pleasure to society’s members—measured in “utiles” or some equivalent—that would result from the policy both in the short and long term, and similarly calculating the costs that would result—the pain or harm caused. We adopt the policy if the aggregate benefits (the summed total gain in utility of each member of society) exceed the aggregate costs. The framework I have laid out above, in which we weigh only legitimate interests in privacy against legitimate government interests in preventing harm, would circumscribe the calculation to a degree. But even so, the problem with this approach is that it seems impossible to carry out: how can we quantify what the widespread consequences of the surveillance policies we have been considering will be?

Try calculating the net social utility of permitting Signal App. Some large number of people will communicate in private, and many of them will derive utility from this. Some unknown subset of this group will engage in criminal acts that harm others, creating disutility to their victims, which is harmful to their victims and to society overall. However, it is possible that if Signal App were not permitted, they could still communicate in private in other ways—people, after all, committed crimes undetected even before we had phones—so in calculating the overall utility of permitting Signal App we really need to calculate the marginal utility of having the convenience of Signal App and not needing to rely on other means of communicating. Even if some people could conspire to commit crimes using the app, how would we know that they could succeed only because the app was available? The app may decrease the probability of their detection to some extent, but how could we calculate that extent? Perhaps we could try to measure the costs and benefits empirically with a social experiment, where we provide Signal App to those in one region and compare this region’s crime rates after introduction of the app, and the utility of Signal App users there, with rates of harm-creating crime and overall utility of individuals in a demographically similar region where Signal App is not available; or we might focus on a particular region and contrast individual utility and crime rates before and after introduction of
Signal App. However, there are so many factors entering into a person’s overall utility and affecting crime rates that attempting to identify the change in utility associated with increased or reduced informational privacy or to quantify the contribution of Signal App to crime rates seems futile. This in itself is an objection not to the ethical framework of utilitarianism, but only to our ability to apply it in assessing Signal App. However, there is a general concern with utilitarianism. The very suggestion that we measure the extent to which privacy interests have been set back in units of utiles is problematic: if we regard the setback as a violation of dignity, how do we measure the loss of dignity in utiles or their equivalent?42

Applying the utilitarian framework to the policy of collecting and storing DNA samples from all members of society may seem more manageable in one respect than applying it to a policy permitting Signal App. It might seem easier to establish the effect of this policy on crime rates by relying on logic instead of empirical evidence that may be impossible to obtain.43 Those highly skilled in leaving behind no DNA evidence at a crime scene may not be impacted but many criminals will, and if they are rational and would face punishment that outweighs the benefits they get from committing the crime, it is reasonable to conclude that they may be deterred, if there is a mass DNA database. The percentage of crimes solved will increase. In assessing the utility of the DNA collection policy, however, we should count the utility of detecting only those crimes that led to a conviction for which DNA evidence was necessary to convict the perpetrator and for which a DNA sample could not have been obtained with a warrant. There will still be criminals convicted based on other physical evidence, witnesses, and video evidence, or for whom there is sufficient evidence to obtain a warrant so that police could obtain their DNA sample, and it may not be clear whether there would have been a conviction without the policy of mass DNA collection.44 Even so, I grant that there could be a significant decrease in some serious crimes because the greater likelihood of getting caught deters some would-be criminals. The question then becomes, how are we to weigh the costs to individual autonomy of having this database? That task is impossible. One cost is the loss of dignity that individuals may suffer, and, as I noted above, dignity is not a value we know how to measure. We might take surveys, asking people how important it is to them or what they would be willing to pay to opt out of having their DNA included, but how could anyone reliably calculate that value since it depends on unforeseeable future consequences? If surveillance policies were put into effect and people got used to them, people might resign themselves to having reduced expectations of privacy, and then may indicate in their survey response that they suffer no disutility from the surveillance. However, this does not show that they would not experience greater utility in an alternate world without such surveillance.

Calculating the net utility of storing location data is similarly difficult. There are cases where individuals were identified as criminals because police could determine that they were at the location of multiple crime scenes exactly when crimes were committed in those locations.45 Yet in many cases, there are other pieces of evidence
that could independently be used to identify and incriminate the perpetrator, and determining the disutility of having people’s locations monitored just is not possible for the same reasons that we cannot calculate the disutility of government keeping a massive DNA database. Having video cameras at high-risk locations such as churches or synagogues in cities where threats of bombings were made, or even in your carport to identify thieves, would not raise the privacy concerns raised by mass surveillance that allows coordination of data to in effect follow people.

