PRIVACY AND CYBERSECURITY LESSONS AT THE INTERSECTION OF THE INTERNET OF THINGS AND POLICE BODY-WORN CAMERAS*

PETER SWIRE** & JESSE WOO***

Prepared for the North Carolina Law Review symposium on police body-worn cameras ("BWCs"), this Article shows that BWCs can be conceptualized as an example of the Internet of Things ("IoT"). By combining the previously separate literatures on BWCs and IoT, this Article shows how insights from each literature apply to the other.

Part I adopts the IoT definition of (1) a sensor connected to the Internet that (2) stores and/or processes data remotely, typically in the cloud. Applied to BWCs, the camera is a sensor, and the video footage and related data are stored outside of the original camera, often in the cloud.

Building on this equivalence of BWCs and IoT, Part II examines lessons from the substantial IoT literature for BWC privacy and cybersecurity. Part II systematically examines leading industry standards and Federal Trade Commission guidance that could be used to develop applicable criteria for good practice for BWCs. Analysis of this literature suggests three themes for operationalizing these best practices. First, police departments can and should learn from the IoT literature to improve privacy and cybersecurity for BWCs. Second, police departments should use their bargaining power to demand security and privacy best

** Holder Chair of Law and Ethics, Georgia Institute of Technology Scheller College of Business. For comments on earlier versions of this Article, the authors thank DeBrae Kennedy-Mayo and participants at the *North Carolina Law Review* symposium on police body-worn cameras. General research support was provided by the Georgia Tech Scheller College of Business, the Georgia Tech Institute for Information Security and Privacy, and the Hewlett Foundation.

*** At the time of writing this Article, Jesse Woo was a research associate faculty member at the Georgia Institute of Technology Scheller College of Business. J.D., University of Washington.

practices from their vendors. Third, where departments lack the in-house expertise to handle BWC security and privacy they should seek it from outside institutions or consultants, including from outside experts in IoT security and privacy.

Part III examines two areas where study of BWCs might offer lessons for the broader domain of IoT. First, to protect police officer privacy during breaks and for other reasons, BWCs are not always on. By contrast, IoT best practices to date have not emphasized the implications of toggling the sensor on and off. Second, an important debate for BWCs is how to promote transparency—to provide accountability while protecting individual privacy. In this respect, BWCs are an application of technology where public disclosure of the entire data feed is a higher priority than for most other IoT applications to date. Studying this debate can inform other IoT debates about when to open full data feeds to the public, consistent with privacy and cybersecurity concerns.

Privacy and cybersecurity risks will continue to evolve for both IoT generally and BWCs more specifically. Recognizing the overlap of these two usually distinct discourses can offer assistance to those in both realms as they face the new risks.

INTRODUCTION

This Article examines privacy and cybersecurity issues for the topic of this symposium, police body-worn cameras ("BWCs"). BWCs already generate, and will increasingly generate, a great amount of video footage and related content. In our era of increasingly effective facial recognition, this video footage generates a vast amount of personally identifiable information, with consequent privacy issues. Over time, the volume of video footage will increase enormously, creating challenging cybersecurity issues for the data that is stored, often in the cloud. Cities and police departments will face substantial challenges in managing these privacy and cybersecurity issues.

To develop good privacy and cybersecurity practices for BWCs, this Article proposes drawing on the already substantial experience with the Internet of Things ("IoT"). Definitions of IoT abound,[1] but key aspects of the technology are (1) a sensor connected to the Internet that (2) stores and/or processes data remotely, typically in the cloud.[2] Applied to BWCs, the camera is a sensor, and the video footage and related data are stored outside of the original camera, often in the cloud. Part I discusses the definition of IoT and describes how the technical capabilities and uses of BWCs fit this definition.

Regulators, industry standards groups, and other experts have already developed documents that set forth best practices for privacy and cybersecurity in the IoT. In Part II, this Article examines three sets of best practices, which we believe will assist large and small police departments in recognizing and responding to privacy and cybersecurity risks:

1. *See* Harald Bauer, Mark Patel & Jan Veira, *The Internet of Things: Sizing up the Opportunity*, MCKINSEY & CO. (Dec. 2014), http://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things-sizing-up-the-opportunity [https://perma.cc/A9LT-CU9K]; Andrew Meola, *What is the Internet of Things (IoT)?*, BUS. INSIDER (Dec. 19, 2016, 2:11 PM), http://www.businessinsider.com/what-is-the-internet-of-things-definition-2016-8 [https://perma.cc/782H-82EN].

2. *See* Sona R. Makker, *Overcoming "Foggy" Notions of Privacy: How Data Minimization Will Enable Privacy in the Internet of Things*, 85 UMKC L. REV. 895, 897 (2017). When we say data is stored "in the cloud," we mean it is stored on a remote server via an internet connection. These servers are part of the infrastructure of "cloud computing," which is defined as "the delivery of on-demand computing resources—everything from applications to data centers—over the internet on a pay-for-use basis." *What is Cloud Computing?*, IBM, https://www.ibm.com/cloud/learn/what-is-cloud-computing [https://perma.cc/SR2J-WU9S].

(1) The Broadband Internet Technical Advisory Group ("BITAG") has promulgated cybersecurity and privacy recommendations for IoT.[3] The BITAG report provides state-of-the-art recommendations for IoT, especially for software.

