UNC SCHOOL OF LAW

NORTH CAROLINA LAW REVIEW

Volume 96
Number 5 *Badge Cams as Data and Deterrent: Enforcement, the Public, and the Press in the Age of Digital Video*

Article 3

6-1-2018

Body Cameras and the Path to Redeem Privacy Law

Woodrow Hartzog

BODY CAMERAS AND THE PATH TO REDEEM PRIVACY LAW*

WOODROW HARTZOG**

From a privacy perspective, the movement towards police body cameras seems ominous. The prospect of a surveillance device capturing massive amounts of data concerning people's most vulnerable moments is daunting. These concerns are compounded by the fact that there is little consensus and few hard rules on how and for whom these systems should be built and used. But in many ways, this blank slate is a gift. Law and policy makers are not burdened by the weight of rules and technologies created in a different time for a different purpose. These surveillance and data technologies will be modern. Many of the risks posed by the systems will be novel as well. Our privacy rules must keep up.

In this Article, I argue that police body cameras are an opportunity to chart a path past privacy law's most vexing missteps and omissions. Specifically, lawmakers should avoid falling back on the "reasonable expectation of privacy" standard. Instead, they should use body cameras to embrace more nuanced theories of privacy, such as trust and obscurity. Trust-based relationships can be used to counter the harshness of the third-party doctrine. The value of obscurity reveals the misguided nature of the argument that there is "no privacy in public."

Law and policy makers can also better protect privacy by creating rules that address how body cameras and data technologies are designed in addition to how they are used. Since body-camera systems implicate every stage of the modern data lifecycle from collection to disclosure, they can serve as a useful model across industry and government. But if law and policy

** Professor of Law and Computer Science, Northeastern University School of Law and College of Computer and Information Science; Affiliate Scholar, Stanford Law School's Center for Internet and Society. The author would like to thank David Ardia, Brannon Denning, Bryce Clayton Newell, Neil Richards, Evan Selinger, and Peter Swire. The author would also like to thank Christian Snow and Taylor Lovejoy for their research assistance and Nicole Gomez Diaz and the staff of the *North Carolina Law Review* for their editing and support.

makers hope to show how privacy rules can be improved, they must act quickly. The path to privacy law's redemption will stay clear for only so long.

INTRODUCTION 1258
I. BODY CAMERAS ARE AN OPPORTUNITY TO FIX PRIVACY LAW 1265
A. The Rush to Implement Body Cameras with No Clear Plan 1265
B. The Window of Opportunity to Change Privacy Law 1267
1. Surveillance 1271
2. Data Protection 1272
3. Public Records and Public Disclosure 1275
II. REFINING THEORY: GET RID OF THE REASONABLE EXPECTATIONS OF PRIVACY TEST 1279
A. The Test is Broken and Unsalvageable 1283
B. Embrace More Specific Notions of Privacy 1286
1. Trust Protects Relationships 1287
2. Obscurity Reveals the Fallacy of "No Privacy in Public" 1290
3. Autonomy Justifies Requiring Authorization 1294
III. REFINING IMPLEMENTATION: DESIGNING A BETTER BODY CAMERA SYSTEM 1297
A. Design Will Determine the Value of Body Cameras 1298
B. Guides for Designing a Body Camera Obscura 1300
1. Data Collection 1301
2. Data Storage 1303
3. Data Processing 1305
4. Data Dissemination 1308
CONCLUSION 1312

INTRODUCTION

Body-worn cameras on every police officer in America are understandably seen as a serious threat to privacy. People have deep concerns about the way in which this potentially pervasive and

powerful surveillance infrastructure is implemented and regulated.[1] The prospect of being watched all the time, especially in our most vulnerable moments, is daunting.[2] So is the risk that comes from the colossal amount of data that will be created, stored, processed, and shared through the use of body camera systems.[3]

Much of this concern stems from the fact that, until relatively recently, there were few specific rules for how body cameras should be built, used, or how the data they collected should be treated.[4] This left police departments, often in conjunction with third-party vendors, to come up with their own rules.[5] Unsurprisingly, the rules we have now, which include everything from state statutes and municipal ordinances to department policies and contracts with vendors, are inconsistent and sporadic. It seems that there is little consensus for key questions such as when the cameras will run and who will be able to tell when they are on; how long footage is kept and who can see it; how footage is secured; and whether biometrics can be used.[6]

In fact, the one thing that seems clear from the body-worn camera debate is that with so many different players and interests involved, it is hard to agree on anything.[7] Lawmakers and advocates

1. *See* Bryce Clayton Newell, *Collateral Visibility: A Socio-Legal Study of Police Body Camera Adoption, Privacy, and Public Disclosure in Washington State,* 92 IND. L.J. 1329, 1139 (2017).

2. *See, e.g.*, *Developments in the Law—Policing*, 128 HARV. L. REV. 1706, 1808 (2015); Newell, *supra* note 1, at 1136–37; Katie Farden, Note, *Recording a New Frontier in Evidence-Gathering: Police Body-Worn Cameras and Privacy Doctrines in Washington State*, 40 SEATTLE U. L. REV. 271, 276 (2016); Erik Nielsen, Comment, *Fourth Amendment Implications of Police-Worn Body Cameras*, 48 ST. MARY'S L.J. 115, 134 (2016). People use several different terms to describe this technology, including "body-worn cameras" and "body cameras." The terms will be used synonymously in this article.

3. *See* Elizabeth E. Joh, *Beyond Surveillance: Data Control and Body Cameras*, 14 SURVEILLANCE & SOC'Y 133, 133–36 (2016), https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/cdebate4/bc4 [https://perma.cc/36PT-EBZZ].

4. *See id.* at 133.

5. *See generally* Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 101 (2017) ("The relationships between surveillance technology vendors and police departments show the increasing degree to which private companies can guide, shape, and limit what the public police do.").

6. *See* Alexandra Mateescu, Alex Rosenblat & danah boyd, *Police Body-Worn Cameras* 2, 16–19 (Feb. 2015) (unpublished manuscript), https://www.datasociety.net/pubs/dcr/PoliceBodyWornCameras.pdf [https://perma.cc/QJF4-FBBS].

7. See THE LEADERSHIP CONFERENCE ON CIVIL & HUMAN RIGHTS & UPTURN, POLICE BODY WORN CAMERAS: A POLICY SCORECARD (2017), https://www.bwcscorecard.org/ [https://perma.cc/GSV7-9VEK], for a useful reference comparing the different body camera policies on criteria such as policy available, officer discretion, personal privacy, officer review, footage retention, footage misuse, footage access, and biometric use.

of body cameras use purported foundational values such as "accountability" and "transparency" in such a vague way that the specific purposes of the cameras are not even clear.[8] Are body cameras meant to provide evidence for when force is used? Or perhaps they are meant to more generally encourage good behavior by reminding people they are being watched? Or are there other goals for body cameras? Should body cameras primarily benefit the subjects of police interaction, the police officers themselves, the public, or all of the above? Which values are paramount in body-camera systems: accountability, transparency, or privacy? And what do we even mean by those concepts? Privacy, in particular, is spacious and could mean a host of things.[9] How police departments and vendors answer those questions will determine both how effective and how harmful police body-worn cameras can be.[10]

But amidst the chaos lies opportunity. The relatively blank slate for body-worn cameras that is creating so much risk is also an opportunity to take a fresh new approach to the rules of surveillance, data protection, and privacy in public records. States, cities, and police departments need not cling to the entrenched and awkward rules out of inertia. Due process and reasonable care can be implemented in many different ways.[11]

Most importantly, those creating rules for body cameras have the opportunity to avoid the broken parts of privacy law that have confounded courts, lawmakers, and officials for years. For example,

8. *See* Caren Myers Morrison, *Body Camera Obscura: The Semiotics of Police Video*, 54 AM. CRIM. L. REV. 791, 795 (2017); Kami C. Simmons, *Body-Mounted Police Cameras: A Primer on Police Accountability vs. Privacy*, 58 HOW. L.J. 881, 884–87 (2015) (identifying possible body camera utilities as identifying the use of excessive, deterring police misconduct and promoting officer safety, force, and use as a training tool to correct structural problems within police departments.); Seth W. Stoughton, *Police Body-Worn Cameras,* 96 N.C. L. REV. 1363, 1378 (2018) (explaining that there has been a "laundry list of advantages" for body-worn cameras); Mateescu, et al., *supra* note 6, at 16–19 (discussing potential issues with body-worn cameras depending on the manner in which policy allows them to be used); danah boyd & Alex Rosenblat, *It's Not Too Late to Get Body Cameras Right*, ATLANTIC (May 1, 2015), https://www.theatlantic.com/technology/archive/2015/05/its-not-too-late-to-get-body-cameras-right/393257/ [https://perma.cc/2VQR-WLNN].

9. *See* Simmons, *supra* note 8, at 889–90 (showing examples of the concerns relating to privacy and who benefits from the use of body cameras).

10. *See* THE LEADERSHIP CONFERENCE ON CIVIL & HUMAN RIGHTS & UPTURN, *supra* note 7 (noting that police departments in various cities addressed privacy in different ways while some police departments did not address privacy at all).

11. *See* THE CONSTITUTION PROJECT, GUIDELINES FOR THE USE OF BODY-WORN CAMERA BY LAW ENFORCEMENT 19–21 (2016), https://constitutionproject.org/wp-content/uploads/2016/12/BodyCamerasRptOnline.pdf [https://perma.cc/2JVA-4V35] (addressing issues of due process and chain of custody).

there is a growing discomfort with the idea that there is no privacy in public or in information shared with third parties.[12] Lawmakers have too often ignored the design of information technologies. They too often conceive of public records as exclusively binary, where the only choices seem to be either to keep it hidden or to release it to the world, with no restrictions.[13] People too often use publicly accessible information to exploit and harass others or expose them in harmful and unjustified ways.[14] Entrenched privacy regimes have to grapple with these problems that have been created by old and narrow conceptualizations of privacy and ineffective strategies to protect it. Body-worn camera rules do not have to repeat the same mistakes.

In this Article, I argue body cameras are an opportunity for law and policy makers to create frameworks that do not repeat privacy law's most vexing missteps and omissions. In doing so, law and policy makers can chart the path for better surveillance and data rules in other contexts. The path to privacy law's redemption has both a theoretical and practical component. Policy makers can use body cameras to embrace more nuanced theories of privacy in law. They can also use body cameras to better protect privacy in practice by embracing a holistic approach to body-camera systems that include rules regarding how body camera and data technologies are built, in addition to how they are used. A sound theoretical and practical framework for body cameras can serve as a model for how to better balance notions of privacy with competing values like government transparency and free speech in other contexts involving surveillance and data protection. Also, a new framework can show how to move beyond ill-fitting theories of privacy that either gradually erode protection for people or awkwardly group information and contexts into "public" or "private" categories.

My goal for this Article is modest within the entire body camera debate, as I am concerned mainly with how these technologies affect privacy. There are critical questions regarding free speech, government accountability, racial justice and freedom from bias, procedural fairness, and evidentiary concerns that lawmakers, judges, and police departments must answer, in addition to data and

12. *See infra* Section II.B.2.

13. *See infra* Section I.B.3.

14. *See* WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (forthcoming 2018) (manuscript at 3) (on file with the North Carolina Law Review) (providing examples of harmful effects of personal information being used in harmful ways); Daniel J. Solove, *Access and Aggregation: Privacy, Public Records, and the Constitution*, 86 MINN. L. REV. 1137, 1141 (2002).

surveillance issues.[15] By focusing only on privacy, I do not mean to diminish the importance of government accountability, equality, due process, and press freedom. In fact, my hope is that the framework proposed in this Article would help to better balance privacy among the other values implicated by body cameras. Nor do I directly address the efficacy of body-worn cameras for their stated goals,

15. *See* Kami N. Chavis, *Body-Worn Cameras: Exploring the Unintentional Consequences of Technological Advances and Ensuring a Role for Community Consultation*, 51 WAKE FOREST L. REV. 985, 988–89 (2016); Mary D. Fan, *Justice Visualized: Courts and the Body Camera Revolution*, 50 U.C. DAVIS L. REV. 897, 898 (2017) ("[T]here is often a difference between the legally relevant truth and the depiction captured on video. Care must be taken therefore to apply the proper perceptual yardsticks and reserve interpretive questions for the appropriate fact-finders."); Mary D. Fan, *Hacking Qualified Immunity: Camera Power and Civil Rights Settlements*, 8 ALA. C.R. & C.L.L. REV. 51, 52 (2017); David A. Harris, *Picture This: Body-Worn Video Devices (Head Cams) as Tools for Ensuring Fourth Amendment Compliance by Police*, 43 TEX. TECH L. REV. 357, 359–60 (2010) ("What is more, this technology can serve numerous other functions that police will find not just useful, but welcome. This versatility makes the idea one of the most promising possibilities for assuring police accountability and compliance with the law to come along in many years." (footnote omitted)); Iesha S. Nunes, *"Hands Up, Don't Shoot": Police Misconduct and the Need for Body Cameras*, 67 FLA. L. REV. 1811, 1815 (2015) ("[B]ody cameras will not only help to increase accountability on behalf of law enforcement, but will also increase the public's trust in those whose duty it is to protect and serve."); Matthew R. Segal & Carol Rose, *Race, Technology, and Policing*, 59 BOS. B.J. lxii, lxii (2015) ("Police departments in Massachusetts and around the nation face heightened scrutiny about racial bias in their stop-and-frisk and use-of-force procedures."); Jocelyn Simonson, *Beyond Body Cameras: Defending a Robust Right to Record the Police*, 104 GEO. L.J. 1559, 1566 (2016) ("With videotaped interrogations, for instance, individuals viewing a video of a confession are more likely to believe the police are being coercive if the video is shot from the point of view of the person being interrogated, pointing at a police officer. When the video is pointed at the suspect, in contrast, viewers are more likely to judge the confession voluntary. Something similar occurs with videos of police conduct: when shot from the point of view of the police officer, as a body camera will do, the 'camera perspective bias' will cause the viewer to sympathize with the officer's actions more than they would with a video taken from a neutral angle or from the perspective of the person engaging with the police officer." (footnote omitted)); Howard M. Wasserman, *Epilogue: Moral Panics and Body Cameras*, 92 WASH. U. L. REV. 845, 848 (2015) ("Even as recent events confirm that body cameras (and the resulting video) are not the infallible solution to police misconduct or to disputes over police-citizen encounters, they reaffirm cameras as worthwhile public policy offering some help in understanding and resolving conflicts between police and their communities."); Howard M. Wasserman, *Moral Panics and Body Cameras*, 92 WASH. U. L. REV. 831, 833 (2015) [hereinafter Wasserman, *Moral Panics*] ("While body cameras are a good idea and police departments should be encouraged and supported in using them, it is nevertheless important not to see them as a magic bullet. The public discussion needs less absolute rhetoric and more open recognition of the limitations of this technology."); V. Noah Gimbel, Note, *Body Cameras and Criminal Discovery*, 104 Geo. L.J. 1581, 1584–85 (2016); Kyle J. Maury, Note, *Police Body-Worn Camera Policy: Balancing the Tension Between Privacy and Public Access in State Laws*, 92 NOTRE DAME L. REV. 479, 481 (2016); Roseanna Sommers, Note, *Will Putting Cameras on Police Reduce Polarization?*, 125 YALE L.J. 1304, 1312 (2016).

though the evidence on their efficacy seems tentative and inconclusive, at best.[16] My goal in this Article is ambitious in one sense, however. Body-camera regimes could inspire future surveillance and data rules, amendments, and opinions that involve other technologies and practices such as biometrics, genomic data, drones, and artificial intelligence. Sustainable and harnessed body-camera regimes could serve as the model, or at least inspiration, for other technologies that sense, store, process, and share information.

My argument proceeds in three parts. In Part I, I argue that the relatively blank slate for police body cameras presents an opportunity for law and policy makers to embrace new privacy notions and strategies that move beyond some of the vexing and misguided concepts entrenched in other areas of surveillance, data protection, and public records law. I briefly review the impetus for police body cameras, the varying interests at stake, and the public and governmental push to adopt use of body cameras. Then, I review the various laws and policies that currently govern body cameras to demonstrate that there is little consensus on both first-order principles, as well as the specifics about what can be collected, how it can be stored and processed, and who can access it. I end this Part by making the case that body cameras are a promising technology to use to chart new trajectories for privacy law because they implicate a wide range of privacy-risky activity like surveillance, data processing, and public dissemination. Also, because body-camera rules are developed from the ground up instead of at the federal level, these rules can be calibrated through experimentation and, ultimately, serve as a firmer foundation for stable change.[17]

In Part II, I address how body cameras are an opportunity to improve how privacy is theorized within the law. I argue that to provide a more nuanced theory of privacy in law, policymakers should abandon the "reasonable expectation of privacy" test for body camera rules. The test is broken and unsalvageable. Lawmakers,

16. Barak Ariel, *Police Body Cameras in Large Police Departments*, 106 J. CRIM. L. & CRIMINOLOGY 729, 729 (2016); Wasserman, *Moral Panics*, *supra* note 15, at 837–40 ("We can only speculate whether recording will deter bad behavior and incentivize good behavior by police and the public. The technology and its use by actual police are too new to know its true effects. . . . [V]ideo does not 'speak for itself.'"); Mayor Muriel Bowser, *Randomized Controlled Trial Metropolitan Police Dep't Body-Worn Camera Program*, LAB@D.C., http://bwc.thelab.dc.gov/#home [https://perma.cc/H8NB-MGCX].