So where does this leave us? An alternative way of balancing competing interests, that does not require us to attempt the impossible task of calculating utilities of an unforeseeable future, or to put a price tag on dignity or trust, is an approach adopted by courts in several nations including the United States. If a policy implicates a right, and the right is important enough, or “fundamental,” we should only permit its infringement (1) for compelling purposes and (2) where those purposes could not be achieved by some alternative policy that would not violate the fundamental right. By using this two-pronged test, we do not need to attempt the futile task of quantifying the value of the interests at stake: if we can make a compelling case that the interest is very important or fundamental, then we would demand strong justification for—we would “strictly scrutinize”—any policy that frustrates that interest. We would require the government to establish not simply that its surveillance policy reduces crime—for the costs to privacy could be greater than the benefit of reducing crime—but that the policy was necessary for achieving a compelling government purpose that could not be achieved in some other less intrusive way.

In defending privacy “at great cost,” I regard the interest in informational privacy as substantial or fundamental; in Section III, I reviewed some reasons why by linking informational privacy to the values of individual autonomy, dignity, and trust. Any policy that threatens this interest must serve a compelling purpose that could not otherwise be obtained by less intrusive alternatives. In section IV, I argued that preventing harm can be a compelling purpose, but morally judging people who are not harming others is not. According to liberal political theory, judging or punishing people who are not harming others but merely are offending the majority’s preferred morality by displaying a corrupt moral character may not even be a legitimate, let alone a compelling purpose that could warrant the use of coercion and intrusive means of surveillance.

A policy of mass surveillance is likely to fail the strict scrutiny test even when the policy has a compelling purpose. The reason is that when the state’s purpose is to “fight crime” in general—rather than target an identifiable criminal—there are less intrusive alternatives to achieve that purpose. For example, using aerial surveillance by flying planes with high-tech cameras over the city of Baltimore to track everyone’s location might be useful in stopping some crime, but there are other methods of dealing with crime there that do not require suspicionless general searches that undermine the autonomy of so many people. The state cannot possibly prove that it needs to prohibit Signal App, or have databases of location data and DNA to prevent some
hypothetical future crime. At best, it can show that implementing these policies could make it easier to catch the criminal. This is a problem endemic to policies permitting general, suspicionless searches. The policy of mass surveillance may be useful in catching criminals, and reducing crime is a compelling government purpose. However, the policy cannot pass the “necessity” prong of the strict scrutiny test—that there be no less intrusive alternatives for achieving the compelling purpose—because to show this, one must appeal to counterfactual claims such as “without the surveillance we would never have caught the criminal,” claims it may be impossible to prove.  

Consider the suspicionless, general surveillance policy that motivated colonists in the U.S. to revolt against the Crown. The British writs of assistance authorized government agents to search individuals’ property to see if they evaded customs laws, without having individualized suspicion that a crime was being committed. No doubt such a policy would help catch lawbreakers, but the policy is much broader than is needed to serve legitimate public interests. The British could legitimately claim a compelling purpose of deterring individuals from violating the customs laws, but they could fulfill that purpose by having the authorities get warrants to search the property only of those whom they have probable cause to suspect are violating the law. The more intrusive surveillance adopted by using the writs of assistance might be helpful in catching every single tax evader, but it may not be necessary even for that. In any case, while deterring lawbreakers is a compelling government purpose, catching every single customs law violator is not. Even if it were, the cost of the policy to colonists’ autonomy was so great that it contributed to a revolution.  

It is easier to balance competing interests using a utilitarian calculation when the issue is not whether a general policy should be adopted, such as mass surveillance using DNA or location data, or permitting a technology like Signal App, but whether in a particular case the societal cost of letting a dangerous criminal avoid capture outweighs the cost of frustrating suspects’ privacy interests. Suppose police have a reasonable suspicion that a man murdered a young girl and hid the body, but lack probable cause to get a search warrant that might help them prove it. If the police proceed to intrude upon the man’s privacy by attaching a GPS device to his car to track his movements without a warrant and discover that he travels to a remote location and digs up the young girl’s body in an effort to bury it someplace else, it seems reasonable to permit this evidence at trial to convict him, though his legitimate interest in privacy was frustrated. The social utility of confining and punishing him exceeds the disutility he suffers by being followed.