(2) Microsoft has issued its Internet of Things Security Best Practices.[4] These complement the BITAG recommendations due to their focus on good physical security and hardware practices.

(3) The Federal Trade Commission ("FTC") has written extensively on IoT for both privacy and cybersecurity issues. Along with the software and hardware recommendations of the BITAG and Microsoft, the FTC has numerous recommendations about appropriate administrative measures for the entire life-cycle of data from collection, through storage and use, to eventual destruction.[5]

The expert IoT literature recommends security best practices, such as patchability and encryption, and privacy best practices, such as data minimization.[6] This Article's analysis of the literature suggests three themes for operationalizing these best practices. First, police departments can and should learn from the IoT literature to improve privacy and cybersecurity for BWCs. Second, police departments should use their bargaining power to demand security and privacy best practices from their vendors. Third, when departments lack the in-house expertise to handle BWC security and privacy, they should seek it from outside institutions or consultants, including from outside experts in IoT security and privacy.

Part III examines two areas where study of BWCs might offer lessons for the broader domain of IoT. First, to protect police officer privacy during breaks and for other reasons, BWCs are not always on.[7] By contrast, IoT sources such as the BITAG report and

3. BROADBAND INTERNET TECH. ADVISORY GRP., INTERNET OF THINGS (IOT) SECURITY AND PRIVACY RECOMMENDATIONS 18 (2016), https://www.bitag.org/documents/BITAG_Report__Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf [https://perma.cc/6AZM-V2XM].

4. *See* Dominic Bets & Yuri Diogenes, *Internet of Things Security Best Practices*, MICROSOFT AZURE (Jan. 17, 2018), https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-best-practices [https://perma.cc/6GQW-VTRY].

5. FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, at iii (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/U3AQ-UTQD].

6. *Id.* at 30–38.

7. JAY STANLEY, AM. CIVIL LIBERTIES UNION, POLICE BODY-MOUNTED CAMERAS 3 (2013), https://www.aclu.org/files/assets/police_body-mounted_cameras.pdf [https://perma.cc/N5V7-S9TZ].

Microsoft recommendations do not emphasize how to govern the possibility of toggling the sensor on and off.[8] Analysis of BWCs thus may help supplement the existing IoT set of best practices. Second, an important debate for BWCs is how to promote transparency—to provide accountability while protecting individual privacy.[9] In this respect, BWCs are an application of technology where public disclosure of the entire data feed is a higher priority than for most other IoT applications to date.[10] Studying this debate can inform other IoT debates about when to open full data feeds to the public, consistent with privacy and cybersecurity concerns.

I. POLICE BODY-WORN CAMERAS ARE PART OF THE INTERNET OF THINGS

This Part discusses the definition of IoT and describes how the technical capabilities and uses of police BWCs fit this definition. It will also review the BWC and IoT scholarship to show how the privacy and cybersecurity problems are similar for both technologies, yet the literature has not typically made this connection.

A. The Functionality of BWCs Fits the Definition of IoT

This Section provides a brief technical definition of IoT and shows how BWCs fit under that definition as an IoT device. IoT is a rapidly growing category of technology that many analysts believe will cause the next great wave of digitization and productivity enhancement.[11] Examples of IoT devices range from the internet-connected Amazon Echo speaker to connected traffic lights and smart utility meters.[12] Many are excited for the potential of IoT

8. *See* BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3, at ii–iv; Bets & Diogenes, *supra* note 4.

9. OFFICE OF THE PRIVACY COMM'R OF CAN. ET AL., GUIDANCE FOR THE USE OF BODY-WORN CAMERAS BY LAW ENFORCEMENT AUTHORITIES 2 (2015), https://www.priv.gc.ca/media/1984/gd_bwc_201502_e.pdf [https://perma.cc/TK28-P24M].

10. *Cf.* Mary D. Fan, *Privacy, Public Disclosure, Police Body Cameras: Policy Splits*, 68 ALA. L. REV. 395, 410–12 (2016) (demonstrating that public debate over police accountability and America's robust tradition of government transparency have spurred enthusiasm for disclosure of BWC footage).

11. *See* Meola, *supra* note 1.

12. *See* Matt Bellias, *3 Ways IoT Will Change Smart Meters for Utilities*, IBM: INTERNET OF THINGS BLOG (Dec. 1, 2016), https://www.ibm.com/blogs/internet-of-things/smart-meter-grid/ [https://perma.cc/VS56-7D3S]; Arjun Kharpal, *Amazon's Alexa Stole the Show at CES in a Bid to Become the Internet of Things Operating System*, CNBC (Jan. 6, 2017 10:43 AM), https://www.cnbc.com/2017/01/06/ces-2017-amazon-alexa-stole-the-show-a-bid-to-become-the-iot-operating-system.html [https://perma.cc/9NXJ-7KNE];

devices to monitor traffic congestion or the electrical grid.[13] Often, the power of IoT comes from the high volume of sensors that can be deployed and connected within a system.[14] Having many sensors allows for precision monitoring of complex systems, which can help with problems such as infrastructure maintenance, by identifying failure points without the need for human inspection.[15] Other applications include smart homes devices (like the Nest thermometer) and internet-connected medical devices that allow for more granular control and personalization.[16] Analysts project that by 2020, the IoT market will grow to over $470 billion in annual revenue, with over thirty billion devices installed.[17]

Definitions of IoT abound,[18] but key aspects of the technology are (1) a sensor connected to the internet that (2) stores and/or processes data remotely, typically in the cloud.[19] The sensor measures some physical property of the world and may be aural, thermal, chemical, or some other type, but in many cases, it is visual.[20] It is also

SierraWireless, *Smart Traffic Lights Help Ease the Burden of Rush Hour on City Infrastructure*, IOT BLOG (Jul. 21, 2017), https://www.sierrawireless.com/iot-blog/iot-blog/2017/07/smart_traffic_lights_help_ease_the_burden_of_rush_hour_on_city_infrastructure/ [https://perma.cc/XE7Z-3YVM].