17. *See* THE LEADERSHIP CONFERENCE ON CIVIL & HUMAN RIGHTS & UPTURN, *supra* note 7 (showing that state and local governments are implementing rules and policies for body cameras in support of the argument that states are experimenting with different rules).

courts, officers, and citizens have been tied into knots trying to divine whether a reasonable expectation of privacy exists in particular contexts.[18] The test has given birth to two of the most misguided notions in all of privacy law—the idea that there is no privacy in "public" or in things shared with third parties. Instead, policymakers should create body camera rules that are focused on protecting more nuanced notions of privacy such as trust and obscurity. Trust is a more accurate description of the value to be protected with data storage and processing rules. Trust is also a good construct to guide vendor recipients of body camera data. Obscurity, the notion that we or our data are unlikely to be found or observed in most contexts, is a much more accurate description of the value threatened by surveillance, data collection, and increased data accessibility.[19]

In Part III, I address how body cameras are an opportunity to show how privacy law can be more pliable, holistic, and calibrated to serve multiple values and mitigate abuses of power. I argue that the introduction of body-camera laws provide an opportune time to make a few practical adjustments to address privacy law's design gap.[20] The way that digital and surveillance technologies and systems are built will shape how they are used. Too often, privacy law focuses exclusively on the activities of the surveiller, data collector, or data recipient.[21] Rules for how surveillance technologies and data systems are built and used are also important for body camera systems. I conclude this article by proposing a more holistic framework for states, cities, and departments. This framework combines rules for data practices with rules for the design of technologies. It also embraces a more nuanced conceptualization of privacy. It will help policymakers better respect people's obscurity, trust, and autonomy while balancing the goals of government accountability and freedom of the press. When the concept of privacy is more specifically articulated, it can be better balanced with clearly defined goals relating to public records and speech while avoiding the conflicts

18. *See* Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511–12 (2010) ("The reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency and incoherence.").

19. *See infra* Section II.B.2.

20. *See generally* HARTZOG, *supra* note 14 (explaining there is a general lack of focus on design when it comes to privacy policies). *But see* Ari Ezra Waldman, *A Statistical Analysis of Privacy Policy Design*, 93 NOTRE DAME L. REV. (forthcoming) (manuscript at 103–05), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3141351 [https://perma.cc/A239-SCFK]; Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 78–79 (2018).

21. *See* HARTZOG, *supra* note 14 (manuscript at 4).

inherent in trying to articulate what is a "reasonable expectation of privacy."

If body cameras are to serve as a model for privacy law, policymakers must act soon. Body-camera laws are already being passed.[22] The window of opportunity to redeem privacy law is closing. If lawmakers do not get these rules right, we will be installing yet another omni-surveillance and personal data infrastructure based on notions of privacy that are increasingly myopic and untenable.

I. BODY CAMERAS ARE AN OPPORTUNITY TO SHOW HOW TO FIX PRIVACY LAW

Body cameras have been around for a little while, but they are not yet fully entrenched. In this Part, I will describe why body cameras present a window of opportunity for policymakers to show how to bypass privacy law's most common mistakes. While many police departments have created policies regarding the use of body cameras, not all states have passed formal legislation specifically addressing the policy of body-worn cameras.[23] Even states that have passed body camera-specific legislation are still working on how to implement it, and the window for change remains open.[24] Among those bodies that have passed rules, many important issues regarding things like access and the use of biometrics remain unresolved and in need of attention.[25] With a little imagination and a lot of hard work and political capital, body-camera law could serve as a model for how to improve information privacy law across the board. But lawmakers must act quickly and decisively. The window for change will only be open for a short time. Once states pass rules and law enforcement departments implement the systems, the concrete hardens.

A. The Rush to Implement Body Cameras with No Clear Plan

Body-worn cameras are not entirely new. The idea to use small surveillance cameras mounted on the bodies of police officers has

22. *See* Stoughton, *supra* note 8, at 1380 (explaining that there is a "laundry list of advantages" for body-worn cameras and addressing the rapid rate at which police body cameras are being implemented throughout the United States).

23. *See* THE LEADERSHIP CONFERENCE ON CIVIL & HUMAN RIGHTS & UPTURN, *supra* note 7 (noting that a few cities in some states have put in place body-camera rules and -policies).

24. *See generally* Mateescu et al., *supra* note 6 (noting that there are areas of body camera-policy which still need to be addressed even in cities where there are policies regarding body cameras).

25. *Id.*

been the subject of public debate at least as early as the 2000s.[26] Dash cams have been around in some form since the 1960s and have been in common use since the 1990s.[27] However, when Michael Brown was shot and killed by Ferguson, Missouri, police officer Darren Wilson under controversial circumstances, the public outcry for policy body cameras intensified.[28] The demand to record police interactions with the public also increased following the deaths of African American men Philando Castile, Freddie Grey, Samuel DuBose, Sean Bell, Eric Garner, Alton Sterling, and others, all of whom died following police encounters.[29]

Remarkably, there is a convergence of interest in seeking to implement police body cameras. Governments, law enforcement organizations, police officers unions, civil rights organizations, the general public, and certainly the body-camera equipment and data industry all, to some degree, support the implementation of body-worn cameras for police officers.[30] Unfortunately, there is little clear consensus on what the rules for body cameras should be or how they should be implemented. Body-camera laws vary dramatically from city to city and state to state with respect to officer discretion over camera activation, footage review rights for officers, privacy, biometric use, and footage retention, use, and accessibility.[31] Even model policies proposed by unions and civil rights organizations are

26. *See, e.g.,* Harris, *supra* note 15, at 360–61 (discussing the use of body-worn cameras in the United Kingdom and the United States as early as 2005).

27. INT'L ASS'N OF CHIEFS OF POLICE, THE IMPACT OF VIDEO EVIDENCE ON MODERN POLICING 5 (2004), https://www.bja.gov/bwc/pdfs/IACPIn-CarCameraReport.pdf [https://perma.cc/Y9YD-HCPY].

28. *See* Adam Lidgett, *How Body Camera Manufacturers Are Cashing in on Michael Brown's Ferguson Death*, INT'L BUS. TIMES (Oct. 8, 2015), http://www.ibtimes.com/how-body-camera-manufacturers-are-cashing-michael-browns-ferguson-death-2123677 [https://perma.cc/W3QM-68W4]; Josh Sanburn, *The One Battle Michael Brown's Family Will Win*, TIME (Nov. 26, 2014), http://time.com/3606376/police-cameras-ferguson-evidence/ [https://perma.cc/KT5U-MUGW] ("In the weeks after Brown's death, numerous law-enforcement agencies around the U.S. began experimenting with body cameras. Anaheim, Calif.; Denver; Miami Beach; Washington, D.C.; and even Ferguson have all begun outfitting officers with cameras or announced plans to start. The movement Brown's family called for the night Wilson was cleared has actually been growing since the day their son was killed.").

29. *See* Daniel Funke & Tina Susman, *From Ferguson to Baton Rouge: Deaths of Black Men and Women at the Hands of Police*, L.A. TIMES (July 12, 2016, 3:45 PM), http://www.latimes.com/nation/la-na-police-deaths-20160707-snap-htmlstory.html [https://perma.cc/X5GM-E4TU)].

30. Mateescu et al., *supra* note 6, at 1, 7.

31. *See* THE LEADERSHIP CONFERENCE ON CIVIL AND HUMAN RIGHTS & UPTURN, *supra* note 7.

different from each other along similar fault lines.[32] The policies developed by local police departments also vary, to the extent that they are even accessible.[33] And this is to say nothing of the different kinds of contracts between governments and third-party body-camera equipment and data vendors. These contracts shape the influence that private industry has over the surveillance technologies and the data they create.[34]

The general ambiguity and uncertain goals for police body cameras likely play a role in its collective appeal to the relevant parties. It is not clear if the cameras are meant to change behavior, provide evidence of interactions, or increase public trust (or all of those things).[35] So for now, body cameras can be all things to all people. But, if body cameras are to be safe and sustainable, specific first-order principles should be identified and agreed upon. Sooner or later, concrete rules will need to be articulated in those jurisdictions that have yet to regulate the use of body cameras. This includes rules designed to protect the privacy of those surveilled and implicated by surveillance.

B. The Window of Opportunity to Change Privacy Law

Given how long courts and lawmakers have been wrestling with privacy issues, you might be tempted to think they would have it worked out by now. Sadly, you would be wrong. Despite over one hundred years of attempting to create a sound body of privacy rules and jurisprudence, courts, lawmakers, and the general public remain confused about how to best protect the protean concept of privacy.[36]

32. *Compare A Model Act for Regulating the Use of Wearable Body Cameras by Law Enforcement*, ACLU, https://www.aclu.org/other/model-act-regulating-use-wearable-body-cameras-law-enforcement?redirect=model-act-regulating-use-wearable-body-cameras-law-enforcement [https://perma.cc/R7DA-4TQD] ("A law enforcement officer who is wearing a body camera shall notify the subject(s) of the recording that they are being recorded by a body camera as close to the inception of the encounter as is reasonably possible."), *with "Model" Body-Camera Policy*, LAB. REL. INFO. SYS. (Sept. 12, 2014), https://lris.com/2014/09/12/model-body-camera-policy/ [http://perma.cc/5DMG-KSGS] (follow "LRIS" hyperlink; then follow "PDF Version" hyperlink) ("Officers have no obligation to stop recording in response to a citizen's request if the recording is pursuant to an investigation, arrest, lawful search, or the circumstances clearly dictate that continued recording is necessary. However, officers . . . may evaluate the situation and . . . honor the citizen's request.").

33. *See* THE LEADERSHIP CONFERENCE ON CIVIL AND HUMAN RIGHTS & UPTURN, *supra* note 7.

34. For more information on these contracts, see Joh, *supra* note 5.

35. *See* Stoughton, *supra* note 8, at 1380–1400 (discussing views and potential benefits of body cameras).

36. *See infra* Part II.

Admittedly, creating rules around a concept as complex as privacy is a daunting task. For starters, the concept defies definition.[37] Is privacy about secrecy, intimacy, control, identity, or dignity? Or something else entirely? Regardless of how it is defined, it is often in tension with other values, such as free speech, safety, accountability, and innovation. Sometimes, privacy means rules about what other people can disclose. Sometimes, privacy means law enforcement might have difficulty obtaining information it needs to keep people safe. Privacy is also an astonishingly cross-cutting concept within legal systems, having relevance in the law of torts, contracts, consumer protection, constitutional free expression, self-incrimination and due process rights, evidence, equity, and many others.[38] Statutes that address government search and seizure, public health, electronic surveillance, data protection, public records, and many more all accommodate some notion of privacy.

The problem is that courts and lawmakers do not seem to be getting any closer to a workable consensus. The debate over what constitutes a privacy "harm" is still wide open.[39] Courts demand "concrete" injury, but even that remains elusive.[40] Is increased risk an injury in itself? Anxiety over information misuse?[41] Regulatory agencies like the FTC are accused of overreach in their failure to properly and publicly identify privacy harms and balance them with privacy benefits.[42] Courts and lawmakers are struggling to articulate

37. *Cf.* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 479–82 (2006) (discussing the present lack of consensus surrounding the definition of "privacy" and its associated body of laws and suggesting a taxonomy to aid in its development).

38. *See, e.g.*, *id.* at 483; Marcy E. Peek, *Information Privacy and Corporate Power: Towards a Re-Imagination of Information Privacy Law*, 37 SETON HALL L. REV. 127, 129 (2006).

39. *See* Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L. J. 1131, 1133 (2010) (offering an account of privacy harm "delineating [its] specific boundaries"); Robert L. Rabin, *Perspectives on Privacy, Data Security, and Tort Law*, 66 DEPAUL L. REV. 313, 324–28 (2017).

40. *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548–50 (2016) (ruling that because the Ninth Circuit "failed to fully appreciate the distinction between concreteness and particularization, its standing analysis was incomplete"); Rabin, *supra* note 39, at 327–28.

41. Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data Breach Harms*, 96 TEX. L. REV. 737, 754 (2018) ("Most courts consider plaintiffs' fear, anxiety, and psychic distress about their increased risk of identity theft and other abuses too remote to warrant recognition.").

42. *See* Angelique Carson, *LabMD Argues 'Matter of Principle' in FTC Data- Security Appeal*, INT'L ASS'N OF PRIVACY PROFESSIONALS (IAAP) (June 26, 2017), https://iapp.org/news/a/11th-circuit-hears-arguments-in-labmd-v-ftc-appeal/ [https://perma.cc/GVA4-FBV5]; Lesley Fair, *Third Circuit Rules in FTC v Wyndham Case*, FED. TRADE COMM'N (Aug. 25, 2015), https://www.ftc.gov/news-events/blogs/business-blog/2015/08/third-circuit-rules-ftc-v-wyndham-case [https://perma.cc/F9XR-9MTG].

the boundaries of surveillance for new technologies like cellphone-tower interception devices and license plate reader technologies, existing technologies like GPS trackers for cars, and even common technologies like the smartphone.[43]

Unsurprisingly, this breadth and ambiguity has resulted in a body of privacy law in the United States that is loosely grouped to communally serve some conceptualization of privacy. Despite this vague common purpose, most areas of privacy law in the U.S. are siloed and developed organically from the bottom-up, rather than a unified set of principles producing rules that flow from the top-down. Not all frameworks deal with a full range of privacy problems. Some target surveillance.[44] Others target problems with data processing.[45] Still others deal with the disclosure of private information.[46] Holistic frameworks that address the lifecycle of information are limited in scope. And there is no requirement that these rules be consistent with each other.

This balkanization of privacy law in the U.S. has made change an atomized process. No one area has been able to serve as a perfect model for another.[47] Some pockets of privacy law seem strangely ossified. The original privacy torts—intrusion upon seclusion, disclosure of privacy facts, misappropriation of name or likeness, and depicting another in a false light—have failed to develop much since their inception.[48] They are limited by the First Amendment and specific harm requirements in addition to a general skepticism by courts.[49] Notwithstanding a chorus of voices in industry and civil society begging for reform, the last time Congress seriously revisited the U.S. electronic surveillance laws was in the mid-1980s. When the Electronic Communications Privacy Act was passed in 1986, computers were outrageously expensive and the computing practices and business models that shaped the rules were quite different than

43. *See* Riley v. California, 134 S. Ct. 2473, 2484–85 (2014); United States v. Jones, 565 U.S. 400, 402 (2012); Carpenter v. United States, 819 F.3d 880, 887 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017).

44. *See, e.g.*, Thomas B. Kearns, Note, *Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns*, 7 WM. & MARY BILL RTS. J. 975, 977–78 (1999).

45. *See, e.g.*, Joseph A. Tomain, *Online Privacy & The First Amendment: An Opt-In Approach to Data Processing*, 83 U. CIN. L. REV. 1, 4–5 (2014).

46. *See, e.g.*, Solove, *supra* note 37, at 530–35.

47. *See id*. at 483 (explaining that the "vast and complex" nature of American privacy law necessitates a "new taxonomy to address privacy violations for contemporary times").

48. *See, e.g.*, Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1189–90 (2010).

49. *Id.* at 1901–02.

they are now.[50] Even the new data protection rules that have been passed in the last forty years like the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Gramm-Leach-Bliley Act ("GLBA") follow the same general set of principles, the fair information practices, or "FIPs."[51] These basic data rules have not changed much since they were conceived in the 1970s.

This ossification has stuck privacy law into a pattern of perpetuating its deficiencies. The persistent mistakes surrounding the conceptualization of privacy seem most visible. Courts and lawmakers keep defining privacy in narrow ways, such as secrecy, ignoring privacy in social contexts and new potential misuses of privacy information. For example, there are few rules that meaningfully mitigate the disparate impact that surveillance and data practices can have on vulnerable and minority communities.[52] Privacy law is often treated as separate from anti-competition law.[53] It is too often silent on how technologies are used to manipulate people in subtle and adversarial ways, or how companies employ powerful algorithms in opaque ways with little accountability.[54]

Courts and lawmakers in privacy disputes cling to binary maxims like "no privacy in public" or "no privacy in information shared with third parties" instead of engaging with more nuanced notions of privacy that require difficult balances with speech, security, and

50. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2522 (2016)); Rainey Reitman, *Deep Dive: Updating the Electronic Communications Privacy Act*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/deeplinks/2012/12/deep-dive-updating-electronic-communications-privacy-act [https://perma.cc/988Y-XV2X]; Brad Smith, *Modern Digital Data Laws That Balance Law Enforcement Needs With Privacy Can Create A Model For The World*, MICROSOFT, https://blogs.microsoft.com/on-the-issues/2017/06/15/modern-digital-data-laws-balance-law-enforcement-needs-privacy-can-create-model-world/#sm.00008opdpuw5pfn9scn1oi8nnyy98 [https://perma.cc/2WJF-22FX].