In reaching this conclusion one is not defending a policy of suspicionless, general searches, the impact of which on individual autonomy would be widespread and the benefits of which may be impossible to quantify. Rather, one is calculating that the cost to society of violating interests in privacy in this case are outweighed by the benefit to public safety of capturing and convicting this particular dangerous criminal. There is of course the objection that if we are willing to make exceptions to the “no GPS search without a warrant” rule in one case, we will make exceptions in others,
and pretty soon the rule dissolves along with our privacy. It is better to avoid that outcome by sticking to our rule requiring probable cause for a search, no matter how much it hurts to do so in a particular case. However, since invasions would occur only with reasonable suspicion, only a very small fraction of people would need to worry about whether they can safely pursue their aims; further, we can more readily determine if invading the suspect’s privacy is really necessary: since we have a suspect in mind, we can assess the sufficiency of alternative evidence that we could obtain in less intrusive ways.

That we should reject “privacy at all costs” is illustrated also by an actual case that presents important twists to the bus driver example I presented in Section II. In this case, the bus driver, Brian Duchow, made abusive statements to and slapped 9-year old Jacob M, when they were alone on the bus. Because Jacob was the first person picked up on the route, no one else witnessed what Duchow did, in contrast to the example I gave earlier. Jacob has Downs Syndrome, and his significant speech impairment meant he was unable to communicate what happened on the bus. But he acted oddly—he would punch his toys, kick the family dog, resist boarding the bus in the morning, and cry when it was time to board the bus to return home. His parents suspected something was happening on the bus, so they put a voice-activated recorder in Jacob’s backpack, and it recorded Duchow making abusive statements and what the parents believed was a slap. Duchow was convicted of disorderly conduct and physical abuse of a child and appealed, claiming the recording violated state privacy law that prohibited recording others without their consent.

Duchow had an interest in keeping his activities on the bus private, and I believe his interest was legitimate: even though he was on a public bus, what he did was not in plain view of anyone who could have revealed it. But the state has a compelling interest in uncovering what he did, and in this case that interest clearly outweighs Duchow’s interest in keeping his activities on the bus private.

The issue the case raises is not whether there should be general surveillance such as secret cameras or microphones on all vehicles, or for that matter in homes, which would surely reduce crime but at tremendous cost to individual autonomy. Unlike when mass surveillance is conducted, in this case there was a reasonable suspicion of harmful conduct (though at the time by an unknown person). Permitting parents of a child with Downs Syndrome to use secret microphones when they have reason to suspect someone is hurting their child would not deter individuals from pursuing their aims out of fear that their activities were being monitored. We should not conclude from this that mass monitoring of all conversations, secretly or otherwise, is permissible.

Letting Duchow get off scot-free would be too great a cost for protecting his privacy. However, while a policy of mass surveillance using DNA and location data or of banning technologies that enable individuals to text each other in complete secrecy could detect or deter crimes that have a great social cost, adopting such policies might impose a greater cost and is not justified given the threat they pose to the autonomy of
so many people.

Mark Tunick received his PhD in Political Science at U.C. Berkeley and taught at Stanford before becoming a founding faculty member of the Wilkes Honors College at Florida Atlantic University, where he teaches political theory and constitutional law. He is the author of Texting, Suicide, and the Law (2019), Balancing Privacy and Free Speech: Unwanted Attention in the Age of Social Media (2015), Hegel’s Political Philosophy (1992; reissued in 2014 as part of Princeton’s Legacy Library), and numerous other publications. Tunick’s primary scholarly interests include the political philosophy of Hegel and J.S. Mill, privacy, toleration, AI ethics, and punishment.

Notes and References


2. I focus here only on informational privacy and not other conceptions of privacy such as the ability to be secluded or anonymous. On the definitions of privacy, see Mark Tunick, Balancing Privacy and Free Speech: Unwanted Attention in the Age of Social Media (NY: Routledge, 2015), available open access at https://library.oapen.org/handle/20.500.12657/52755, 24–30.


4. His conviction was upheld by the U.S. Supreme Court in Maryland v. King, 569 US 435 (2013).


9. Arnold Loewy asks a related question: if, hypothetically, the government could use a divining rod that determines only if you commit a crime and nothing else, why should an innocent person care if the divining rod is pointed at them? See Arnold Loewy, “The Fourth Amendment as a Device for Protecting the Innocent,” Michigan Law Review 81, no. 5 (1983), 1229-1272, at 1244–5.
10. I thank James Branca for suggesting this point.