13. *See, e.g.*, Qinghai Ou et al., *Application of Internet of Things in Smart Grid Power Transmission*, 2012 THIRD FTRA INT'L CONF. ON MOBILE, UBIQUITOUS, & INTELLIGENT COMPUTING 96, 96, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6305831 [https://perma.cc/9DDH-X4ND (staff-uploaded archive)]; Tanvi T. Thakur et al., *Real Time Traffic Management Using Internet of Things*, 2016 INT'L CONF. ON COMM. AND SIGNAL PROCESSING 1950, 1950, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7754512 [https://perma.cc/2PWG-844Z (staff-uploaded archive)].

14. *See* Makker, *supra* note 2, at 897.

15. *See* Ou et al., *supra* note 13, at 99.

16. Mathias Cousin, Tadashi Castillo-Hi & Glenn H. Snyder, *Devices and Diseases: How the IoT is Transforming Medtech*, DELOITTE INSIGHTS (Sep. 11, 2015), https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-in-medical-devices-industry.html [https://perma.cc/5JUA-8RW3]; Andrew Meola, *How IoT & Smart Home Automation Will Change the Way We Live*, BUS. INSIDER (Dec. 19, 2016, 4:44 PM), http://www.businessinsider.com/internet-of-things-smart-home-automation-2016-8 [https://perma.cc/U7A8-7FGS].

17. Louis Columbus, *Roundup of Internet of Things Forecasts and Market Estimates, 2016*, FORBES (Nov. 27, 2016, 1:06 PM), https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#50c87fef292d [https://perma.cc/L8L9-KYDN].

18. Bauer et al., *supra* note 1; Meola, *supra* note 1.

19. Makker, *supra* note 2, at 897–98 ("The ubiquitous deployment of sensors form [sic] the backbone of what has been dubbed the 'Internet of Things' (IoT).") Another important aspect of some IoT applications is the ability of machines to communicate with one another, as with autonomous vehicles, but that definition is less pertinent to our discussion here.

20. *Id.* at 897.

embedded into physical objects (the "Thing" of Internet of Things) that in the past have not normally contained computational power or internet connectivity.[21] Streetlights with internet-connected cameras are an increasingly common example of a visual IoT sensor.[22] The sensor is a necessary component of IoT because it collects data, and that data collection opens up numerous useful applications.[23]

A similarly important part of the IoT definition is the storage and processing of all that sensor data in the cloud. Cloud storage allows the people who run sensor networks to harness the massive amounts of data that IoT generates,[24] and therefore enables the many benefits that can come from the combination of "Big Data" analysis and IoT devices.[25] Cloud storage is also necessary because many IoT devices have limited storage and computational power on the device itself, so they require the cloud to function effectively.[26]

Police BWCs fit both parts of this definition of IoT. A BWC is a camera and microphone typically worn near the officer's front chest pocket or head-mounted on eyewear or a helmet.[27] As a camera, it is a sensor by definition.[28] In some cases, the audio-visual footage (the

21. In earlier work, Swire and co-authors proposed shifting the name to "Internet of Devices," to highlight the fact that the devices are connected to the internet, while many "things" will remain unconnected (such as trees, to illustrate the point). RICHARD L. RUTLEDGE ET AL., GA. INST. OF TECH., DEFINING THE INTERNET OF DEVICES: PRIVACY AND SECURITY IMPLICATIONS 2 (2014), https://smartech.gatech.edu/bitstream/handle/1853/52020/plsc2014-IoD.pdf [https://perma.cc/2VSB-DQBR]. In this Article, the authors use the now-pervasive term "Internet of Things."

22. Lily Hay Newman, *Sheesh, Even Streetlights Are Getting Cameras and Internet Connections*, SLATE (Oct. 2, 2015, 4:14 PM), http://www.slate.com/blogs/future_tense/2015/10/02/ge_intelligent_lamp_posts_have_cameras_sensors_may_come_to_new_york_city.html [https://perma.cc/6AD7-XRW4].

23. *See* Daniel Burrus, *The Internet of Things is Far Bigger Than Anyone Realizes*, WIRED, https://www.wired.com/insights/2014/11/the-internet-of-things-bigger/ [https://perma.cc/BAK9-M49H].

24. Andrew Meola, *The Roles of Cloud Computing and Fog Computing in the Internet of Things Revolution*, BUS. INSIDER (Dec. 20, 2016, 5:11 PM), http://www.businessinsider.com/internet-of-things-cloud-computing-2016-10 [https://perma.cc/4DB6-LRKS].

25. EXEC. OFFICE OF THE PRESIDENT, BIG DATA 5 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [https://perma.cc/44RE-YRJG].