51. *See* Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 29 U.S.C. and 42 U.S.C.); Financial Services Modernization (Gramm-Leach-Bliley) Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12, 15, and 16 U.S.C.); Woodrow Hartzog, *The Inadequate, Invaluable Fair Information Practices*, 76 MD. L. REV. 952, 953–54 (2017).

52. *See* Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CALIF. L. REV. 671, 677 (2016); Woodrow Hartzog, *Unfair and Deceptive Robots*, 74 MD. L. REV. 785, 785 (2015); Andrew P. Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109, 115–16 (2017).

53. *See* MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA & COMPETITION POLICY 55 (2016).

54. *See* FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 19–20, 103 (2015); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008).

autonomy, and often unsatisfying compromises and line-drawing exercises.[55] Bright-line rules like the "third-party doctrine" are justiciable and easy to work with, but as I will discuss in Part II, they are too often under inclusive of privacy interests. Sometimes privacy harms are individually small but widely dispersed, like subtle forms of manipulation using personal information to target your weak points or the collective loss of massive data breaches.

In short, privacy law seems stuck. It is still grappling with old problems even as new ones are on the way. Inertia might explain some of this state of affairs. It is hard to change entrenched systems. It is even harder, and often unwise, to propose something entirely new. Established rules can reflect custom, wisdom, and feasibility. However, body cameras provide a unique opportunity to create at least a workable model for change. This technology implicates a broad spectrum of privacy threats along the entirety of the information lifecycle and requires a framework that addresses them all, from surveillance and data collection to data storage and use to data access and dissemination. Body cameras implicate problems that are addressed in electronic surveillance law, data and consumer protection law, public records rules, and free expression doctrine. Because police body-camera rules can be created locally, they can develop in an organic and stable way through dispersed experimentation and revision.

1. Surveillance

The primary function of policy body cameras is surveillance. danah boyd and Alex Rosenblat wrote, "[s]urveillance has an economic and social price. Advocates [of body cameras] hope that the psychological cost of being watched will dissuade officers from abuse, but members of these communities will face these costs too."[56] They noted that "[p]olice-worn body cams do not face the police. They face members of the community—everyday people doing everyday things. The goal may be to capture criminal activities by civilians and by police, but to get there, these cameras will film people walking down the street minding their business."[57] Body cameras can capture people at their most vulnerable. They can also reveal things through persistent surveillance that people do not anticipate, even in public. Even the mere knowledge of surveillance can result in chilling effects

55. *See infra* Section II.B.
56. boyd & Rosenblat, *supra* note 8.
57. *Id.*

and harms to autonomy.[58] The dangers of surveillance have been long studied and articulated by scholars.[59] The worst burden of surveillance will be felt by the most vulnerable and underrepresented communities.[60]

In addition to the specific surveillance harms against individuals, the push for body cameras represents an even more ominous threat of the slow but persistent creep to expand surveillance systems into all areas of our life. Once these systems are built, it is incredibly difficult to curtail and mitigate their influence over us. The mere existence of cameras will increase their demand. For example, in the aftermath of the police shooting of Justine Damond at her home in Minnesota, many publicly asked why the officers' body cameras had not been activated.[61] The mere presence of cameras will likely lead to questions like "if you have the cameras, why don't you use them?"[62] The absence of footage could be seen as evidence of wrongdoing,[63] even if that presumption is not justified. The result is a one-way ratchet that will steadily demand and facilitate more surveillance in the absence of clear, justified, and feasible rules that limit when a camera is to be on capturing video and audio.

2. Data Protection

Body cameras also implicate the concerns about how organizations collect, store, use, and share personal data. Elizabeth

58. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935, 1945 (2013).

59. *Id.* at 1934–36. *See generally* GARY T. MARX, WINDOWS INTO THE SOUL: SURVEILLANCE AND SOCIETY IN AN AGE OF HIGH TECHNOLOGY (2016) (addressing concerns such as the abuse of surveillance by "offering a framework that more systematically defines surveillance questions with respect to structure, organization, practice, function, and process" (footnote omitted)).

60. boyd & Rosenblat, *supra* note 8 ("Those who will be surveilled by body-worn cameras are already the most marginalized members of society, and they already experience a disproportionate amount of surveillance from other law-enforcement cameras. This is particularly true for people who lack private residences to retreat to, either because they are homeless or are resident[s] in public housing, where the police have greater freedom to enter over a resident's objection.").

61. Gordon Severson, *Expert: Body Cameras Should Have Recorded Australian Woman's Shooting*, USA TODAY (July 19, 2017), https://www.usatoday.com/story/news/nation-now/2017/07/19/body-cameras-should-have-recorded-justine-damond-shooting/491064001/ [https://perma.cc/5CS6-6LGV].

62. Wasserman, *Moral Panics*, *supra* note 15, at 842 ("As police cameras become more pervasive, it becomes impossible to escape demands—from courts, litigants, juries, citizens, the media, and civilian review boards—that cameras always will be used, that video always will be available.").

63. *Id.* (stating that people will demand the use of body cameras and "the absence of video evidence is itself suspicious and suggestive of misconduct").

Joh wrote that the data generated by body cameras present just as much of a challenge as their surveillance capabilities.[64] She argues, "Police body camera policies must address not only concerns about surveillance, but also data control. The absence of clear data control policies will result in confusion, both for the police and the public, about who has access to see, share, and delete data produced from body-worn cameras."[65] According to Joh, "without strong presumptions in favor of sharing the data with the public, the reform, accountability, and legitimacy potential of body worn cameras will go unfulfilled."[66] However, making data public in a safe and sustainable way is challenging.

Data harms are wide-ranging and pervasive.[67] Personal information can reveal secrets and confidences, but it can also be misused against the data subject and others. Our data reveals what makes us tick and can be used to manipulate us. For example, Ryan Calo has observed that personal information can be leveraged for the "mass production of bias," "disclosure ratcheting," and "means-based targeting."[68] He calls this a kind of "digital market manipulation."[69]

Personal data also presents systemic threats. Data powers automated technology and machine learning. It is used to power decision-making algorithms that can reinforce human biases[70] and have disparate impacts on minority and vulnerable populations. In previous research, I have written that "[d]ecisions that used to be made by humans based upon a small amount of information are now going to be made by automated software based upon exabytes of data."[71] Danielle Citron has said that computers are increasingly the primary decision-makers in systems that have significant consequences for humans.[72] Automated decision-making systems now leverage personal data when terminating "individuals' Medicaid, food

64. Joh, *supra* note 3, at 133.

65. *Id.*

66. *Id.*

67. M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133 (2011) (categorizing the wide range of date harms into objective and subjective).

68. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1007, 1012, 1015 (2014).

69. *Id.* at 1051.

70. Hartzog, *supra* note 51, at 971.

71. *Id.* at 970. An exabyte is 1 billion gigabytes. *See* Daniel Price, *Surprising Facts and Stats About the Big Data Industry*, CLOUDTWEAKS (Mar. 17, 2015), http://cloudtweaks.com/2015/03/surprising-facts-and-stats-about-the-big-data-industry/ [https://perma.cc/5EC3-J8WM].

72. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1252 (2008).

stamp, and other welfare benefits,"[73] as well as excluding people from air travel.[74] Citron observed that "[c]omputer programs identify parents believed to owe child support and instruct state agencies to file collection proceedings against those individuals. Voters are purged from the rolls without notice, and small businesses are deemed ineligible for federal contracts."[75] Therefore, data collection and processing implicates serious due process issues,[76] disparate impact on minority and other vulnerable communities,[77] and invasions of privacy and stigmatization due to the predictive power of data analytics.[78]

Further, soon it might not even be possible to opt out of automated decision-making. Danielle Citron and Frank Pasquale have warned that we are at risk of becoming what they call a "scored society," whereby people are assigned numbers similar to credit scores, but for everything.[79] Industry is also working to deploy algorithmic decision making to rank, file, and sort us in nearly every way imaginable, including many that people have yet to realize.[80] Our subjugation to algorithms has already started. China aims to "give every citizen a score based on behavior such as spending habits, turnstile violations[,] and filial piety, which can blacklist citizens from loans, jobs, [and] air travel."[81] The sustainability, safety, and efficacy

73. *Id.* at 1252, 1256, 1268–73 (discussing the issuance of hundreds of thousands of incorrect Medicaid, food stamp, and welfare eligibility determinations across numerous state programs as an example of a failed automated system).

74. *Id.* at 1252, 1274–75 (discussing erroneous classifications, in which innocent individuals are mistakenly identified as terrorists, on the "No Fly" list).

75. *Id.*

76. *See generally id.* (discussing the threat data collection and processing, specifically in the context of automated systems, poses to due process).

77. *See generally* Barocas & Selbst, *supra* note 52 (positing that data mining can perpetuate discriminatory behavior, often by picking out proxy variables for protected classes).

78. Woodrow Hartzog & Evan Selinger, *Big Data in Small Hands*, 66 STAN. L. REV. ONLINE 81, 83–85 (2013); Ian Kerr & Jessica Earle, *Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy*, 66 STAN. L. REV. ONLINE 65, 71–72 (2013), https://review.law.stanford.edu/wp-content/uploads/sites/3/2016/08/66_StanLRevOnline_65_KerrEarle.pdf [https://perma.cc/UAC6-66M4].

79. Danielle K. Citron & Frank Pasquale, *The Scored Society: Due Process for Automated Predictions*, 89 WASH. L. REV. 1, 2–4, 8 (2014); *see also* PASQUALE, *supra* note 54, at 191–92 (2015); Tal Z. Zarsky, *Understanding Discrimination in the Scored Society*, 89 WASH. L. REV. 1375, 1376 (2014) (identifying discrimination as an additional concern related to the emergence of a scored society).

80. *See* Citron & Pasquale, *supra* note 79, at 3–4, 8 (citing the secrecy of the scoring systems and metrics as a major criticism to the emergence of a scored society).

81. Josh Chin & Gillian Wong, *China's New Tool for Social Control: A Credit Rating for Everything*, WALL ST. J. (Nov. 28, 2016, 11:46 AM),

of these systems depends upon whether we have rules for how they are built and used.[82]

Kate Crawford and Ryan Calo have argued that "[a]utonomous systems are already deployed in our most crucial social institutions, from hospitals to courtrooms. Yet there are no agreed methods to assess the sustained effects of such applications on human populations."[83] Body cameras are a great opportunity to create rules that understand how data and automation will impact people, culture, and politics, because these technologies will likely seek to leverage algorithms and automated decision-making, yet their rules and policies remain nimble and dispersed. There is room for experimenting with rules without disrupting the whole.[84]

3. Public Records and Public Disclosure

Finally, body cameras raise incredibly important questions about what constitutes a public record, who gets to access those records and under what circumstances, how they access them, and what can be done with them upon disclosure.[85] Public records laws are critical for

http://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590 [https://perma.cc/JX77-MNBG (dark archive)].

82. Hartzog, *supra* note 51, at 971.

83. Kate Crawford & Ryan Calo, *There Is a Blind Spot in AI Research*, 538 NATURE 311, 311 (2016).

84. For more on the important role that states play with algorithmic accountability, see Julia Powles, *New York City's Bold, Flawed Attempt to Make Algorithms Accountable*, NEW YORKER (Dec. 20, 2017), https://www.newyorker.com/tech/elements/new-york-citys-bold-flawed-attempt-to-make-algorithms-accountable [https://perma.cc/HNL4-8U4C] (discussing legislation in New York to create a task force that will examine the state's automated decision systems).

85. *See, e.g.*, Mary D. Fan, *Privacy, Public Disclosure, Police Body Cameras: Policy Splits*, 68 ALA. L. REV. 395, 435–36 (2016) (arguing for safe harbor laws that encourage automated redaction of records and incentivize the development of redaction technology); Brian Liebman, Recent Development, *The Watchman Blinded: Does the North Carolina Public Records Law Frustrate the Purpose of Police Body Cameras?*, 94 N.C. L. REV. 344, 348 (2015) (arguing that "unless the public records law is changed to allow the public, rather than the police, to decide when footage of potential police misconduct should be released, the beneficial effects of body cameras will be frustrated."); Richard Lin, Note, *Police Body Worn Cameras and Privacy: Retaining Benefits While Reducing Public Concerns*, 14 DUKE L. & TECH. REV. 346, 365 (2016) (suggesting "shortening data retention policies, tagging videos, and using redaction technology" to balance privacy and disclosure concerns with evidentiary and accountability benefits of body cameras); Chris Pagliarella, Comment, *Police Body-Worn Camera Footage: A Question of Access*, 34 YALE L. & POL'Y REV. 533, 534 (2016) ("BWC programs *must* provide full footage access to the victims of suspected undue police violence and their families—allowing for an accountability baseline and setting victims' rights as paramount. Public record policies should not impede this core goal by imposing public access where the associated costs could stymie such programs altogether." (emphasis in original)); Joseph Wenner, Comment, *Who Watches the Watchmen's Tape? FOIA's Categorical Exemptions and*

government accountability and journalism in the public interest. Generally, public records laws dictate the type of records created or stored by government entities that will be made available to anyone that requests them and the circumstances under which they will be released or withheld.[86] But the concept of public records also has blurry edges. Black's Law Dictionary defines a public record as "[a] record that a governmental unit is required by law to keep."[87] One of the central questions in the law of public records concerns which public records should be ultimately released—and which should not—based on certain policy considerations, including privacy.[88]

Two major privacy issues related to public records arise when they are aggregated into massive datasets that dramatically reduce the search costs for the curious and when they include information that is already "public" or involves "public surveillance."[89] First, people's names, ages, addresses, and similar regularly disclosed information might not be seen as "private" in the traditional sense of the word but can still be used in adverse ways against them.[90] Courts and lawmakers regularly consider much of this information to be public and thus not subject to a public records privacy exemption, perhaps because we expose and share this information with others all the time. The same holds true for the release of surveillance that occurred "in public." There is a litany of cases that hold surveillance in public spaces and in "plain view" does not infringe a reasonable expectation

Police Body-Worn Cameras, 2016 U. CHI. LEGAL F. 873, 876 (arguing that "examining the applicability of exemptions to body-worn camera videos on a case-by-case basis strengthens their transparency benefits without unduly eroding personal privacy or the integrity of ongoing investigations.").

86. *See generally* ACCESS TO GOVERNMENT IN THE COMPUTER AGE: AN EXAMINATION OF STATE PUBLIC RECORDS LAWS (Martha Harrell Chumbler ed., 2007) (discussing the public records laws of several states and the federal government).

87. *Public Record*, BLACK'S LAW DICTIONARY (10th ed. 2014).

88. *See* David S. Ardia & Anne Klinefelter, *Privacy and Court Records: An Empirical Study*, 30 BERKELEY TECH. L.J. 1807, 1807, 1813 (2015); Grayson Barber, *Personal Information in Government Records: Protecting the Public Interest in Privacy*, 25 ST. LOUIS U. PUB. L. REV. 63, 63 (2006); Amanda Conley et. al., *Sustaining Privacy and Open Justice in the Transition to Online Court Records: A Multidisciplinary Inquiry*, 71 MD. L. REV. 772, 774 (2012); Jane E. Kirtley, *"Misguided in Principle and Unworkable in Practice": It Is Time to Discard the Reporters Committee Doctrine of Practical Obscurity (and Its Evil Twin, the Right to Be Forgotten)*, 20 COMM. L. & POL'Y 91, 109 (2015); Samuel A. Terilli & Sigman L. Splichal, *Public Access to Autopsy and Death-Scene Photographs: Relational Privacy, Public Records and Avoidable Collisions*, 10 COMM. L. & POL'Y 313, 322 (2005).

89. *See* Solove, *supra* note 14, at 1138; *see also* Ardia & Klinefelter, *supra* note 88, at 1807–08; Conley et. al., *supra* note 88, at 777 ("[C]ourts have an obligation to rewrite rules governing the creation of, and access to, public court records in light of substantive changes that online access augurs.").