11. For a response to the general objection that innocent people with nothing to hide have no reason to care about privacy, see Daniel Solove, “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy,” San Diego Law Review 44 (2007):745–72.


13. In this paper I weigh the interest in privacy against the interest in public safety. In an earlier work I weigh the interest in privacy against the interest in free speech: see Tunick, Balancing Privacy and Free Speech, especially 130–34.


16. Use of a pole camera or an ALPR to record who is in a particular location may not violate reasonable expectations of privacy, either; but mass surveillance involving a comprehensive, coordinated network of cameras and aerial surveillance differs, in that it lets government track the movements of people over time.


18. I discuss the Valle case in Mark Tunick, “Brain Privacy and the Case of Cannibal Cop,” Res Publica 23, no. 2 (2017):179–96. Another example, suggested by the journal editors: a child fantasizes about being cruel to animals, which may be an early sign of sociopathy. The community, and particularly those at the child’s school, have an interest in having the parents reveal this potential safety danger; but the parents and child have a competing interest in protecting the child from reputational harm that could set back the child’s future welfare.

19. I draw on Tunick, Balancing Privacy and Free Speech, ch. 2, and the works cited there, some of which I will refer to in the following discussion.


24. Stanley Benn, “Privacy, Freedom and Respect for Persons,” in Philosophical
Dimensions of Privacy, ed. Ferdinand Schoeman, 223–44; Edward Bloustein,
“Privacy as an Aspect of Human Dignity,” in Philosophical Dimensions of Privacy,
ed. Ferdinand Schoeman, 156–202; discussed in Tunick, Balancing Privacy and Free
Speech, 54–59.


26. I say ‘distinctly human’ because while some other species on earth can have an
interest in seclusion or isolation, because when closely confined with others they have
a shortened life span, so far as I know none have an interest in informational privacy.

27. Benn, “Privacy, Freedom and Respect for Persons,” 230; see also 230–1: I
can resent someone watching me at work without my knowledge “as though it didn’t
matter whether I liked it or not.”

28. Scott Sundby, “Everyman’s Fourth Amendment: Privacy or Mutual Trust Be-

29. See Mark Tunick, “Privacy in Public Places: Do GPS and Video Surveillance
Provide Plain Views?,” Social Theory and Practice 35 no. 4 (2009): 597–622, at

Capitol Riot,” New York Times, April 28, 2021; Liam Stack, “Druggings, Deaths and
Robberies Put New York’s Gay Community on Edge,” New York Times, December 3,
2022.


32. I leave aside the distinction between legitimate and illegitimate interests of
private individuals and corporations in conducting private searches. Cannibal Cop’s
wife may have a legitimate interest in accessing the laptop her husband used; but a
company’s interest in accessing trade secrets of a competitor may not be legitimate.

33. A classic statement of liberal pluralism is given in John Rawls, “The Idea of
A recent example of a conservative position is Adrian Vermeule, Common Good
Constitutionalism: Recovering the Classical Legal Tradition (Medford, MA: Polity
Press, 2022); and for a shortened version, Vermeule, “Beyond Originalism,” The
Atlantic, March 31, 2020. Vermeule argues that the Supreme Court should seek to
promote the common good, including traditional morality, rather than protect what
Vermeule regards as the “progressive” agenda of seeking “endless liberation” from
the “unchosen bonds of tradition, family, religion...and even biology”: see Vermeule,
Common Good, 22. For a defense of ‘progressivism,’ see Erwin Chemerinsky, We the
People: A Progressive Reading of the Constitution for the 21st Century (NY: Picador,
2018).

35. See Feinberg, Harm to Others, 12.

36. One alternate to the harm principle is that each should be free to adequately pursue their aims so long as they leave others a similar freedom to adequately pursue theirs—see Jeremy Waldron, “Toleration and Reasonableness,” in Culture of Toleration in Diverse Societies, ed. Catriona McKinnon and Dario Castiglione (Manchester: Manchester University Press, 2003); discussed in Mark Tunick, “Religious Freedom and Toleration: A Liberal Pluralist approach to Conflicts over Religious Displays,” Journal of Church and State 64, no. 2 (2022): 280–300.