26. Mike Chen, *Why Cloud Computing is the Foundation of the Internet of Things*, THORN TECHS. (Feb. 15, 2017), https://www.thorntech.com/2017/02/cloud-computing-foundation-internet-things/ [https://perma.cc/DNV5-UGQ8].

27. VIVIAN HUNG, STEVEN BABIN & JACQUELINE COBERLY, A PRIMER ON BODY-WORN CAMERAS FOR LAW ENFORCEMENT 5 (2016), https://www.justnet.org/pdf/00-Body-Worn-Cameras-508.pdf [https://perma.cc/D9D5-TN8R].

28. *Camera*, MERRIAM-WEBSTER (3d ed. 1993).

data) may be stored locally on the camera and later uploaded to a central repository,[29] but newer models upload or stream the data directly to the cloud.[30] The data may stream directly to the cloud or through another piece of equipment such as the patrol car.[31] Axon (formerly Taser), the largest BWC manufacturer, also offers data storage and processing services where the company can manage and analyze the footage for police departments.[32] Like some other IoT manufacturers, Axon has evolved from a producer of hardware to a "data as a service" vendor by maintaining the cloud services for BWC data.[33] In short, BWCs are examples of IoT devices—they have sensors and their data is generally stored and analyzed remotely, typically in the cloud. Use of BWCs is beginning to migrate from the policing context into other sectors, including healthcare and education.[34] This expansion of BWC deployment also fits the conceptual model of BWCs as a type of general purpose IoT device rather than a pure policing tool.

Having established that BWCs qualify as a type of IoT application, the next two Sections will demonstrate how the BWC and IoT literatures identify similar privacy and cybersecurity issues. Section I.B introduces the privacy and cybersecurity concerns presented in the BWC literature. In brief, these concerns are the

29. A model where data is recorded and later uploaded to the cloud from a central access point does not perfectly fit the definition of IoT, but the analogy that a distributed network of sensors funnel data back to a central point for storage and processing does fit.

30. *See* Matt Stroud, *Taser Plans to Livestream Police Body Camera Footage to the Cloud by 2017*, MOTHERBOARD (July 18, 2016, 3:06 PM), https://motherboard.vice.com/en_us/article/4xa43g/taser-axon-police-body-camera-livestream [https://perma.cc/DZD5-YJFN]. Facial recognition is another emerging capability of BWCs that raises privacy concerns, but it is not yet widespread. *Id.*

31. *See* Matt Stroud, *The Company That's Livestreaming Police Body Camera Footage Right Now*, MOTHERBOARD (July 27, 2016, 6:00 AM), https://motherboard.vice.com/en_us/article/9a3ddv/visual-labs-police-body-camera-livestream [https://perma.cc/P7DE-DPB3].

32. Alex Pasternack, *Why Taser Changed Its Name and Offered Every Cop A Body Camera*, FAST COMPANY (Apr. 6, 2017), https://www.fastcompany.com/40402050/taser-axon-police-body-cameras-video-evidence-data [https://perma.cc/4UY5-W25W].

33. *Id.*

34. Our research to date has discovered these deployments in the United Kingdom. Sarah Knapton & Peter Walker, *Doctors and Nurses Could be Issued with Body Cameras to Record Violent Patients*, TELEGRAPH (May 5, 2017) http://www.telegraph.co.uk/science/2017/05/05/doctors-nurses-could-issued-on-body-cameras-record-violent-patients/ [https://perma.cc/N515-QBYY]; Rozina Sabur, *Teachers Wearing Body Cameras to Control Students' Behavior in New Trial*, TELEGRAPH (Feb. 8, 2017) http://www.telegraph.co.uk/news/2017/02/08/teachers-wearing-body-cameras-control-students-behaviour-new/ [https://perma.cc/Y86Y-93SV].

challenge of ubiquitous sensors to privacy in public and private spaces; the difficulties with consent, raising trade-offs between privacy and transparency; and the security of digital evidence gathering tools. Section I.C will show how these issues relate to IoT.

B. BWCs Raise Privacy and Cybersecurity Issues

BWCs pose challenges for privacy in both public and private spaces. Private spaces are those where a person has a reasonable expectation of privacy, such as inside a home or a bathroom.[35] Public spaces are locations where individuals do not possess a reasonable expectation of privacy, and from where they are generally not able to exclude others.[36] The U.S. Department of Justice ("DOJ") Bureau of Justice Assistance writes that "[p]rivacy rights of the public are a primary concern" for BWCs.[37] As BWCs are more widely deployed, "ever larger amounts of personal information (both video and audio) are being collected in increasingly diverse circumstances (both static and mobile) with the potential of being linked with yet other personal information (e.g., facial recognition, metadata)."[38] Deploying BWCs on just fifty officers could generate the equivalent of 1.6 million feature-length movies in just three months.[39] Similar widespread recording by new technology is beginning to challenge traditional legal limits of privacy in public spaces.[40]

Moreover, BWCs can also infringe on the privacy of *private* spaces. The Police Executive Research Forum ("PERF") warns that "while stationary surveillance cameras generally cover only public spaces, body-worn cameras give officers the ability to record inside private homes and to film sensitive situations that might emerge

35. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

36. *See id.*

37. BUREAU OF JUSTICE ASSISTANCE, U.S. DEP'T OF JUSTICE, BODY-WORN CAMERA TOOLKIT FREQUENTLY ASKED QUESTIONS 6 (2015), https://www.bja.gov/bwc/pdfs/bwc_faqs.pdf [https://perma.cc/4L4D-HBJ6].