90. *See* Solove, *supra* note 14, at 1138.

of privacy.[91] Second, another concern with such a dramatic increase in public records is the great potential and incentives for companies to exploit data for their own personal gain, rather than for public accountability purposes.[92] Will body-camera vendors be able to sell or export the data it captures and stores?[93] Or might this data somehow end up in the hands of unscrupulous businesses that post embarrassing information about people gleaned from public records, like mugshots, then charge a high fee to have that information taken down?[94]

Police body-camera rules should grapple with the privacy implications of exabytes[95] of surveillance data being made available as public records. Many of them already do. But questions remain. When should data be deleted? In what format should footage be made available and how soon? Should police-body camera footage and data be somehow redacted or obfuscated? Should access be granted only subject to certain restrictions on further use or dissemination? Public records laws have existed for a long time. Lawmakers do not often have the occasion or impetus to wholesale

91. *See, e.g.*, Horton v. California, 496 U.S. 128, 136–137 (1990); California v. Greenwood, 486 U.S. 35, 40–41 (1988); California v. Ciraolo, 476 U.S. 207, 215 (1986) ("The Fourth Amendment simply does not require police traveling in the public airways at 1,000 feet to obtain a warrant in order to observe what is visible to the naked eye." (footnote omitted)); United States v. Legg, 18 F.3d 240, 242 (4th Cir. 1994); Daily Times Democrat v. Graham, 162 So. 2d 474, 476 (Ala. 1964) (noting that there was no expectation of privacy at a fair but permitting a tort suit by a woman who was photographed at a county fair with her skirt blown up over her head, relying in part on the fact that the photographer was lying in wait to catch the woman in an embarrassing situation); Creel v. I.C.E. & Assocs., Inc., 771 N.E.2d 1276, 1276 (Ind. Ct. App. 2002); Patricia Sánchez Abril, *Recasting Privacy Torts in A Spaceless World*, 21 HARV. J. L. & TECH. 1, 6, 18 (2007) ("Courts have generally held that anything capable of being viewed from a 'public place' does not fall within the privacy torts' protective umbrella. . . . Under the Restatement, an individual cannot have a reasonable expectation of privacy in any public place. More formally, any activity that is visible to the public eye—whether that eye is human or mechanical—is not actionable under the public disclosure tort. For example, courts have found that there is no reasonable expectation of privacy in a restaurant, in a church service, or at a county fair.") (footnotes omitted)).

92. *See* Margaret B. Kwoka, *Inside FOIA, Inc.*, 126 YALE L.J. F. 265, 266 (2016); Margaret B. Kwoka, *FOIA, Inc.*, 65 DUKE L.J. 1361, 1361, 1377 (2016) [hereinafter Kwoka, *FOIA, Inc.*].

93. *See, e.g.*, Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 959 (2004); Solove, *supra* note 14, at 1138.

94. *See, e.g.*, David Segal, *Mugged by a Mugshot*, N.Y. TIMES (Oct. 5, 2013), http://www.nytimes.com/2013/10/06/business/mugged-by-a-mug-shot-online.html [https://perma.cc/ZX5J-GQA7 (dark archive)].

95. "A unit of information equal to one quintillion (10^{18}) or, strictly, 2^{60} bytes." *Exabyte*, OXFORD ENG. DICTIONARY, https://en.oxforddictionaries.com/definition/exabyte [https://perma.cc/K3TD-T7HS].

reimagine a public records framework that better balances government transparency and accountability with more nuanced conceptualizations of privacy. But body cameras are just such an opportunity.

* * *

Because body-camera systems leverage sensors, algorithms, and data in ways that implicate privacy, government transparency, and free speech, they are an opportunity to modify surveillance, data, and public records rules all at once and stake out new ground at the municipal and state levels. This kind of ground-up federalism has the benefit of flexibility and more stable foundation over time. For example, Paul Schwartz has argued that states can be "laboratories for innovations in information privacy law."[96] Regarding drones—another surveillance technology that necessitates new rules—Margot Kaminski has written that the tension between privacy and First Amendment freedom is better resolved by the states than an attempt by the federal government to resolve the tension in "one fell swoop."[97] According to Kaminski, federal legislation is expensive, burdensome to enact, and more likely to be overturned by courts. She argues, "[r]ather than attempt to get federal legislation right on the first try, and risk having it rejected by First-Amendment-protective courts, we should allow states to run through less costly iterations."[98] Kaminski's argument resonates with body cameras as well.

Given the state's interest and providence regarding policing, body-camera law is less likely to be preempted by federal legislation than privacy rules for drones, which have caught the attention of federal regulators like the Federal Aviation Administration ("FAA").[99] Cities and states have an increasingly important role to play in privacy law. Body-camera law is a good example of what Ira Rubinstein calls "privacy localism," a focus on municipal and state privacy rules. Rubinstein argues that privacy localism is important because "privacy issues are highly salient to cities" in light of big data policing and the "smart city" movement, that cities have significant flexibility to create privacy rules due to the lack of privacy legislation at the state and federal level, and cities have historically been more willing than state governments or the federal government to try out

96. Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 916 (2009).

97. Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CALIF. L. REV. CIR. 57, 64 (2013).

98. *Id.*

99. *Unmanned Aircraft Systems*, FEDERAL AVIATION ADMINISTRATION, https://www.faa.gov/uas/ [https://perma.cc/J9JK-99UN].

innovative new privacy protections.[100] This Article echoes Rubinstein's calls for privacy localism, particularly with respect to body-worn cameras.

To meaningfully address the faults of privacy law, lawmakers and courts must act quickly. Cities and states are already passing or considering legislation. Policies are already getting adopted and the cameras, systems, and storage software are already being built. But if law and policy makers seize the moment and explicitly move beyond traditional notions of the data protection and the fatally flawed "reasonable expectations of privacy" test, they can start a revolution.

II. REFINING THEORY: GET RID OF THE REASONABLE EXPECTATIONS OF PRIVACY TEST

Lawmakers and courts should not rely on the concept of a "reasonable expectation of privacy" as a threshold for body camera privacy rules. This concept is entrenched, so it is easy to see why lawmakers might look to it when crafting rules for body cameras. It determines the scope of protections under the Fourth Amendment and other aspects of privacy law, including the privacy torts, surveillance statutes, and public records law.[101] The test for determining the boundaries of surveillance and data practices was popularized in the influential case of *Katz v. United States*.[102] Ostensibly, in order to determine whether surveillance or data practices are allowable, courts and lawmakers are to ask whether an individual has an actual, subjective expectation of privacy and also whether society recognizes that expectation as reasonable.[103] In theory, this test fits alongside the longstanding tradition of

100. Ira Rubinstein, *Privacy Localism* 6–7 (N.Y.U. Sch. Of L., Working Paper No. 18-18, 2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124697 [https://perma.cc/V7NF-TVBM].

101. *See, e.g.*, Katz v. United States, 389 U.S. 347, 351–52 (1967); *see also* Solove, *supra* note 18, at 1512–13.

102. 389 U.S. at 353.

103. *See id.* at 352 (stating that Katz, seeking to exclude the uninvited ear, is entitled to assume that his conversation will be private when he enters the telephone booth). *But see* Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 114 (2015) ("This Essay argues that *Katz* is only a one-step test. Subjective expectations are irrelevant. A majority of courts that apply *Katz* do not even mention the subjective inquiry; when it is mentioned, it is usually not applied; and when it is applied, it makes no difference to outcomes.").

"reasonableness" thresholds within the law.[104] In practice it has not worked out that well.

This test has far outlived its usefulness. The concept of privacy is far too vague and difficult to define for it to be deployed as a term of art. Additionally, the reasonableness test too often defaults into descriptive accounts of both people and society's actual expectations of secrecy, rather than normative accounts of which personal boundaries *should* be protected.[105]

So far, several cities and states have already made the mistake of relying upon reasonable expectations of privacy for body-camera rules. According to research conducted by The Leadership Conference & Upturn, as of August 2016, of the major cities they studied that have enacted body-camera policies, many either prohibit or mitigate recording or regulate data use and access in contexts where individuals have a "reasonable expectation of privacy."[106] For example, in Philadelphia police body cameras cannot be used or activated "[i]n places where a reasonable expectation of privacy exists

104. *See* Benjamin C. Zipursky, *Reasonableness in and out of Negligence Law*, 163 U. PA. L. REV. 2131, 2146 (2015) (surveying the various uses of "reasonableness" in the law and noting that it is the standard for Fourth Amendment search and seizure cases).

105. *See* Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 149 (2016).

106. *See* THE LEADERSHIP CONFERENCE ON CIVIL AND HUMAN RIGHTS & UPTURN, *supra* note 7. Boston uses the concept of "reasonable expectation of privacy" to limit officers' discretion when choosing to record but then provides a longer list of considerations for officers in privacy-sensitive contexts without actually deploying the specific language and concept of "reasonable expectations":

> BWC officers should be mindful of locations where recording may be considered insensitive, inappropriate, or may be prohibited by privacy policies. Such locations may include locker rooms, places of worship, religious ceremonies, certain locations in hospitals or clinics, law offices, day care facilities, etc. At such locations, at the officer's discretion and based on the circumstances, BWCs may be turned off. The officer may consider the option to divert the BWC away from any subjects and record only audio, if appropriate. When exercising discretion in such situations, the decision whether to stop recording, divert the BWC, or record only audio should generally be based on the following BWC Discretionary Recording Considerations: the extent to which the officer observes activities or circumstances of a sensitive or private nature; the presence of individuals who are not the subject of the officer-civilian interaction; the presence of people who appear to be minors; any request by a civilian to stop recording; and the extent to which absence of BWC recording will affect the investigation.

BOS. POLICE DEP'T, POLICE COMM'R'S SPECIAL ORDER NO. 16-023: BODY-WORN CAMERA PILOT PROGRAM POLICY § 2.4 (2016), https://static1.squarespace.com/static/5086f19ce4b0ad16ff15598d/t/57a0d592725e25a1855d9143/1470158226345/Body_Camera.pdf [https://perma.cc/DQ7D-TUQT].

(i.e., locker rooms, dressing rooms or restrooms)."[107] Sometimes these policies employ the "reasonable expectations" language as a "catch all" provision in combination with other, more specific rules that dictate when the body camera should not be used.[108] Other times, the "reasonable expectations" language is used to determine when officers should exercise discretion when recording; when surveillance subjects should be notified that they are being recorded; and, in some cities, when surveillance subjects will be given the option to request the camera be turned off.[109]

A number of body-camera policies even permit the officer to record in certain circumstances where there is a reasonable expectation of privacy. Atlanta has rules that state law enforcement officers may use body-worn cameras to "record the activities that

107. PHILA. POLICE DEP'T, DIRECTIVE 4.21: BODY-WORN CAMERAS § 4-C (2017), http://www.phillypolice.com/assets/directives/D4.21-BodyWornCameras.pdf [https://perma.cc/7UX7-XWVG].

108. *See, e.g.*, CLEVELAND DIV. OF POLICE, GEN. POLICE ORDER NO. 3.2.20: WEARABLE CAMERA SYSTEM (WCS) § V (2015), https://www.bja.gov/bwc/pdfs/oh_clevelandpd_wcs_policy.pdf [https://perma.cc/2NCU-U9YK]. Cleveland's policy states that, unless otherwise required, the camera shall not be used to capture the following:

> D. Protected health information and treatment when requested by the patient, or on-scene Emergency Medical Service or Division of Fire personnel.
> E. Gratuitous captured media (i.e. effects of extreme violence or injury, exposed genitalia or other erogenous areas, etc.).
> F. Any place where there is a reasonable expectation of privacy (i.e. dressing rooms, restrooms, etc.).
> G. Images of confidential informants or undercover members, unless requested by the undercover member, their supervisor, or commanding member.
> H. Conversations of citizens and/or members (i.e. administrative duties, court, community meetings, etc.).

Id. at § V(D)–(H).

109. *See, e.g.*, CITY OF FERGUSON, OFFICE OF THE CHIEF OF POLICE, GEN. ORDER NO. 481.00, § 481.3(3) (2016), https://www.bwcscorecard.org/static/policies/2016-02-26%20Ferguson%20-%20BWC%20Policy.pdf [https://perma.cc/AD43-LS4C] ("In exercising this discretion, officers should be aware of and sensitive to civilians' reasonable privacy expectations."); FAIRFAX CTY. POLICE DEP'T, DRAFT MODEL POLICY FOR BODY WORN CAMERA § IX (2017), https://www.bwcscorecard.org/static/2016/policies/2015-05-17%20Fairfax%20County%20-%20BWC%20Policy.pdf [https://perma.cc/P6B5-BAWQ] ("When officers are recording persons in locations where the person should have a reasonable expectation of privacy (i.e. home, business office not open to the public, restroom, locker room, etc.), the officer should whenever practical . . . inform the person(s) that they are being recorded."); MIAMI-DADE POLICE DEP'T, DIRECTIVE NO. 16-18, REVISION TO THE DEPARTMENTAL MANUAL, NEW POLICY: CHAPTER 33 - PART 1 - BODY-WORN CAMERA SYSTEM § VII(H) (2016), https://www.miamidade.gov/police/library/bwc-policy.pdf [https://perma.cc/D423-E7NZ] ("In locations where victims have a reasonable expectation of privacy, such as a residence, hospital, or place of worship, an officer may honor a victim's request to turn off the BWC unless the recording is being made pursuant to an arrest or search of the residence or the individuals.").

occur in places where there is a reasonable expectation of privacy *if they occur in the presence of the law enforcement officer*."[110] However, Atlanta's body-camera policy protects the privacy of recorded individuals by exempting recordings "used by law enforcement in places where there is a reasonable expectation of privacy from disclosure" under the Georgia Open Records Act.[111] Aurora, Colorado, provides that "[t]he body-worn camera will not be activated in public places where a reasonable expectation of privacy exists, such as locker rooms, changing rooms, or restrooms unless the activation is for the purpose of official law enforcement activity."[112] Dallas follows the trend of privacy law in refusing to recognize any privacy in "public," as its policy states: "Officers are not required to obtain consent from a private person when in a public place or in a location where there is no reasonable expectation of privacy."[113]

110. ATLANTA POLICE DEP'T, POLICY MANUAL: STANDARD OPERATING PROCEDURE NO. 3133, BODY WORN CAMERAS (BWC) § 4.3.1 (2017), http://www.atlantapd.org/Home/ShowDocument?id=954 [https://perma.cc/6KYJ-QS6G]. However, the policy does prohibit recording in dressing rooms, locker rooms and restrooms, as well as "exposed genitals or other sexually sensitive areas." *Id.* at § 4.4.1.

111. *Id.* at § 4.9.1.

112. AURORA POLICE DEP'T, DIRECTIVES MANUAL § 16.4.4 (rev. 2017), https://www.auroragov.org/common/pages/DisplayFile.aspx?itemId=10473413 [https://perma.cc/BK6S-9J9L]. Chicago's policy states that "[t]he BWC will not be used to record . . . in locations where a reasonable expectation of privacy exists, such as dressing rooms or restrooms, *unless required for capturing evidence*." CHI. POLICE DEP'T, SPECIAL ORDER S03-14 § V.H (2016) (emphasis added), http://directives.chicagopolice.org/directives/data/a7a57b38-151f3872-56415-1f38-89ce6c22d026d090.pdf?ownapi=1 [https://perma.cc/2TCF-SWAE]; *see also* CINCINNATI POLICE DEP'T, PROCEDURE MANUAL, PROCEDURE NO. 12.540 BODY WORN CAMERA SYSTEM § A.5.c (2017), https://www.cincinnati-oh.gov/police/assets/File/Procedures/12540.pdf [https://perma.cc/Y8ZZ-NPSY] ("Officers will not use the BWC to record the following . . . [i]n any place where there is a reasonable expectation of privacy (e.g., restroom, locker room) except during an active incident (e.g., foot pursuit that leads into a locker room)"); DENVER POLICE DEP'T, OPERATIONS MANUAL § 119.04(3)(b)(4) (2018), https://www.denvergov.org/content/dam/denvergov/Portals/720/documents/OperationsManual/OMSBook/OM_Book.pdf [https://perma.cc/XV77-2HGG] ("The BWC will not be activated in places where a reasonable expectation of privacy exists (such as detox, medical, and/or healthcare facilities, locker rooms or restrooms, etc.) unless the activation is for the purpose of official law enforcement activity."); MEMPHIS POLICE DEP'T, POLICY AND PROCEDURE INFORMATION AND UPDATES § V.C. (2016), http://www.memphispolice.org/pdf/BWC.pdf [https://perma.cc/ZQZ6-QYTC] ("The [BWC] will not be activated in places where a reasonable expectation of privacy exists, such as locker rooms or restrooms, unless the activation is for the purpose of official law enforcement activity such as a call for service. When possible, every precaution shall be taken to respect the dignity of the victim by avoiding recording videos of persons who are nude or when sensitive areas are exposed. If this is unavoidable, the video can later be redacted.").

113. DALLAS POLICE DEP'T, GENERAL ORDER 332.00 BODY WORN CAMERAS § 332.04(A)(4) (2015), https://www.bwcscorecard.org/static/policies/2015-08-31%20Dallas%20BWC%20Policy.pdf [https://perma.cc/GQC9-8UYW]. This policy also provides:

The states that have proposed or enacted legislation around body cameras use the concept of a reasonable expectation of privacy in a similar way. The statute in Illinois requires notice of surveillance be given in contexts where people have a reasonable expectation of privacy.[114] In determining whether to release video footage, Missouri requires courts consider "[w]hether . . . video . . . contains information . . . reasonably likely to disclose private matters in which the public has no legitimate concern; bring shame or humiliation to a person . . . ; was taken in place where a person . . . has a reasonable expectation of privacy."[115] Louisiana's law prohibits the release of body-camera data that violates a reasonable expectation of privacy.[116]

In this Part, I will join the chorus of scholars that argue that the reasonable expectation of privacy test is broken and unsalvageable. I argue in favor of rules that favor more specific privacy-related values such as trust, obscurity, and autonomy, with an emphasis on process, relationships, and risk.