37. There is an ambiguity in Mill’s harm principle: can the government coercively restrict an individual’s liberty only to prevent that individual from harming others? Or can it coercively restrict anyone’s liberty if doing so would prevent harm? David Lyons takes Mill’s principle to permit the state to compel me to pay taxes, or save another’s life, or testify in court, to prevent harm to others even though I do not cause that harm (David Lyons, “Liberty and Harm to Others,” in Mill’s on Liberty, ed. Gerald Dworkin [Lanham, Maryland: Rowman and Littlefield, 1997]). D.G. Brown argues otherwise: that Mill’s harm principle permits coercion of me only to prevent me from causing harm to others (D.G. Brown, “Mill on Liberty and Morality,” The Philosophical Review 81 [1972]: 133–58). In a work in progress, I defend Brown’s interpretation.


39. By tolerate, here, I mean ‘do not legally punish.’ Even Mill allows that we can discourage and criticize harmless but indecent self-regarding conduct and avoid those who engage in it.


41. Jeremy Bentham gives a classic account of the ‘primary and secondary mischiefs’ that might result from a crime, including the alarm created in society, as well as the danger that results when criminals encourage others to commit crimes in the future: see Jeremy Bentham, An Introduction to the Principle of Morals and Legislation (Oxford: Clarendon Press, 1907), ch. 12.

42. On the difficulty of measuring the benefits of privacy, dignity, autonomy, or fairness in units of utiles (or dollars or other units), see Mark Tunick, “Efficiency, Practices, and the Moral Point of View: Limits of Economic Interpretations of Law,” in Theoretical Foundations of Law and Economics, ed. Mark White, (NY: Cambridge University Press, 2009).

43. Empirically measuring the effect would be challenging. We might try a
localized implementation and extrapolate from it, by requiring everyone living in a certain region to provide a DNA sample and assessing the impact of that policy on individuals’ autonomy and on crime in this location. However, this might only encourage local criminals to target outside areas, and outside criminals to move into the region; and of course there is the difficulty of accounting for the many factors that might explain crime rates and overall utility.

44. Some may defend the use of DNA surveillance to exonerate innocent people: but mass DNA collection isn’t needed to do that: an innocent suspect would volunteer a DNA sample to prove it isn’t a match with DNA at the crime scene.


46. Since on my approach we cannot say whether an interest should be regarded as a right until after we balance that interest against competing interests, I would use the term ‘interest’ instead of ‘right’ here—but courts use the term ‘right’.

47. An example of the U.S. Supreme Court strictly scrutinizing a law that infringes on a fundamental right is Griswold v. Connecticut, 381 U.S. 469 (1965); in the European Union a similar approach is taken when balancing privacy and freedom of speech: see Peck v. U.K., [2003] 36 EHRR41, Par. 100: “the more substantial the interference with human rights, the more the court would require by way of justification before it was satisfied that the decision was reasonable.”

48. The scope of police powers on a liberal theory may depend on how broadly we construe ‘harm to others’. For example, can the state punish politicians who got elected by lying on their resume? Yes, if we regard such behavior as ‘harming’ our institutions.


50. One might argue that in the past there were crimes we would not have solved without DNA evidence, and reason that we can then assume there’d be crimes like that in the future; but how can we prove the counterfactual that the crimes would not have been solved without the DNA evidence? Or that police would not have gathered evidence on a suspect sufficient for a warrant to obtain a sample of their DNA?


52. This would be the rule-utilitarian response. For a classic statement of rule-utilitarianism, see John Rawls, “Two Concepts of Rules,” Philosophical Review 64, no. 1 (1955): 3–32.

53. This is a public policy argument. As a matter of constitutional law, the Supreme Court ruled that police may not attach a GPS device to a car without a warrant (U.S. v. Jones, 565 U.S. 400 [2012]); and to get a search warrant the 4th
Amendment requires probable cause, not reasonable suspicion.

54. State v. Duchow, 310 Wis.2d 1 (2008) (Supreme Court of Wisconsin).

55. The Court reasoned otherwise—that Duchow could not expect privacy on a bus. While earlier I agreed that he could not if others who could report what he did were also present, that was not the case. See Mark Tunick, Texting, Suicide, and the Law (NY: Routledge, 2019), 35–6, criticizing the court’s reasoning, but agreeing with its conclusion.