38. OFFICE OF THE PRIVACY COMM'R OF CAN. ET AL., *supra* note 9, at 2.

39. *See* St. John Barned-Smith, *As Authorities Study Use of Body Cameras, Logistical Concerns Mount*, HOUS. CHRON. (Apr. 17, 2015), http://www.houstonchronicle.com/news/houston-texas/houston/article/As-authorities-study-use-of-body-cameras-6201620.php [https://perma.cc/M2RZ-JGF6].

40. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring); Carpenter v. United States, 819 F.3d 880, 886 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017) (No. 16-402).

during calls for service."[41] Advocates and the media have raised concerns about BWCs in private homes[42] and other private spaces, such as locker rooms.[43]

Another problem is whether and how to obtain consent to record, an issue closely related to the rules governing when BWCs are turned on and off. Obtaining consent before recording data is a longstanding and important privacy principle, embodied in widely accepted best practices like the Fair Information Practices.[44] If BWCs are always recording or recording by default, individuals may be unable to express their preferences about being on video before they are recorded. PERF notes that always-on recording may interfere with "routine and casual situations" that constitute community policing, or infringe on the privacy rights of victims or witnesses.[45] Consent can also be an issue for bystanders, who may not know they have been recorded by a BWC at all or may learn about the recording after the fact, when a video is made public.

Scholars and advocates have varied in how they trade off this privacy principle, the gathering of consent by those whose data is collected, with the goal of transparency. There are important reasons to release camera footage to the public to support police transparency and accountability, including to document possible police misconduct.[46] Some states have emphasized the importance of privacy by limiting the public disclosure of police BWC footage, citing privacy

41. LINDSAY MILLER & JESSICA TOLIVER, POLICE EXEC. RESEARCH FORUM, U.S. DEP'T OF JUSTICE, IMPLEMENTING A BODY-WORN CAMERA PROGRAM: RECOMMENDATIONS AND LESSONS LEARNED 11 (2014), http://www.policeforum.org/assets/docs/Free_Online_Documents/Technology/implementing%20a%20body-worn%20camera%20program.pdf [https://perma.cc/SW8H-WKTD].

42. Matthew Feeney, *Police Body Cameras Raise Privacy Issues for Cops and the Public*, CATO INST. (Feb. 12, 2015, 1:27 PM), https://www.cato.org/blog/police-body-cameras-raise-privacy-issues-cops-public [https://perma.cc/9CJF-UY5J].

43. *Cops' Body Cameras Raise Privacy Concerns*, N.Y. DAILY NEWS (Mar. 15, 2014, 6:24 PM), http://www.nydailynews.com/news/national/cops-body-cameras-raise-privacy-concerns-article-1.1722969 [https://perma.cc/9TJM-F6VA (dark archive)].

44. *See* ROBERT GELLMAN, FAIR INFORMATION PRACTICES 3 (2017), https://bobgellman.com/rg-docs/rg-FIPshistory.pdf [https://perma.cc/T8Y7-8JYM]; *see also OECD Privacy Principles*, ORG. FOR ECON. CO-OPERATION & DEV., http://oecdprivacy.org/ [https://perma.cc/C4R8-P387].

45. MILLER & TOLIVER, *supra* note 41, at 12.

46. *See* Fan, *supra* note 10, at 410; Kelly Freund, Note, *When Cameras Are Rolling: Privacy Implications of Body-Mounted Cameras on Police*, 49 COLUM. J. L. & SOC. PROBS. 91, 95 (2015).

concerns.[47] Some scholars and advocates have disagreed with this approach, emphasizing the need for transparency.[48] According to one survey, police policies governing BWC use generally agree that certain locations are linked to an expectation of privacy where cameras should not record, particularly bathrooms.[49] Professor Mary Fan writes that "[t]he widespread consensus on restrooms is not surprising given that concerns about recording officers in bathrooms were often raised by police unions."[50]

The position of the American Civil Liberties Union ("ACLU") illustrates the topic's difficulty. The ACLU's stance has evolved over time for addressing the twin goals of privacy and transparency. The ACLU originally called for recording of all encounters with the public to maximize the accountability for officers.[51] It has since modified its position, however, to account for privacy. The ACLU now accepts cameras being turned off in some instances, while supporting cameras being turned on by default and remaining active for the duration of "any other law enforcement or investigative encounter" with the public.[52] This Article does not seek to provide a general resolution to the question of how to achieve the goals of both privacy and transparency. The debate is noted here and Part III emphasizes that consideration of transparency that we believe deserves greater attention within the general IoT literature.

A third important consideration for BWCs is the cybersecurity of the data they generate. Cybersecurity, defined as "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack,"[53] is a growing concern as police departments grapple with increasing amounts of digital evidence. The International Association of Chiefs of Police warns that "[t]here is an ever-growing risk of law enforcement organizations being the target

47. THE MEDIA FREEDOM & INFO. ACCESS CLINIC, POLICE BODY CAM FOOTAGE 16–17 (2015), http://isp.yale.edu/sites/default/files/publications/police_body_camera_footage-_just_another_public_record.pdf [https://perma.cc/L9SK-GNF7].

48. *See* Fan, *supra* note 10, at 410.

49. *Id.* at 429.