A. The Test is Broken and Unsalvageable

The problem with the reasonable expectations of privacy test is that it is too vague and too descriptive. Scholars have long protested the reasonable expectations text.[117] Daniel Solove wrote, "The

> While in public areas, officers are not required to advise a subject that they are recording their interaction unless the subject specifically asks if they are being recorded, at which point the officer will inform the subject that they are being recorded. When in a private residence in an official capacity, officers are not required to advise the resident they are recording. The officer is not prohibited from but encouraged to advise the citizen of the recording if doing so if it would better serve the handling of the incident.

Id. at § 332.04(A)(5)–(6).

114. 50 ILL. COMP. STAT. 706/10-20(a)(5) (West, Westlaw through 2018 Reg. Sess.).

115. MO. REV. STAT. § 610.100(5)(3)(b)–(d) (West, Westlaw through 2017 First Reg. Sess. and First and Second Extraordinary Sessions of the 99th Gen. Assembly).

116. LA. STAT. ANN. § 44:3(A)(8) (West, Westlaw through 2017 Second Extraordinary Sess.)).

117. Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002); Solove, *supra* note 18, at 1511–12 (citing Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1321 (1981)); Richard G. Wilkins, *Defining the "Reasonable Expectation of Privacy": An Emerging Tripartite Analysis*, 40 VAND. L. REV. 1077, 1080 (1987). *But see* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 506–07 (2007) ("Scholars and students of Fourth Amendment law find the current approach frustrating because the courts routinely mix and match the four models . . . . But appearances can be deceiving. What at first looks like conceptual confusion turns out to be a much-needed range of approaches.").

reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency and incoherence. Debates rage over whether particular government information gathering activities invade 'privacy.'"[118] He was not always a critic. Solove wrote, "For a long time, I believed that with the appropriate understanding of privacy—one that is well-adapted to modern technology, nimble and nuanced, forward-looking and sophisticated—Fourth Amendment jurisprudence could be rehabilitated. I now realize I was wrong."[119] According to Solove, the focus on reasonable expectations of privacy is misguided with respect to the Fourth Amendment. A focus on privacy invasions often is only tenuously related to problems caused by government surveillance and investigation. Solove argues that a focus on privacy "also bears little relation to whether it is best to have judicial oversight of law enforcement activity, what that oversight should consist of, how much limitation we want to impose on various government information gathering activities, and how we should guard against abuses of power."[120] Other critics have labeled the law surrounding the Fourth Amendment as "confusing, illogical, chaotic, and inconsistent."[121]

The reasonable expectations test is also too often just a proxy for identifying people or society's subjective expectations instead of rules for mitigating surveillance and data practices as exercises of power.[122] Pre-existing perceptions of exposure can be used to justify invasive surveillance practices. Scholars have noted that there is not enough of

118. Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L. J. 549, 554–55 (1990) ("[W]e should return to the privacy test intended by [Justices] Stewart and Harlan and to the underlying values that motivated it."); Brian J. Serr, *Great Expectations of Privacy: A New Model of Fourth Amendment Protection*, 73 MINN. L. REV. 583, 642 (1989) ("[T]he Court's current [F]ourth [A]mendment analysis is based on simplistic and logically incorrect theories of public exposure."); Solove, *supra* note 18, at 1511–12.

119. Solove, *supra* note 18, at 1512.

120. *Id.* at 1513.

121. *See* Tokson, *supra* note 105, at 144 (citing Ronald J. Allen & Ross M. Rosenberg, *The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge*, 72 ST. JOHN'S L. REV. 1149, 1149–50 (1998); Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1321 (1981); and Donald R.C. Pongrace, *Stereotypification of the Fourth Amendment's Public/Private Distinction: An Opportunity for Clarity*, 34 AM. U. L. REV. 1191, 1208 (1985)).

122. *See* Solove, *supra* note 18, at 1521 ("From the way it is formulated, the test purports to be an empirical metric of societal views on privacy."); *cf.* Tokson, *supra* note 105, at 144 (noting that the Fourth Amendment test is "well-defined"). *But see* Matthew B. Kugler & Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U. CHI. L. REV. 1747 (2017) (arguing that the Fourth Amendment test is not circular).

a moral floor for the privacy test.[123] Solove wrote that it is not people's expectations that should matter, but rather what they desire regardless of their expectations. He wrote, "We look to the law not just to preserve the status quo, but to change it and to shape society into what we want it to be."[124] Mathew Tokson proposed looking exclusively to positive law or having courts engaging in direct normative balancing as an alternative to relying upon expectations that might not contain an ethical infrastructure.[125] The lack of moral floor allows unchallenged privacy encroachments to serve as the justification that people can no longer expect privacy. Even worse, it ignores the need for rules even when surveillance and data practices might not threaten certain conceptualizations of privacy, such as secrecy.[126]

I agree with the critics, perhaps for slightly different reasons than some. While many find fault in the application of the test, my critique lies with the fatal inclusion of the concept of privacy within the text itself. What is "privacy," anyway? It has no set meaning, which creates real problems. Since no one knows what privacy really means, any rules that are built around the malleable general concept of privacy, instead of more specific concepts like confidentiality, secrecy, or obscurity, are destined to be ill-fitting and exploited. When courts and lawmakers allow privacy to be subject to definition at every turn,

123. *See* Solove, *supra* note 18, at 1524 (citing Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974)) (noting that Supreme Court pronouncements themselves affect society's future expectations of privacy and that "the government could condition the populace into expecting less privacy. For example, as Professor Anthony Amsterdam has observed, the government could diminish expectations of privacy by announcing on television each night that we could all be subject to electronic surveillance.").

124. *Id.*

125. Tokson explains that under a positive law regime, the "absence of a law or common law tort prohibiting some government information-gathering activity would definitively establish that the activity was not a search under the Fourth Amendment. The reverse would also apply—when a government investigative action violated positive law, it would constitute a per se Fourth Amendment search." Tokson, *supra* note 105, at 190 (footnote omitted). Alternatively, "[a] direct normative balancing test would find a Fourth Amendment search when the harms to citizens of allowing police to engage in a certain type of surveillance without a warrant outweigh the benefits to society via improved law enforcement." *Id.* at 196.

126. Solove, *supra* note 18, at 1525 ("But even measuring desires fails to address an overarching problem: we might want to regulate government information gathering even when it does not violate privacy. The problem with a doctrinal test based on privacy is that it ensnares courts and commentators into a debate over the meaning of privacy and takes the focus away from the full range of problems the Fourth Amendment needs to address. Practical consequences are ignored in an analytic approach that is nearly blind to the results.").

those seeking to surveil and collect data will consistently argue for the most narrow interpretation possible. Without a more specific value or goal to guide how privacy should be conceptualized, they will win. It is time to get rid of the reasonable expectations test throughout privacy law, and police body cameras are an ideal place to chart more protective, accurate, and sustainable benchmarks.

B. Embrace More Specific Notions of Privacy

Every time law and policy makers invoke the concept of privacy to define people's expectations or obligations, they should clarify what they mean by that word. Privacy can be conceptualized many different ways.[127] How it is conceptualized will dictate which values it ultimately serves or ignores. For example, if privacy is conceptualized only as secrecy, information shared with groups of people will be excluded, and the values of trust and obscurity will not be served.

Prioritizing values can help determine how the reasonable expectation of privacy test is administered with respect to body cameras. For example, if privacy rules are meant to facilitate the value of intimacy, then prohibitions on filming nude people or in people's bedrooms make sense and might be sufficient. If privacy rules are meant to facilitate solitude, then privacy rules might be interpreted in similar ways to prevent filming when people thought they were isolated. But intimacy and solitude are not the only ways to conceptualize privacy. Data-protection regimes and identity rights seek to protect privacy by providing people control over their personal information and preserving their dignity. Rules of evidence and fiduciary responsibility seem to advance privacy interests by preserving confidentiality. When the concept of "privacy" is used in law without any meaningful clarification, courts and lawmakers have no clear guidance on which conceptualization to use and which privacy values to prioritize.

Too often, the reasonable expectation of privacy test merely acts as a proxy for "expectation of secrecy." There are, of course, good reasons not to film in places where we expect near total secrecy, seclusion, and discretion, such as bathrooms and dressing rooms. But the problem is when the entirety of privacy is framed in this way.[128] Consider Milwaukee's body-camera policy, which states "[body worn-

127. *See generally* Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002) (evaluating different conceptions of privacy).

128. *See* DANIEL SOLOVE, UNDERSTANDING PRIVACY 6 (2008); Daniel Solove, "*I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 746 (2007); Solove, *supra* note 127, at 1089.

cameras] will not be activated in a place where a reasonable expectation of privacy exists, such as dressing rooms, locker rooms and restrooms."[129] This policy frames privacy as secrecy—something not known or seen or not meant to be known or seen by others.[130] But what about every other aspect of our lives? Can we only expect privacy when we are naked?

The better approach to the reasonable expectations of privacy test is to build rules that serve more specific values than the near-generic conceptualization of privacy. Specifically, I recommend relying upon the concepts of trust and obscurity to mitigate two of the biggest weaknesses of the "reasonable expectations" test: the misguided third-party doctrine and the fallacy that there is "no privacy in public."

1. Trust Protects Relationships

People place their trust in others every day. We should formulate rules requiring recipients of information to be discreet, protective, honest, and—most importantly—loyal. This is particularly true as an ethos for third-party vendors of body cameras and the data they create.

Professor Neil Richards and I have argued that modern privacy law is incomplete because, from its inception, it has failed to account for the importance of trust.[131] We adopted the definition of trust as the willingness to make one vulnerable to the actions of others, which emphasizes the role of power within relationships.[132]

Trust is an essential component of healthy relationships and healthy societies. Although different disciplines define trust in various

129. MILWAUKEE POLICE DEP'T., GEN. ORD. NO. 2015-42: STD. OP. PROC. 747—BODY WORN CAMERAS (BWCS) § 747.25.E.1 (2015), https://www.rcfp.org/bodycam_policies/WI/MilwaukeeWI_BWC_policy_update.pdf [https://perma.cc/9QVF-64F8].

130. *Secret*, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY (3d. 1993).

131. For a discussion of the importance of trust and its relation to privacy, see generally ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (forthcoming 2018); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180 (2017) [hereinafter Richards & Hartzog, *Privacy's Trust Gap*]; Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016) [hereinafter Richards & Hartzog, *Taking Trust Seriously*]; Neil Richards & Woodrow Hartzog, *Trusting Big Data Research*, 66 DEPAUL L. REV. 579 (2017) [hereinafter Richards & Hartzog, *Trusting Big Data Research*].

132. *See, e.g.*, Richards & Hartzog, *Privacy's Trust Gap*, *supra* note 131, at 1213; Richards & Hartzog, *Taking Trust Seriously*, *supra* note 131, at 433.

ways,[133] it is useful to think of trust as a "state of mind that enables its possessor to be willing to make herself vulnerable to another—that is, to rely on another despite a positive risk that the other will act in a way that can harm the truster."[134] Trust allows cooperation with other people despite the fact that exposing ourselves enables them to harm us. In the context of information relationships, trust means the willingness to become vulnerable to a person or organization by disclosing personal information.

Every disclosure of personal information in the modern age leaves the discloser vulnerable in some way, if only incrementally. As a result, every information relationship involves some degree of trust, or willingness to become vulnerable.[135] This is true even if that trust is not a conscious one. Trust is a key component in the relationship between citizens and police, particularly with respect to the data that is created from body cameras. In cities and states where consent is used to justify body-camera use, that consent is likely going to be based on trust that the officer is going to protect what is recorded and keep it from getting into the wrong hands or used in a way that violates the people's privacy.

So, how can privacy rules for body cameras further trust? One way is to break the concept down into its component parts. Richards and I articulate the various tenets of trust as discretion, honesty, protection, and loyalty.[136] We have argued that those who we entrust with our information and well-being have "a duty to avoid unreasonable and dangerous self-dealing."[137]

These four concepts—discretion, honesty, protection, and loyalty—can guide rules that support trust. They are not new. They are foundations of one of the most established legal concepts involving trust in relationships—the law of fiduciaries.[138] The "central goal of fiduciary law is to protect against the exploitation of a vulnerability created by trust in another."[139] Jack Balkin has argued

133. *See, e.g.*, Batya Friedman & Peter H. Kahn, Jr., *Human Values, Ethics, and Design*, *in* THE HUMAN-COMPUTER INTERACTION HANDBOOK: FUNDAMENTALS, EVOLVING TECHNOLOGIES AND EMERGING APPLICATIONS 1177, 1190 (Julie A. Jacko & Andrew Sears eds., 2003) ("[T]rust is said to exist between people who can experience good will, extend good will toward others, feel vulnerable, and experience betrayal." (citation omitted)).

134. Claire A. Hill & Erin Ann O'Hara, *A Cognitive Theory of Trust*, 84 WASH. U. L. REV. 1717, 1724 (2006)

135. *See* Richards & Hartzog, *Taking Trust Seriously*, supra note 131, at 431.

136. *See, e.g.*, *id.* at 457.

137. *Id.*; *see also* Richards & Hartzog, *Privacy's Trust Gap*, *supra* note 131, at 1214.

138. *See* Richards & Hartzog, *Taking Trust Seriously*, *supra* note 131, at 457.

139. *Id.* (citations omitted).

that the notion of fiduciaries is a great fit for modern information privacy problems, which arise within relationships that involve power and information asymmetries and are characterized by the collection or exchange of personal information.[140]

Certain body-camera policies already recognize the importance of trust by seeking to protect confidential informants. For example, Philadelphia's body-camera policy states that "Body-Worn Cameras shall not be used or activated to . . . [r]ecord conversations with confidential informants and undercover officers."[141] Austin's policy does not require the activation of body cameras when "[a] potential witness who requests to speak to an officer [asks for] confidential[ity] or desires anonymity" or when "[a] victim or witness . . . requests that he or she not be recorded as a condition of cooperation and the interests of justice require such cooperation."[142] These kinds of provisions require or permit confidentiality and discretion in order to build trust.

However, if the laws and policies regulating body camera use are to be sustainable, trust must be ensured throughout the lifecycle of data, not just at the point of surveillance and capture. This means that state actors and verified, accountable third-party vendors that obtain body-camera data must be discreet in who the data is disclosed to (either as a public record or bulk data exchange), must protect the data from leaks to unauthorized third parties by engaging in reasonable data security and denitrification, and must be honest with those being surveilled and the public at large about when surveillance is occurring and their data is being processed.

Some policies seem to actively state that people cannot trust police officers with their personal information. For example, Cincinnati's policy dispels any notion that officers might be discrete with surveillance subjects by stating that "[u]nlike the back of a police car or empty police interrogation room, which requires notification recording equipment is in use, the personal contact between an individual and an officer does not constitute an environment where there is a reasonable expectation of privacy."[143]

140. *See generally* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016) (discussing the concept of information fiduciaries).

141. PHILA. POLICE DEP'T, *supra* note 107, at 4.

142. AUSTIN POLICE DEP'T, POLICY MANUAL: BODY WORN CAMERA SYSTEMS § 303.2.5(d) (1–2) (2017), http://www.austintexas.gov/sites/default/files/files/Police/policy_9-28-17.pdf [http://perma.cc/C4HC-7PLY].

143. CINCINNATI POLICE DEP'T, *supra* note 112, at 2.

Perhaps one of the largest benefits that would come from a focus on trust instead of a general expectation of privacy is that it would ameliorate the harshness that often results from the application of the third-party doctrine, which treats disclosures to anyone, no matter how trusted, as a waiver of privacy rights.[144] There may be many instances in which disclosures to third parties carry no implication of or need for trust in a police officer, government, or third party. But, the doctrine applies harshly in instances where people make themselves vulnerable to officers when they need help, for example, when they need to report that they are in an abusive relationship. Without the protections of privacy and confidentiality and with a camera pointed right on them, victims of abuse might be hesitant to report abuse, seek help, or fully confide in others.[145]

2. Obscurity Reveals the Fallacy of "No Privacy in Public"

Obscurity is the notion that, when information is hard or unlikely to be found, it is relatively safe.[146] People rely upon this obscurity all the time. In work with Evan Selinger and Fred Stutzman, I have explored the concept of obscurity as an essential component of modern notions of privacy.[147] Every day we make decisions about where we go, what we do, and what we share based upon how obscure we think we are. Most of our information online is obscure as well. We use passwords, privacy settings, and disappearing messages to make information hard to be found by the wrong audience. Think of obscurity as the counterpart to trust. When we can reliably trust

144. *See, e.g.*, Balkin, *supra* note 140, at 1230 (arguing against the third-party doctrine's assumption that when people disclose information to a third party, the disclosers have "no reasonable expectation of privacy in the information" and proposing, instead, that many third parties "owe us fiduciary duties or duties of confidentiality"); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORD. L. REV. 611, 611, 616 (2015) (arguing that the third-party doctrine should be limited where a person shares information with an "information fiduciary"). *But see* Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009) (defending the third-party doctrine).

145. *See* Fan, *supra* note 85, at 438–39.

146. *See* Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way To Think About Your Data Than 'Privacy*,*'* ATLANTIC (Jan. 17, 2013), http://http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283 [https://perma.cc/FA9K-B2TQ].

147. *See* Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 388 (2013); Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 9, 11 (2013) [hereinafter Hartzog & Stutzman, *Online Obscurity*]; Evan Selinger & Woodrow Hartzog, *Obscurity and Privacy*, *in* ROUTLEDGE COMPANION TO PHILOSOPHY OF TECHNOLOGY 2 (Joseph Pitt & Ashley Shew eds., forthcoming 2018).

people, we have less of a need to be obscure. However, in contexts where there is no one to trust, obscurity becomes invaluable.

Unlike trust, obscurity is not a widely established concept in law or policy. Obscure is defined as "[n]ot readily noticed or seen; inconspicuous; . . . Not clearly understood or expressed; ambiguous or vague."[148] It is a simple concept that involves at least two parties: the individual and the observer. "An individual is obscure to an observer if the observer does not possess or comprehend critical information needed to make sense of the individual."[149] For example, does an observer know your personal identity, social connections, or the context in which you disclosed something about yourself? Without this information, an observer has a limited ability to make sense of what you do and what you say. You are just a face in the crowd. Finding this information is often costly.[150] In the language of privacy as obscurity, transaction costs are a good thing.

When we are obscure, we are protected by an observer's inability to comprehend our actions. We seek to be obscure in our everyday lives. We close doors, talk in hushed tones, and take risks of very briefly exposing ourselves, comfortable that the odds of adverse results are low. Without a sense of obscurity, we would be forced to assume that everything we do outside of our homes and physician's offices is going to be observed, stored, or used. People simply do not have the resources or ability to protect against that kind of threat model.

Obscurity provides an alternative for those who revolt at the idea that there is "no privacy in public." Many body-camera laws and policies are built around the notion that surveillance is "public," poses no privacy threats and is therefore justified.[151] For example, the Dallas Police Department policy provides that "[w]hile in public areas, officers are not required to advise a subject that they are recording their interaction unless the subject specifically asks if they are being recorded, at which point the officer will inform the subject that they are being recorded."[152] The Dallas Police Department's body-camera policy also states that "[o]fficers are not required to

148. *Obscure*, THE AM. HERITAGE DICTIONARY OF THE ENG. LANGUAGE (5th ed. 2018), http://www.ahdictionary.com/word/search.html?q=obscure [https://perma.cc/27W5-5Q8P].

149. Hartzog & Stutzman, *Online Obscurity*, *supra* note 147, at 5.

150. *Id.* at 4.

151. *See* MINN. STAT. ANN. § 13.825 (West, Westlaw through 2017 Reg. and First Special Sess.) ("[D]ata are public if a subject of the data requests it be made accessible to the public.").

152. DALL. POLICE DEP'T GEN. ORDER, *supra* note 113, at § 332.04(A)(5).

obtain consent from a private person when in a public place or in a location where there is no reasonable expectation of privacy. It is at the discretion of the officer to determine if they want to announce a recording is occurring."[153] The Oklahoma City Police Department policy states "[e]ach officer shall activate his or her body-worn camera in the following circumstances: 1. Voluntary contact (only in a public place or a place where the public and the officer have a right to be)."[154]

The question of what is public, however, is often just a plot on the spectrum of things that range from completely obscure to totally obvious or known. People's risk calculus is often built around how obscure they are, not whether what they do is theoretically accessible by someone.[155] Rather, they care whether what they are doing at any one particular time and context is likely to be seen, preserved, disseminated, or used against them later.[156] The calculus for what makes things obscure is complex and includes many different factors, such as search visibility, permanence, comprehensibility, identifiability, and the resources, motivation, and pre-existing knowledge of those who seek to surveil or make use of data. These factors should be better valued when formulating accounts of what public information is or what constitutes being "in public."

Additionally, the idea that there is no privacy in public is problematic because the notion of "public" is itself an undertheorized and amorphous construct. Torts, statutes, and constitutional amendments dictate that there can be "no privacy in public information."[157] Yet courts, lawmakers, and society have no consistent

153. *Id.* at § 332.04(A)(4)–(5).

154. OKLA. CITY POLICE DEP'T: OPERATIONS MANUAL § 188.30 (2016), https://www.okc.gov/home/showdocument?id=9198 [https://perma.cc/UJ6A-43GT]; *see also* SAN JOSE POLICE BODY CAMERA POL'Y § 7, http://www.sjpd.org/InsideSJPD/BodyCameras/SJPD_BWC_Policy_06-29-15_with_POA_approval.pdf [https://perma.cc/PSQ6-N2BP] ("Generally, officers are not required to advise or obtain consent to utilize the body-worn camera from a private person when: A. In a public place; or B. In a location where there is an expectation of privacy (e.g., inside a building or dwelling) but the officer is lawfully present."). *But see* AURORA POLICE DEP'T DIRECTIVES MANUAL, *supra* note 112, at § 16.4.4 ("The body-worn camera will not be activated in public places where a reasonable expectation of privacy exists, such as locker rooms, changing rooms, or restrooms unless the activation is for the purpose of official law enforcement activity.").

155. *See, e.g.*, Frederic Stutzman & Woodrow Hartzog, *Boundary Regulation in Social Media* 769–77 (publication in the Proceedings for the ACM 2012 conference on Comp. Supported Coop. Work) (2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1566904 [https://perma.cc/UZ2V-ZB26].

156. *Id.* at 773–76.

157. *See* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013); Illinois v. Caballes, 543 U.S. 405, 409–10 (2005); California v. Ciraolo, 476 U.S. 207, 211–12 (1986); United States v.

conceptualization for "public" or "public information." In everyday conversation and even within regulatory schemes, what constitutes public information is essentially based on a hunch.[158]

Body-camera law could correct this problem by refusing to let broad, descriptive notions of "public" dictate legal protection. Up to this point, courts have looked to see if society classifies something as "public" and shapes the law accordingly. We should flip that approach. Designating information as public is not and should not be a clinical, empirical judgment, but a normative one meant to shape outcomes and serve values. Lawmakers and departments should formulate rules aimed at preserving the obscurity of people and their data to guide rules for protection. In other work, I have criticized the concept of "obscurity lurches," that is, actions like the use of facial recognition technology or making information searchable and easily accessible in ways that violate people's relied upon zones of obscurity.[159]

The main problem with the reasonable expectations of privacy test is not the "reasonableness" approach, which is a foundational concept in various areas of the law.[160] The problem lies in the concept of privacy itself. Even a focus on "reasonable expectations of obscurity" might be more useful. A reasonableness approach to obscurity would be more focused than the "reasonable expectation of privacy" standard because it would direct authorities to identify and evaluate contextual factors like perceived structural protections, threat modeling, and other things that would seem to make the cost of finding or understanding information high and, as a result, unlikely to occur. In other words, at least the concept of a reasonable expectation of obscurity would more directly identify specific factors like signals

Jacobsen, 466 U.S. 109, 120–21 (1984); United States v. Place, 462 U.S. 696, 706–07 (1983); Smith v. Maryland, 442 U.S. 735, 744–46 (1979); United States v. Miller, 425 U.S. 435, 442 (1976); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001); United States v. Maxwell, 45 M.J. 406, 419 (C.A.A.F. 1996); Gill v. Hearst Pub. Co., 253 P.2d 441, 444 (Cal. 1953); Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 862–63 (Cal Ct. App. 2009); Melvin v. Reid, 297 P. 91, 93 (Cal. Dist. Ct. App. 1931).

158. For more regarding this critique, see generally Solove, *supra* note 14 (arguing that "the regulation of public records in the United States must be rethought in light of the new technologies in the Information Age") and Woodrow Hartzog, *The Public Information Fallacy*, 98 B.U. L. Rev (forthcoming 2018) (Northeastern Univ. Sch. of Law, Working Paper No. 309-2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3084102 [https://perma.cc/4YMD-N34K] (theorizing that the "no privacy in public" justification is "misguided" due to the lack of a clear definition of the word "public").

159. Hartzog, *supra* note 51, at 966–70.

160. *See generally* Benjamin Zipursky, *Reasonableness In and Out of Negligence Law*, 163 U. PA. L. REV. 2131 (2015) (analyzing the imbrication of "reasonableness" and negligence law).

and transaction costs that can more accurately and consistently define a legal threshold.

3. Autonomy Justifies Requiring Authorization

Finally, body-camera rules should serve the autonomy of those surveilled. In order to flourish, people need some degree of freedom from external control or influence. To many, autonomy is the reason privacy is important. This notion is at the heart of the "right to be let alone" articulation of privacy developed so many years ago by Warren and Brandeis.[161] Alan Westin, one of privacy's most famous theorists, wrote that the most significant threat to one's autonomy is the notion that someone might violate one's "inner zone" to learn their deepest secrets.[162] Westin wrote, "This deliberate penetration of the individual's protective shell, his psychological armor, would leave him naked to ridicule and shame and would put him under the control of those who knew his secrets."[163]

Autonomy is at the core of a number of developed theories of privacy. Julie Cohen argued, "[a] protected zone of informational autonomy is valuable, in short, precisely because it reminds us what we cannot measure."[164] Helen Nissenbaum observed that the relationship between privacy and autonomy can be thought of in three different ways: (1) control over the information itself, (2) contributing to an environment where individual autonomy will flourish, and (3) as creating space for individuals to follow through on autonomous decisions.[165]

161. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193–95 (1890).

162. ALAN WESTIN, PRIVACY AND FREEDOM 33 (1967).

163. *Id.*

164. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1423–26 (2000); *see also* Hyman Gross, *Privacy and Autonomy*, *in* NOMOS XIII: PRIVACY 169, 173–74, 181 (J. Roland Pennock & John W. Chapman eds., 1971) (arguing that informational privacy is desirable because it permits individual self-determination over how one appears and to whom, and concluding that "an offense to privacy is an offense to autonomy"); Joel Feinberg, *Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution?*, 58 NOTRE DAME L. REV. 445, 454 (1983) (stating that autonomy includes the right to decide "what personal information to disclose," or conceal, from others); Charles Fried, *Privacy*, 77 YALE L.J. 483, 475–93 (1968) ("Privacy, thus, is control over knowledge about oneself."); Adam D. Moore, *Toward Informational Privacy Rights*, 44 SAN DIEGO L. REV. 809, 812–13 (2007) (favoring a "control-based definition of privacy" that affords individuals the space to develop, "while maintaining autonomy over the course and direction of one's life").

165. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 81–83 (2009).

One key way to serve people's autonomy is to give them control over when they are surveilled and how their data is processed. Control is often given through rules requiring "consent" from surveillance and data subjects. An individual's capacity for self-determination and freedom from external influence is then respected when surveillance and data processing can occur only if the subject agrees to it. Prohibiting surveillance without the consent of the surveilled respects the agency of those being watched and helps mitigate the power disparities inherent in surveillance.

I have been critical of data protection regimes that make use of the concept of "consent" and "control" in the past.[166] Too often, the limitations of "consent" and "control" regimes are easily exploited by those who seek to surveil and process data. People have limited resources to process risk and make decisions regarding when they will be watched and what is to be done with their personal information. If too many requests are made of people, they risk making poor or ill-informed decisions, and their autonomy is actually reduced, not enhanced. When consent regimes are exploited, their main function is to burden the data or surveillance subject with the costs and risk of harm.[167]

However, the infrequency and potential danger of body camera surveillance might counsel a prioritization of autonomy in certain contexts. Requiring consent at the moment of surveillance can clarify exactly what is happening and help individuals determine for themselves whether an encounter is to be recorded and stored. Additionally, giving surveillance subjects the deletion and other data subject rights might be just as beneficial. Governments could borrow the wisdom of data protection regimes around the world, which embrace the fair information practices.[168] These simple data collection and processing principles give data subjects meaningful rights such as rights of correction and deletion, among others. Given the likely

166. Hartzog, *supra* note 51, at 965–66; Woodrow Hartzog, *Privacy and the Dark Side of Control*, IAI NEWS (Sep. 4, 2017), https://iainews.iai.tv/articles/privacy-the-dark-side-of-control-auid-882 [https://perma.cc/U8KD-84JW] [hereinafter Hartzog, *Privacy and the Dark Side of Control*]; *see also* Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information*, 111 PA. ST. L. REV. 587, 610–13 (2007).

167. *See* Haynes, *supra* note 166, at 593–97; Idris Adjerid, Alessandro Acquisti & George Loewenstein, Framing and the Malleability of Privacy Choices 2–4 (June 2014) (unpublished paper prepared for the 2014 Workshop on the Economics of Information Security, Pennsylvania State University, 2014), http://www.econinfosec.org/archive/weis2014/papers/AdjeridAcquistiLoewenstein-WEIS2014.pdf [https://perma.cc/7FNF-V7G8]; Hartzog, *Privacy and the Dark Side of Control*, *supra* note 166.

168. Hartzog, *supra* note 51, at 952.

volatile and sensitive nature of body camera recordings and how vulnerable people are in police encounters, governments might even implement some more robust version of a deletion right, akin to the European Union's "right to be forgotten" or the "sealed" nature of certain juvenile records.[169]

Of course, consent could still be a problem for body camera systems. First, it might not be feasible for an officer to get the consent of everyone who will be captured on camera. This is likely why the policies of most cities that require consent or permit deactivation upon request limit the power of consent sometimes to particular individuals like victims or witnesses who wish to make a statement and residents of homes.[170] Notification requirements might be easier to implement as a default rule for everyone better than consent requirements, even though these notification regimes widely vary in their efficacy.[171]

The second problem is that people might feel pressured to give consent for surveillance. The "I've got nothing to hide" argument remains pervasive in both law and society, and the mere act of requesting deactivation might cause officers and others to react differently to or become suspicious of those who do not want to be watched.[172] Additionally, what should the policy be in circumstances

169. Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, 2014 E.C.R. 317; *Expungement*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/expungement/#federal [https://perma.cc/65YH-D8BG] ("[Forty-five] states and the District of Columbia provide for expungement for some ex-offenders or other similar relief.").

170. *See, e.g.*, BALT. POLICE DEP'T BODY CAMERA POL'Y: EXCEPTIONS TO RECORDING § 2 (2017), https://www.baltimorepolice.org/sites/default/files/Policies/824_Body_Worn_Cameras.pdf [https://perma.cc/VY7K-4KTV] ("When victims, witnesses or other individuals wish to make a statement or share information during a voluntary interaction with police, but refuse to do so while being recorded, members may Deactivate the BWC in order to obtain the statement or information."); BOS. POLICE DEP'T BODY CAMERA POLICY § 2.3 (2016), https://www.bwcscorecard.org/static/policies/2016-07-12%20Boston%20-%20BWC%20Policy.pdf [https://perma.cc/Z8UP-YAP3] ("Before entering a private residence without a warrant or in non-exigent circumstances, the BWC officer shall seek the occupant's consent to continue to record in the residence. If the civilian declines to give consent, the BWC officer shall not record in the residence.").

171. *See* CARL E. SCHNEIDER & OMRI BEN-SHAHAR, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 173 (2014); BOS. POLICE DEP'T, *supra* note 170, § 2.5 ("Notice of Recording: Unless there is an immediate threat to the officer's life or safety, making BWC notification impossible or dangerous, BWC officers shall inform civilians that they are being recorded. BWC officers shall notify civilians with language such as 'Ma'am/Sir, I am advising you that our interaction is being recorded by my Body Worn Camera.' BWC officers shall not record civilians surreptitiously.").

172. *See* DANIEL SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 21–32 (2011).

where some people present at an officer interaction wish for the camera to be turned on while others do not? Whose wishes should be respected?[173] There is no clear answer to these questions. One possible strategy would be to give surveillance subjects more robust data access, redaction, and deletion rights in the case of conflicting requests regarding body-camera deactivation.

* * *

In sum, body-camera law and policy can largely avoid the problems caused by the "reasonable expectations of privacy" standard by creating rules built around trust, obscurity, and autonomy. There are, of course, other values that body cameras should also embrace that are relevant to surveillance and personal data. For instance, surveillance and data protection invoke many equality issues. People should be protected against targeted use of body cameras based upon their race, religious beliefs, sexual orientation, or other characteristics. For example, the Austin Police Department policy prohibits using body cameras "[t]o monitor persons based solely upon the person's political or religious beliefs or upon the exercise of the person's constitutional rights to freedom of speech and religious expression, petition, and assembly under the United States Constitution, or because of the content or viewpoint of the person's protected speech."[174] The only way body cameras will be safe and sustainable is if they can accommodate all of these values.