50. *Id.*

51. STANLEY, *supra* note 7, at 2.

52. AM. CIVIL LIBERTIES UNION, A MODEL ACT FOR REGULATING THE USE OF WEARABLE BODY CAMERAS BY LAW ENFORCEMENT § 1(b) (2017), https://www.aclu.org/other/model-act-regulating-use-wearable-body-cameras-law-enforcement?redirect=files/field_document/aclu_police_body_cameras_model_legislation_may_2015.pdf [https://perma.cc/UHT4-WN6U].

53. *Cybersecurity*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/cybersecurity [https://perma.cc/G4UX-WELV].

of a cyber-attack."[54] Risks include exposure of confidential information, denial of service attacks, ransomware, and tampering with evidence.[55] Experts warn that the databases that house digital evidence such as BWC footage are vulnerable to attack.[56] When evidence is digitized and stored as data, it becomes vulnerable to the same types of attacks that plague other types of digital data. These vulnerabilities not only create privacy risks for the subjects of BWC footage and others but could impact the chain of custody and evidentiary value of data in the event of a hack,[57] which could imperil prosecutions. Police departments thus face the challenge, shared by other organizations that hold personal data, of how to use their available resources to respond as well as possible to the wide range of possible cyberattacks. To assist police departments in responding to these risks, Part II examines IoT best practices for cybersecurity and privacy.

C. The IoT Literature's Analysis of Similar Privacy and Cybersecurity Concerns

This Section summarizes key points from the extensive literature on how to address privacy and security concerns for the IoT. This literature has already addressed the three topics just discussed for BWCs: the challenge of ubiquitous sensors to privacy in public and private spaces, difficulties with consent, and security of digital evidence gathering tools. By demonstrating that the issues are similar, this Article indicates how some of the responses provided in that literature can apply to BWCs as well.

As with BWCs, scholars have studied how ubiquitous recording by IoT devices creates privacy issues both in public and in private. IoT devices accumulate types of data not previously collected and do so in ever greater volumes, thus revealing in unprecedented ways how people move through public spaces.[58] The extensive literature on

54. INT'L ASS'N OF CHIEFS OF POLICE, MANAGING CYBERSECURITY RISK 2 (2017), http://www.iacpcybercenter.org/wp-content/uploads/2015/04/Managing_Cybersecurity_Risk_2017.pdf [https://perma.cc/ET45-ZTAY].

55. *Id.*

56. Steven Melendez, *Police Departments Are Vulnerable to Cyberthreats As Evidence Goes Digital*, FAST COMPANY (Jan. 28, 2016), https://www.fastcompany.com/3055955/police-departments-are-vulnerable-to-cyber-threats-as-evidence-goes-digital [https://perma.cc/J6GX-L679].

57. MILLER & TOLIVER, *supra* note 41, at 44.

58. Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 816 n.71 (2016).

"smart city" technology directly applies to BWC issues. "Smart city" technologies include audio gunshot recorders and streetlights with on-board, internet-connected cameras, and this information gathering raises many of the same issues as BWCs.[59] As IoT devices enter the home, consumers lose privacy in those previously private spaces.[60] For instance, the FTC recently published a consent decree with a fine of $3.2 million against a smart TV manufacturer for deceiving consumers about its practice of tracking personal information via the TV set.[61] Risks come not only from consumer devices like smart thermometers and speakers but also from technology that is less visible to the consumer, such as smart utility meters.[62] The IoT-generated data streaming from intimate spaces combined with Big Data can reveal surprisingly sensitive and personal information.[63] When police wear a BWC into a house, the camera and microphone of the BWC become examples of IoT devices within the home.

The IoT literature has extensively analyzed how IoT may challenge the notice and consent model (requiring the entity collecting data to first provide notice and obtain consent) that for years has been a pillar of privacy law.[64] Scholars have noted that because many IoT devices—like connected pacemakers or traffic lights—lack a screen or other user interface, providing meaningful notice and consent can be a challenge.[65] In addition, when IoT devices are deployed in public spaces, individuals lack a meaningful choice to opt-out or withdraw consent from tracking because doing so would require withdrawing from the public sphere.[66] This lack of a clear consent mechanism is similar to the issues discussed above, where

59. *See, e.g.*, Jesse W. Woo, *Smart Cities Pose Privacy Risks and Other Problems, But That Doesn't Mean We Shouldn't Build Them*, 85 UMKC L. REV. 953, 955 (2017).

60. Meg Leta Jones, *Privacy Without Screens & the Internet of Other People's Things*, 51 IDAHO L. REV. 639, 641 (2015).

61. Stipulated Order for Permanent Injunction and Monetary Judgment at 8–9, Fed. Trade Comm'n v. Vizio, Inc., No. 2:17-cv-00758 (D.N.J. Feb. 14, 2017), 2017 WL 7000553, at *4.

62. *See Getting a Grip on the Grid*, HORTONWORKS, https://hortonworks.com/solutions/energy/ [https://perma.cc/4RVY-M77W].

63. EXEC. OFFICE OF THE PRESIDENT, *supra* note 25, at 5.

64. *See* GELLMAN, *supra* note 44, at 21–22 (noting that "notice and choice" does not meet fair information practices such as data quality, enforcement, and access).

65. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 140–141 (2014); Jones, *supra* note 60, at 640.

66. *See* Kelsey Finch & Omer Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 FORDHAM URB. L.J. 1581, 1582, 1596 (2014); Woo, *supra* note 59, at 965.

bystanders or other individuals who are recorded by BWCs often lack an opportunity to consent.