III. REFINING IMPLEMENTATION: DESIGNING A BETTER BODY CAMERA SYSTEM

In addition to embracing more nuanced notions of privacy, body cameras are an opportunity to create a holistic framework that addresses both data practices and the design of information technologies. In this Part, I make two arguments. First, body-camera frameworks should include rules for the design of technologies. Design is currently a bit of a blind spot for large areas of privacy law.[175] Lawmakers and courts outline rules for how information is to be collected, used, and shared. But they are often silent on how

173. For a deeper exploration of the tension amongst those who share a common story but have divergent exposure interests, see Sonja R. West, *The Story of Us: Resolving the Face-Off Between Autobiographical Speech and Information Privacy*, 67 WASH. & LEE L. REV. 589, 591–96 (2010). Perhaps one answer would be to require elevated authorization process to record or perhaps vesting all those who object with additional rights of deletion or redaction.

174. AUSTIN POLICE DEP'T, *supra* note 142, at 303.2.5(d)(8).

175. *See generally* HARTZOG, *supra* note 14 (analyzing how technological designs are slowly but steadily enabling privacy degradations).

surveillance and data technologies are actually built and function. These rules often do little to address the effect that powerful new technologies have on people. For example, surveillance rules often do not address the configuration and deployment of surveillance technologies. Data protection rules sometimes ignore the default settings for consumer-facing technologies or are silent on how far user interfaces can go in shaping user expectations of privacy.[176] In this Part, I argue that the law and policy of body cameras can provide a template and momentum for taking design more seriously in privacy law generally.

Second, I propose a model framework for policymakers to combine rules for data processing and surveillance as well as the design of technologies for a holistic approach to privacy. This approach is built around the lifecycle of data collection, storage, processing, and disclosure. I propose data and design rules that serve the values of trust, obscurity, and autonomy.

A. Design Will Determine the Value of Body Cameras

Design choices affect nearly every way in which body cameras will be used. Each of these decisions matter. Someone must decide if the cameras will collect video, audio, or both. Someone must decide if the camera is going to be built and configured to be on by default, or if it will be activated manually or automatically. Someone must decide if the cameras are to be designed so that the data captured by the camera is stored locally or remotely. Authorities must also decide whether the data will be decrypted and/or redacted; how it will be deleted and when, through what technology and format it will be released; and whether redaction technologies will be used to obscure the data.

Design is also power. Biometrics allow more people to be surveilled and identified at a fraction of the cost. Alert lights and sounds on body cameras can indicate to people when the camera is activated. Encryption technologies can protect data against hackers and snoops. And technologies designed to redact and blur can mitigate the harm from public disclosure of surveillance.

176. *Id*. A few notable exceptions include biometrics laws in Illinois, Texas, and Washington and the European Union's requirement within its General Data Protection Regulation to implement privacy by design and default. Rebecca Yergin, *Washington Becomes the Third State with a Biometric Law*, INSIDE PRIVACY (May 31, 2017), https://www.insideprivacy.com/united-states/state-legislatures/washington-becomes-the-third-state-with-a-biometric-law/ [https://perma.cc/BH2J-XK5J]; *see also* Council Regulation 2016/679, 2016 O.J. (L 119) 7.

Most importantly, design is political. People often say the design of technologies can be neutral. "It's the best available evidence that's neutral," Steve Tuttle, vice president of communications at camera company TASER, told *The Wire*.[177] "It's just an observer. The truth is the truth."[178] Except when it's not. The design of body cameras is never neutral. Every body-worn camera system design decision makes a certain reality (and perception of that reality) more or less likely. For example, cameras that do not include a blinking "on" light will result in less awareness of surveillance than those cameras that by design indicate when they are in operation.[179] As a result, design reflects the prioritization of values by those who control and implement systems. When buttons are easy to find and redundancies are built in, there will be fewer mistakes turning on and off the camera. Whether the camera is designed to be placed on the shoulder, on a gun, or even on a drone, affects what is captured and how the video will be perceived by the public.[180] boyd and Rosenblat wrote,

> Advocates imagine that [body cameras] will surveil the police, but unlike most footage that has rallied the public, body-cam footage does not make visible the facial expressions or movements of the police officer's body because it doesn't face the officer. Instead, it casts a spotlight on the other people among whom police operate. Worse, it focuses attention on the limited angles that can be seen from that vantage point. As any videographer knows, camera angles matter. You can tell radically different stories depending on the angle. For instance, due to the average heights of male officers and the women they encounter, a lapel camera can capture a steady stream of cleavage when an officer is facing her.[181]

Even persistent surveillance only captures some of the story. Red activation lights on body cameras and systems that allow for deactivation upon request show respect for people's autonomy.[182] Use of biometrics shows a lack of respect for people's obscurity because they can make things that were previously difficult to find, for example your location or identity in a public place, easy to track.[183]

177. Shirley Li, *The Big Picture: How Do Police Body Cameras Work?*, ATLANTIC (Aug. 25, 2014), https://www.theatlantic.com/national/archive/2014/08/how-do-police-body-camera-work/378940/ [https://perma.cc/3V6A-NG82].

178. *Id.*

179. Mateescu et al., *supra* note 6, at 13.

180. *Id.* at 5; boyd & Rosenblat, *supra* note 8.

181. boyd & Rosenblat, *supra* note 8.

182. Mateescu el al., *supra* note 6, at 13.

183. Stoughton, *supra* note 8, at 1398.

Design is important to get right because it is very difficult to change once it is implemented. Governments choose to fund certain kinds of systems with certain specifications. Contracts with vendors are formed. Officers and employees are trained upon the equipment that is decided upon. Policies and rules are built around the capabilities of the equipment. This entrenches the design of the technologies that are initially chosen and makes changing them difficult. As a result, the time to focus on the design of body cameras is now, before they become fully entrenched and the rules become set in stone.[184]

B. Guides for Designing a Body Camera Obscura

What should design rules for body cameras look like? As an initial matter, of course body-camera policies should address more than just privacy. Safe, sustainable body-camera laws and policies require a careful balancing of sometimes competing interests and ethics beyond the scope of this Article.[185] Different cities and states have different needs, resources, and values.

Instead, this Part suggests a series of guides, default presumptions, and possible boundaries, rights, or systems that could be used to create better rules for privacy that also can serve values of justice, due process, accountability, and free speech. I use the concept of obscurity to develop a guiding ethic for body cameras and privacy: To best protect privacy while still retaining the utility of body cameras, surveillance and the subsequent data collection, use, and dissemination should be "hard but possible" and proportional to allowances elsewhere in the system.[186]

The best way to follow this ethic and ensure privacy while also providing for accountability is to take an accounting of the body camera system as a whole, rather than assessing the merit of individual privacy protections and surveillance and data process allowances in isolation. To do that, we must follow the data. In her article on body cameras, Elizabeth Joh ask a series of questions that follow the data lifecycle, such as "Who controls the data?" and how will it be stored, processed and shared?[187] Mateescu, Rosenblat and boyd ask questions along the same data lifecycle, such as "When Will Cameras Be Running, and How Will Subjects Know?"; "How Long

184. boyd & Rosenblat, *supra* note 8.
185. *Id.*; Mateescu et al., *supra* note 6, at 8.
186. Paul Ohm, *Good Enough Privacy*, 2008 U. CHI. LEGAL F. 1, 49 (2008).
187. Joh, *supra* note 3, at 133–35.

Will Law Enforcement Agencies Retain Footage, and Who Can See It?", "How Is Footage Secured?"; and "When Can Biometrics Be Collected or Used?"[188] These questions loosely plot along what some conceptualize as the four major stages of a data lifecycle: collection, storage, processing, and dissemination.

These are also the four places where design decisions can support more nuanced conceptualizations of privacy such as trust and obscurity. Lawmakers and departments should strive to protect privacy by ensuring these values are proportionally respected throughout a body camera system. If there is a need for more surveillance and data processing at the collection point, then perhaps more robust obscurity and trust protections could be given to data subjects at the storage, processing, and dissemination stage. Permissive surveillance rules could dictate more robust redaction and deletion rights for data subjects and greater restrictions on access. And if the risks of surveillance or data processing are too great to compensate for downstream, then those particular acts of surveillance or data practices should be prohibited.

1. Data Collection

To protect obscurity, body cameras should, by default, be inactive until a set time, condition, or action. If the cameras are set to sense and record by default, they will be tools of persistent surveillance. Body-camera advocates might have several reasons to adopt a persistent surveillance regime. It maximizes the amount of camera footage and, thus, the perception of transparency. It might be easier for law and policy makers to carve out narrow exemptions rather than to articulate narrow activation triggers.[189] Persistent surveillance regimes also allow police departments to limit officer discretion over when to activate and deactivate the cameras.

However, a default for persistent surveillance also creates a host of problems because it is costly to store, curate, redact, and manage access to the footage.[190] It will inevitably result in less obscurity and more exposure, often when people are at their most vulnerable. Automated triggers could help solve the problem with officer discretion while simultaneously fostering people's obscurity by enacting rules that the cameras are to remain off until activated.[191]

188. Mateescu et al., *supra* note 6, at 9, 14, 19, 22.

189. *Id.* at 10.

190. Joh, *supra* note 3, at 134.

191. The ACLU's Jay Stanley has written "The balance that needs to be struck is to ensure that officers can't manipulate the video record, while also placing reasonable limits

For example, tech companies are experimenting with and marketing body camera technologies that automatically activate according to certain triggers that might indicate the need for video surveillance, such as when a gun is drawn from a holster, when a police cruiser's door is opened or lights and sirens are activated, or when raised voices are detected or an officer's pulse is quickened.[192] A built-in historical buffer can ensure that the prior few minutes leading up to activation are also captured.[193] The goal for lawmakers and police departments looking to protect privacy should be creating just enough data to serve very clearly articulated purposes, such as video evidence of the use of force or contentious police encounters, not a general surveillance and storage mandate.

With some imagination, lawmakers and police departments could also fashion rules about what kinds of information were collected by body-camera sensors upon automated triggers. For example, perhaps tiers of risk could be envisioned whereby the mere opening of a cruiser's door or voluntary activation of the camera by the officer recorded only audio, whereby sirens, raised voices, and drawn guns trigger both audio and high-quality video. Rules that limit recording in certain venues such as homes, hospitals, and other places where people are undressed or expect discretion would also help establish zones of obscurity within which people can feel more protected from digital surveillance.[194]

Lawmakers who seek to preserve trust between officers and the public should also consider mandating obvious warnings to people that the camera was on, such as a bright red, blinking recording light as well as verbal notice when feasible.[195] General prohibitions such as Jacksonville Sheriff's Office mandate that "[body cameras] shall not be used surreptitiously" are useful.[196] They could be clarified with a

on recording in order to protect privacy. One possibility is that some form of effective automated trigger could be developed that would allow for minimization of recording while capturing any fraught encounters—based, for example, on detection of raised voices, types of movement, etc." Jay Stanley, *Police Body-Mounted Cameras: With Right Policies in Place, A Win for All*, ACLU, https://www.aclu.org/other/police-body-mounted-cameras-right-policies-place-win-all [https://perma.cc/4BVR-LN88].

192. Alex Pasternack, *Police Forget to Turn on Body Cameras. Can Taser's Connected Holster Fix That?*, FAST CO. (Feb. 28, 2017) https://www.fastcompany.com/3068594/taser-connected-holster-automatic-body-camera-recording [https://perma.cc/9PC6-U2Y6].

193. *Id.*

194. Mateescu et al., *supra* note 6, at 13–14.

195. *Id.* at 13.

196. JACKSONVILLE, FLA. SHERIFF'S OFFICE, ORDER 463: BODY WORN CAMERA POLICY § II.D.5 (2017), https://www.bwcscorecard.org/static/policies/2017-07-18%20Jacksonville%20BWC%20Policy.pdf [https://perma.cc/2MPS-USQU].

design mandate that all body cameras have a clear signal to those being surveilled that the camera is operating and recording. This notification should be persistent and verbal notification should be a requirement where feasible even in "public" spaces.[197]

Autonomy rules would vest some control over whether the recording was turned on at all (or preserved) in the hands of victims and third parties. These rules might include a permission requirement and certain retention, deletion, and obscuring rights for surveillance and data subjects. Even if full control for surveillance subjects is not possible or feasible, policies should give officers some discretion to honor requests to turn off body cameras.[198] In sum, body camera data collection should be obvious, sparse, as obfuscated to the extent feasible, and possible for victims and third parties to control.

2. Data Storage

To store data is to create a privacy risk.[199] Data is searchable and persistent. It never deteriorates, unlike our memory, which naturally obscures information and contexts. Stored data is also hackable. Lawmakers should require that police departments and any third-party vendors take all reasonable measures to secure body-camera data. Given the sensitivity of this information, this standard expects a fair bit from departments and vendors.

Thankfully, lawmakers do not need to come up with a robust set of data protection practices from scratch. They simply need to ensure that departments and vendors adhere to the same full set of principles for ideal data stewardship as those in industry who collect and process personal information. This means articulating rules around data and risk identification; the necessary technical, physical, and administrative safeguards for personal information; and breach response plans. This might include mandated obscurity, data

197. *See* DALL. POLICE DEP'T, *supra* note 113, § 332.04.A.5 ("While in public areas, officers are not required to advise a subject that they are recording their interaction unless the subject specifically asks if they are being recorded, at which point the officer will inform the subject that they are being recorded.").

198. "If a request is made for a BWC to be turned off by a party being contacted, the officer should take into account the overall circumstances and what is most beneficial to all involved, before deciding to honor the request. For example, an officer may choose to turn off the BWC if its operation is inhibiting a victim or witness from giving a statement. Factors to consider may include the type of call and the vulnerability of the victim, such as the victim of a sexual assault." MINNEAPOLIS, MINN. POLICE DEP'T, BODY WORN CAMERAS § 4-223.IV.F.2 (2017), http://www.ci.minneapolis.mn.us/police/policy/mpdpolicy_4-200_4-200 [https://perma.cc/9B7F-66VP].

199. Paul Ohm, *Don't Build a Database of Ruin*, HARV. BUS. REV. (Aug. 23, 2012), https://hbr.org/2012/08/dont-build-a-database-of-ruin [https://perma.cc/7FY3-8QW3].

protection, and security impact assessments of particular policies and design choices, mandated encryption, and other de-identification and access controls such as hashing, salting, and "scrubbing" data.[200] It also might include rules about ensuring the security of data in transit from the camera to the cloud storage, or perhaps even a local storage on the camera with specific transfer times and mechanisms that do not require the camera itself to be connected to the internet.

Perhaps just as importantly in terms of storage, lawmakers should mandate regular deletion as well as give data subjects deletion rights. These are not easy lines to draw. Mateescu, Rosenblat, and boyd note that there is no generally agreed upon time or formula to determine how long footage is to be kept.[201] They note that there are many factors to be considered, including the cost of retention, what types of footage to keep and flag for review, how long to keep footage that has value in investigations or as evidence, the risk of retained footage being misused for unconstitutional or harmful surveillance, and the risk "that footage can be analyzed to divergent purposes, with differing and prescribed rules for access, review, and analysis."[202] Joh wrote, "[t]he few states that have addressed body-worn camera video storage limits have generally erred on the side of limiting video storage unless it is involved in a criminal investigation."[203] She notes that the tradeoff is difficult because there are several advantages to longer storage times:[204]

> Shorter storage times means there is less data (of the innocent as well as the guilty) available for inspection and analysis. Yet longer data storage periods may enhance public accountability if it means that the public—citizens, journalists, and researchers—can access video that can illuminate individual cases as well as general policing practices.[205]

But these lines mandating deletion after a certain time and upon certain requests must be drawn. The alternative is persistent retention, which is a risk to people's obscurity and autonomy. While it is costly to create a system to protect and scrub data, flag certain data

200. *See, e.g.*, Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 WASH. L. REV. 703, 743 (2016). Hashing, salting, and "scrubbing" data are all concepts that involve changing certain characteristics of data to make it unintelligible, inaccessible, or de-identified.

201. Mateescu et al., *supra* note 6, at 14.

202. *Id.*

203. Joh, *supra* note 3, at 135.

204. *Id.*

205. *Id.*

for retention, and delete the rest, this is a minimum price for the safe implementation of body cameras.

3. Data Processing

Data can be processed in ways that destroy obscurity and erode people's trust and autonomy. Industry already processes data and uses algorithms in inscrutable and dangerous ways.[206] As a starting matter, governments and departments that are particularly committed to privacy might even consider adopting some of the framework of the European Union's General Data Protection Regulation for data.[207] This framework prohibits data processing without a legitimate reason.[208] Academics and governments have written volumes on the virtues of a data protection framework.[209] This Article merely proposes it as an established guide for the development of fair data processing rules, with a preference for design restrictions instead of consent of the data subject as a legitimatization lever.

However, protecting obscurity and trust might require more. Lawmakers should create rules to prevent obscurity lurches like the use of biometrics and disloyal repurposing of data. Biometrics are a particular area of concern for body cameras. The Police Executive Research Forum ("PERF") report states that "Body-worn cameras raise many privacy issues that have not been considered before. Unlike many traditional surveillance methods, body-worn cameras can simultaneously record both audio and video and capture close-up images that allow for the potential use of facial recognition technology."[210] The Leadership Conference argued that "[b]iometric evaluation of footage must be strictly limited to narrow, well-defined uses, and subject to judicial authorization."[211] I agree. Facial

206. *See* PASQUALE, *supra* note 54, at 216.

207. Council Regulation 2016/679, 2016 O.J. (L 119) 7–8.

208. *Id.*

209. *See generally* COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE (2003) (discussing privacy protections in a global context); GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE AND HUMAN RIGHTS PERSPECTIVES (2014) (discussing privacy laws in Asia); Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115 (2017) (addressing privacy protection measures in the European Union and the United States).

210. POLICE EXEC. RESEARCH FORUM, IMPLEMENTING A BODY-WORN CAMERA PROGRAM: RECOMMENDATIONS AND LESSONS LEARNED 11 (2014), https://www.justice.gov/iso/opa/resources/472014912134715246869.pdf [https://perma.cc/RP63-GPBF]. PERF sent out a survey to 500 agencies, of which 254 responded. *Id.* at 2.

211. Letter from Wade Henderson, President & CEO, Leadership Conference on Civil & Human Rights ("LCCHR"), & Nancy Zirkin, Exec. Vice President, LCCHR, to the President's Task Force on 21st Century Policing (Jan. 30, 2015), https://www.bja.gov/bwc

recognition should be an exceptional event. Biometrics allow for dramatic lurches in obscurity. Elsewhere, I have explored with Evan Selinger about why facial recognition is a corrosive menace to our cherished obscurity.[212] We argued that people don't have the expectation they will be practically monitored everywhere they go, nor do they have the ability to fully embrace paranoid risk-management strategies to hide from surveillance.[213] Rather, we have always been able to "hide in plain sight."[214] We argue that "[u]biquitous and unrestrained facial recognition technologies wouldn't just alter this longstanding presumption, it would shatter it entirely."[215]

Lawmakers should either prohibit the use of facial recognition technologies outright or subject them to procedural protections like mandatory privacy impact assessments before implementation and judicial authorization before use. Additionally, lawmakers should limit the reuse of data collected by body cameras for other facial recognition programs. As I have written elsewhere with Evan Selinger, the full potential of facial-matching technologies requires a comprehensive name-face database to compare with current surveillance images.[216]

There will likely be a great incentive or demand for police departments to share the data and biometrics databases with others. But if we value autonomy and obscurity and all the benefits of freedom from surveillance, lawmakers should create rules against the use of body-camera data for facial recognition.

Additionally, lawmakers should establish rigid rules limiting or prohibiting the reuse of data collected by body cameras. One of the key tenets of fair information process is what some call "purpose limitation."[217] This key ethic has been described by many as having

/pdfs/2015-01-30-letter-to-task-force-on-21st-century-policing.pdf [https://perma.cc/AVS4-MG7M].

212. Evan Selinger & Woodrow Hartzog, *Opinion: It's Time for an About-Face on Facial Recognition*, THE CHRISTIAN SCIENCE MONITOR (June 22, 2015), https://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0622/Opinion-It-s-time-for-an-about-face-on-facial-recognition [https://perma.cc/6TAP-JXDC].

213. *Id.*

214. *Id.*

215. *Id.*

216. Woodrow Hartzog & Evan Selinger, *I See You: The Databases That Facial-Recognition Apps Need to Survive*, ATLANTIC (Jan. 23, 2014), https://www.theatlantic.com/technology/archive/2014/01/i-see-you-the-databases-that-facial-recognition-apps-need-to-survive/283294/ [https://perma.cc/L5P3-KGB6].

217. *See* Opinion of the Article 29 Data Protection Working Party on "Purpose Limitation" 00569/13/EN, WP 203, at 3–5 (Apr. 2, 2013). *But see* Lokke Moerel & Corien

two parts: the first, often referred to as "purpose specification," holds that "data must be collected for specified, explicit and legitimate purposes only," and the second, often referred to as "compatible use," holds that "data must not be further processed in a way that is incompatible with those purposes."[218] In essence, data collected for one very specific purpose cannot and should not be used for another incompatible purpose. This is a key data ethic that underlies many international data protection regimes, including Europe's General Data Protection Regulation.[219]

Given the sensitive nature of the information collected by body cameras, mere purpose limitations might not be enough. In previous research, I have argued with Neil Richards that part of the duty of trust includes a duty of loyalty—a data processor's obligation to avoid self-dealing at the expense of those who trust them.[220] We wrote that many of our fears about big data are really fears about organizations being disloyal to us and using information in ways adverse to us.[221] Will big data analytics deny us meaningful opportunities such as mortgages or jobs?[222] Will big data redlining have a disparate impact on minority and marginalized populations?[223]

Lawmakers should prohibit departments and vendors from reusing information not just in ways incompatible with the purpose specified for collection, but also in disloyal ways. This means limiting those who can access data and making governments and third-party vendors promise not to engage in self-dealing. One way to prevent the incentive to reuse information in disloyal ways is to ensure that governments pay for vendor services with money, not data. As we have seen, the dominant business model on the web in which technology companies offer free services in exchange for personal

Prins, *On the Death of Purpose Limitation*, INT'L ASS'N OF PRIVACY PROFESSIONALS (Jun. 2, 2015) https://iapp.org/news/a/on-the-death-of-purpose-limitation/ [https://perma.cc/Q6TM-QXC2] (arguing that the purpose limitation test is outdated and should be replaced by a test based on legitimate interest).

218. *Id.*

219. Council Regulation 2016/679, 2016 O.J. (L 119) 35. ("Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, . . . not be considered to be incompatible with the initial purposes.").

220. Richards & Hartzog, *Taking Trust Seriously*, *supra* note 131, at 469–71.

221. *Id.* at 471.

222. *Id.*

223. *Id.*

information, is a model for exploitation.[224] Elizabeth Joh has chronicled the corrosive influence that body-camera vendors have over body-camera policy.[225] Lawmakers must create rules to counter the power incentives for department and vendor exploitation.

4. Data Dissemination

Finally, lawmakers and courts must determine when data is disclosed and to whom. There are many possible considerations regarding the release of body-camera data. Answering them will involve confronting the traditional journalistic aspects of a story: Who can access the data? What can they access? When and where can they access the data? And how can they access the data?

Instead of binary rules that either keep information locked up or release to the public for any and all uses, it might be best to use the relative obscurity and confidentiality of information as a slider to determine the extent to which information is protected and released. Some parties might have more access than others based on their need for information. Other kinds of data might be less sensitive or better obscured, for example with faces or sound blurred out or the entire screen blurred with a filter.

In confronting the many different factors relevant to disclosure, lawmakers might consider adopting rules that leverage promises of trust through contracts and rules that limit things like commercial use of body cameras or attempts at re-identification. Lawmakers might also consider innovative redaction, blurring, video-only, audio-only, and other redaction techniques. The goal of a safe disclosure regime is to tailor the disclosure to the need to serve the multiple values of privacy, due process, and government accountability.

As an initial matter, body-camera policies can probably better balance privacy with other values by differentiating who is allowed to access the records. Many policies already reflect this differentiation.[226]

224. *See* HARTZOG, *supra* note 14, at 1–5; Chris Jay Hoofnagle & Jan Whittington, *Free: Accounting for the Costs of the Internet's Most Popular Price*, 61 UCLA L. REV. 606, 608–12 (2014).

225. Joh, *supra* note 5, at 112–17.

226. For example, the Las Vegas body camera policy provides that

> [t]o timely process requests and ensure that privacy rights, confidentiality laws, and laws regarding the release of criminal history are complied with, the Department has classified requestors into three general categories. These categories are: (1) Media; (2) Involved Citizens (may include attorney representatives with letters of representation and client authorization); and (3) General Public. Each group necessitates slightly different procedures. These procedures are outlined below by category.

Putting aside important questions over access to evidence, in order to protect their autonomy, those who have been surveilled should be guaranteed access or at least a presumption of access to body camera data. Some policies already provide this. For example, the Newark Police Department has a policy to tag recordings that raise privacy concerns and limit access to those tagged recordings.[227]

One important problem to protect against is officers accessing records for retaliation purposes or just general snooping. This can be a violation of trust, obscurity, and autonomy. The ACLU has advocated that "[t]he use of recordings should be allowed only in internal and external investigations of misconduct, and where the police have reasonable suspicion that a recording contains evidence of a crime."[228] "Otherwise," according to the organization, "there is no reason that stored footage should even be reviewed by a human being before its retention period ends and it is permanently deleted."[229] Snooping in entrusted and generally inaccessible information is disloyal and serves the interests of the voyeur only. Provisions should be put in place to prohibit it.[230]

LAS VEGAS METRO. POLICE DEP'T, BODY WORN CAMERA RECORDINGS, https://www.lvmpd.com/en-us/Pages/Body-Worn-Camera-Recordings.aspx [https://perma.cc/45ZS-FZQN].

227. The Newark Police Division's body-worn camera policy states:

> To identify BWC recordings that may raise special, privacy or safety issues, officers shall tag recordings. Recordings containing any of the following shall be tagged: 1) The image of a victim of a criminal offense; 2) The image of a child; 3) Images in a residential premise (e.g., home, apartment, college dormitory room, hotel/motel room, etc.), a school or youth facility, healthcare facility or medical office, substance abuse or mental health treatment facility, or a place of worship.); 4) Conversation with a person whose request to deactivate the BWC was denied; 5) Special operations event or execution of an arrest and/or search warrant where confidential tactical information may have been recorded; 6) The image of an undercover officer or confidential informant; 7) The screen of a law enforcement computer monitor that is displaying confidential personal or law enforcement sensitive information.

NEWARK POLICE DIV., BWC POLICY § VII(5), http://npd.newarkpublicsafety.org/bodyworncamera/policy [https://perma.cc/CRZ4-ARSP].

228. Stanley, *supra* note 191.

229. *Id.*

230. For example, the Ferguson Police Department policy states that "General access to digital recordings shall be granted to Department-authorized users only. It is the responsibility of authorized users to keep their username and password confidential. Accessing, copying, or releasing any recordings for other than official law enforcement purposes is strictly prohibited, except as required by law or this policy and procedure." FERGUSON OFFICE OF THE CHIEF OF POLICE, GENERAL ORDER PR481.6: AUTHORIZED USER ACCESS TO UPLOADED MEDIA OR DATA, (2016), https://www.bwcscorecard.org/static/policies/2016-02-26%20Ferguson%20-%20BWC%20Policy.pdf [https://perma.cc/GN46-A8MG]. The Las Vegas policy states that "Employees, other than those assigned to the

Finally, lawmakers must seek to facilitate public disclosure of body-camera data in a safe, sustainable way. Public records law is the primary vehicle for dissemination of government information and facilitation of government transparency. Mateescu, Rosenblat, and boyd write that "[p]ublic records laws are intended to grant citizens access to government records. This raises a question of whether body-worn camera video is a public record, and if so, whether it may or must be disclosed."[231] Each state has different rules about which records are to be made public and which are to be withheld under certain exceptions for things like privacy, trade secrets, and ongoing investigations.

Mateescu, Rosenblat, and boyd summed up the different views on public disclosure of body camera footage and data:

> According to the ACLU, policymakers must "carefully balance," "the need for government oversight and openness, and privacy," when creating policies about public disclosure. To do that, it suggests flagging those videos "for which there is the highest likelihood of misconduct" and redacting video "when feasible" and asserts that unredacted video should only be publicly disclosed with the consent of the subject. However, redacted video and unredacted flagged video should be subject to disclosure, and according to the Leadership Conference, redacted footage should be made available for non-commercial public interest purposes, with the right protections for witnesses and victims. PERF suggests that agencies should have clear protocols for releasing recorded data to the public, consistent with public disclosure laws.[232]

Regarding what kinds of data parties can access, certain policies limit the public disclosure of information that is "private" or vaguely "confidential." The Charlotte-Mecklenburg Police Department has a policy that limits disclosure if "[t]he recording contains information that is otherwise confidential or exempt from disclosure or release

Body Camera Detail, Internal Affairs, Force Investigative Team (FIT) or Critical Incident Review Team (CIRT) shall not download, copy, or record BWC recordings from Evidence.com onto any computer, device, drive, CD/DVD, or any other format without the express written consent of the Body Camera Detail Lieutenant," and "Employees shall not publish or display BWC recordings to the internet or social media sites." LAS VEGAS METRO. POLICE DEP'T, EVIDENCE AND PROPERTY PROCEDURES § 5/210.01: BODY WORN CAMERAS (2015), https://www.bwcscorecard.org/static/policies/2015-10%20Las%20Vegas%20-%20BWC%20Policy.pdf, [https://perma.cc/DZK5-8398].

231. Mateescu et al., *supra* note 6, at 18.

232. *Id.* at 19

under State or federal law."[233] But these terms could use some clarification. We've already discussed how the term privacy is not helpful. When policies use the term "private," do they mean confidential? Obscure?

If they do mean confidential, the policy should clarify that it is the data subject's confidence that is to be kept, not a general wish for secrecy that could mask a desire to protect against embarrassment. Some examples would also be helpful besides simply "social security numbers," like the vague policy of the Columbus Police Department which provides "[r]eleased video/audio footage will not contain any confidential information such as social security numbers, personal information about police officers, etc. unless expressly requested and approved by the Chief of Police and the prosecuting attorney."[234] Confidence is ultimately determined by the terms of a relationship and disclosure, even if the sensitive nature of information might affect whether an implied confidence exists.

If the policy is meant to protect obscurity, then it should provide a framework for determining the relative obscurity of information. I have written in the past that obscurity is a combination of factors including structural protections, cultural norms, and the desirability of information by other parties.[235] Online, obscurity is a product of lack of searchability, limited access, de-identification, and opacity of meaning.[236] The more people rely upon being obscure, the greater protections that might apply.

Access need not be granted on an all-or-nothing basis. Information can be blurred and redacted to obscure sensitive aspects of information while providing the public access to important records.[237] Seattle has taken the innovative step of releasing blurred

233. CHARLOTTE-MECKLENBURG POLICE DEP'T, INTERACTIVE DIRECTIVES GUIDE 400-006: BODY WORN CAMERA (BWC) (2017), https://www.bwcscorecard.org/static/policies/2017-05-08%20Charlotte-Mecklenberg%20BWC%20Policy.pdf [https://perma.cc/F3TY-7B5P].

234. COLUMBUS POLICE, DEP'T STANDARD OPERATING PROCEDURES 1.15, BODY WORN VIDEO SYSTEM (2015), https://www.bwcscorecard.org/static/policies/2015-02-03%20Columbus%20BWC%20Policy.pdf [https://perma.cc/2H94-J9FS].

235. Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1358 (2015); Hartzog & Stutzman, *Online Obscurity*, *supra* note 147, at 21.

236. *See* Hartzog & Selinger, *supra* note 235, at 1358; Hartzog & Selinger, *supra* note 146.

237. *See* Ardia & Klinefelter, *supra* note 88, at 1825–28 (2015); David S. Ardia, *Privacy and Court Records: Online Access and the Loss of Practical Obscurity*, 2017 U. ILL. L. REV. 1385 (2017).

and obscured body camera data on YouTube.[238] The data need not be made available by default, either. Lawmakers might experiment with releasing some information in limited formats, such as at a terminal in person but not in an easily sharable digital format.

Finally, lawmakers might condition public access on a few important rules. If the information has been redacted or de-identified, lawmakers could prohibit attempts at re-identification through technological means. Additionally, lawmakers might consider rules that mitigate the problem of commercial entities clogging the public records system with requests for records they can monetize in bulk.[239] While lawmakers might consider prohibiting some kinds of egregious bulk commercial uses of body camera data, Margaret Kwoka has suggested the answer to the commercial public records problem is to affirmatively disclose the kinds of records that are subject to routine public records problems.[240] It remains to be seen which actors will make the most requests for body camera data. But it is clear that lawmakers must try to carefully balance interests of access with obscurity and autonomy interests.

CONCLUSION

If lawmakers keep applying the same privacy frameworks to the rules for body cameras, they will get what they've always gotten: an inconsistent set of rules that do not seem to match people's actual expectations of privacy and actually seem to facilitate the slow creep toward more surveillance. It is hard to balance privacy with other critical interests such as government accountability and free speech when privacy is poorly defined. Privacy law has a blind spot when lawmakers only focus more on when surveillance is conducted and what people do with data and less on how data and surveillance technologies are built. Body cameras are an opportunity to change that. Or give us more of the same.

238. Wylie Wong & Phil Goldstein, *Seattle Shares Body-Cam Footage on YouTube*, STATETECH (Jan. 21, 2016), https://statetechmagazine.com/article/2016/01/seattle-shares-body-cam-footage-youtube [https://perma.cc/SE4B-664L].

239. Kwoka, *FOIA, Inc.*, *supra* note 92, at 1429–36.

240. *Id.*