Just as experts are beginning to worry about the cybersecurity of BWCs and other digital evidence, experts have already developed a large and growing literature on IoT cybersecurity.[67] In a prominent example, hundreds of thousands of IoT devices were hacked and used to launch a distributed denial of service ("DDoS") attack that harmed significant parts of the internet infrastructure.[68] There have already been numerous accounts of IoT home cameras or children's toys left vulnerable to attack or spying.[69] Part of the reason IoT devices are so insecure is that they are produced by manufacturers who lack experience or expertise in computer security.[70] There are also technical challenges to strong IoT cybersecurity; for instance, devices may lack the computational power to perform complex encryption or other security measures.[71] While this security environment appears bleak, there is a growing body of expert literature on security best practices that, if implemented properly, promises to substantially reduce this risk.[72] Because IoT security issues have arisen already for a wide range of industries,[73] other IoT sectors have developed

67. *See generally* Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J. L. & TECH. 1 (2015) (discussing cybersecurity issues presented by IoT technology as it relates to "wearable" items).

68. Michael Kan, *An IoT Botnet is Partly Behind Friday's Massive DDOS Attack*, PC WORLD (Oct. 21, 2016, 4:21 PM), https://www.pcworld.com/article/3134056/hacking/an-iot-botnet-is-partly-behind-fridays-massive-ddos-attack.html [https://perma.cc/98FZ-6SNW].

69. *See, e.g.*, *Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children*, FBI (July 17, 2017) https://www.ic3.gov/media/2017/170717.aspx [https://perma.cc/7NSE-5BWV]; Samuel Gibbs, *Hackers Can Hijack Wi-Fi Barbie to Spy on Your Children*, GUARDIAN (Nov. 26, 2015, 6:16 AM), https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children [https://perma.cc/ZXT7-Y5UB]; Elisabeth Leamy, *The Danger of Giving Your Child 'Smart Toys'*, WASH. POST (Sep. 29, 2017), https://www.washingtonpost.com/lifestyle/on-parenting/giving-your-child-internet-connected-smart-toys-could-be-dumb/2017/09/29/a168218a-a241-11e7-8cfe-d5b912fabc99_story.html [https://perma.cc/PV87-MD9A].

70. Peppet, *supra* note 65, at 135.

71. *See* Chris James, *Cybersecurity Law and the Internet of Things*, SOC'Y FOR COMPUTERS & L. (June 6, 2016, 4:58 PM), https://www.scl.org/articles/3670-cybersecurity-law-and-the-internet-of-things [http://perma.cc/R89G-GKJB].

72. *See generally* BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3 (analyzing cybersecurity concerns and security practices to alleviate those concerns).

73. *From Connected Cars, Healthcare to Uranium Enrichment Facilities, 5 IoT Security Hacking Instances to Take Note of!*, EMBITEL: EMBEDDED BLOG (Sept. 22, 2017), https://www.embitel.com/blog/embedded-blog/security-challenges-faced-by-iot-based-industries [https://perma.cc/5PAD-U8B7].

experience about categories of attacks and best practices for mitigating the risks.

The foregoing discussion has demonstrated how police BWCs technologically match the definition of IoT devices—sensors connected to the storage in the cloud.[74] The two literatures—about IOT and police BWCs—have identified similar privacy and cybersecurity issues.[75] To date, however, the IoT literature has largely ignored the connection with BWCs, and vice versa.[76] Neither body of literature has explored how the lessons from each side—IoT and BWC—inform policy and best practices for the other. Part II of this Article will present lessons from IoT for BWCs. Part III presents lessons from BWCs for IoT.

II. IOT BEST PRACTICES APPLIED TO POLICE BWCS

This Part explains IoT privacy and security best practices from expert organizations in the field. BITAG,[77] the Microsoft Corporation,[78] and the FTC,[79] each a major stakeholder with an established expertise in IoT privacy and security, have offered privacy and security best practices.[80] This Section briefly analyzes the recommendations from each source and explains whether and how they apply to police BWCs. Each set of this Article's best practices is listed in their entirety to give readers a sense of the universe of recommendations in the IoT literature. This Article's hope is to identify applicable best practices for police departments and policy makers to make informed decisions, not to create the definitive guide for BWC privacy and security.

74. *See supra* Section I.A.

75. *See supra* Section I.B.

76. Adam Thierer identified BWCs as a type of IoT wearable device that raised heightened privacy concerns because of the Fourth Amendment. He did not, however, extensively discuss the implications of the two literatures for each other. Thierer, *supra* note 67, at 28–29, 115–17.

77. *See generally* BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3 (suggesting practices for avoiding cybersecurity risks with IoT devices and software).

78. *See generally* Bets & Diogenes, *supra* note 4 (discussing security strategies for IoT infrastructures).

79. *See generally* FED. TRADE COMM'N, *supra* note 5 (providing recommendations to protect consumers from security risks related to IoT).

80. *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 230–31 (2016).

A. BITAG: Internet of Things Security and Privacy Recommendations

BITAG is a group that brings "together engineers and other similar technical experts to develop consensus on broadband network management practices or other related technical issues."[81] It is composed of experts from both academia and industry.[82] Its report on IoT security and privacy is a leading expert resource, especially for security best practices.[83]

1. "IoT Devices Should Use Best Current Software Practices"[84]

a. "IoT Devices Should Ship With Reasonably Current Software"[85]

"BITAG recommends that IoT devices should ship to customers or retail outlets with reasonably current software that does not contain severe, known vulnerabilities."[86] Because IoT devices are physical objects embedded with computers, they operate using computer software.[87] BITAG recommends that this software be reasonably current because software is constantly being updated and improved.[88] Running older versions of software creates a security risk, and shipping IoT devices with outdated software places these devices in the market with already lagging security.[89]

Like other IoT devices, BWCs run on software to record video and typically to transmit those recordings to the cloud.[90] BWCs with outdated software or known vulnerabilities leave the devices susceptible to hacking.[91] Such vulnerabilities could compromise the

81. *See* BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3.

82. *Technical Participants*, BROADBAND INTERNET TECH. ADVISORY GROUP, http://bitag.org/tech_work_group.php?action=participants [https://perma.cc/3NSG-RMPN].

83. *See* Josephine Wolff, *Coalition Seeks to Protect Internet From Weaknesses of Many 'Connected' Devices*, PRINCETON U. (Nov. 22, 2016, 1:07 PM), https://www.princeton.edu/news/2016/11/22/coalition-seeks-protect-internet-weaknesses-many-connected-devices [https://perma.cc/HD3S-NE7D].

84. BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3, at 18.

85. *Id.*

86. *Id.*

87. *See supra* text accompanying note 21.

88. Deb Shinder, *The Risk of Running Obsolete Software (Part 1)*, TECHGENIX (Feb. 24, 2016), http://techgenix.com/risk-running-obsolete-software-part1/ [https://perma.cc/2WDJ-UVRG].

89. *Id.*

90. *See supra* Section I.A.

91. *See* Shinder, *supra* note 88.

BWCs themselves or, possibly worse, expose a police department's entire network.[92] Hacking and exposure of BWC footage or other evidence could also violate the privacy of victims, suspects, witnesses, or officers.[93] BWCs may be in service for long periods of time depending on the financial resources of the police department,[94] so purchasing cameras with the most current software will help ensure security over the life of the device.

b. "IoT Devices Should Have a Mechanism for Automated, Secure Software Updates"[95]

According to BITAG, IoT manufacturers should "design systems and processes to ensure the automatic update of IoT device software, without requiring or expecting any type of user action or even user opt-in."[96] No software is perfect, bugs that impact security or privacy are widespread, and attackers constantly develop new attacks.[97] This reality will continue to hold true for IoT devices that run software and are connected to the internet.[98] IoT patchability is important enough that the Department of Commerce through the National Telecommunications and Information Administration has engaged in a multi-stakeholder process to ensure IoT security upgradability and patching.[99]

BWCs run on software to digitally record and transmit video,[100] and that software will need to be patched to maintain security. This recommendation clearly applies to BWCs.

92. *Id.*

93. *See* INT'L ASS'N OF CHIEFS OF POLICE, *supra* note 54, at 2.

94. *See, e.g.*, ANNE FRANCES JOHNSON & LYNETTE I. MILLET, NAT'L ACAD. OF SCIS., ENG'G, & MED., SOFTWARE UPDATE AS A MECHANISM FOR RESILIENCE AND SECURITY: PROCEEDINGS OF A WORKSHOP 61–62 (2017), https://www.nap.edu/catalog/24833/software-update-as-a-mechanism-for-resilience-and-security-proceedings [http://perma.cc/2VAB-QY5K (staff-uploaded archive)].

95. BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3, at 18.

96. *Id.*

97. *See id.*

98. *See supra* Section I.A.

99. *Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching*, NAT'L TELECOMM. & INFO. ADMIN., U.S. DEP'T OF COM., https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security [https://perma.cc/9HGA-P8JN]; *see also* JOHNSON & MILLET, *supra* note 94, at 60–61.

100. *See supra* notes 27–30 and accompanying text; *see, e.g.*, *Solutions for Law Enforcement*, AXON, https://www.axon.com/solutions/law-enforcement [http://perma.cc/2BDZ-L5JP].

c. "IoT Devices Should Use Strong Authentication by Default"[101]

"BITAG recommends that IoT devices be secured by default (e.g. password protected) and not use common or easily guessable user names and passwords (e.g., 'admin,' 'password')."[102] Authentication is necessary to determine when an individual is permitted to use or modify an IoT device.[103] Weak authentication can allow unauthorized users to access sensitive data collected by IoT devices.[104]

As a result, strong authentication is a best practice with traditional computing as well as IoT,[105] and the practice should apply to BWCs too. It is necessary to protect the potentially sensitive data collected by BWCs and provide assurance about the integrity of data when used as evidence. Strong passwords should protect access to the camera footage stored in the cloud,[106] and possibly to the BWC as well.

d. "IoT Device Configurations Should Be Tested and Hardened"[107]

"BITAG recommends that manufacturers test the security of each device with a range of possible configurations, as opposed to simply the default configuration."[108] Testing device software for vulnerabilities is a vital means of ensuring security.[109] Like other IoT devices, BWCs and storage of camera footage should undergo thorough testing, and the results of those tests should be incorporated

101. BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3, at 19.

102. *Id.*

103. *See, e.g.*, *Securing the Internet of Things: A Proposed Framework*, CISCO, https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html#9a [https://perma.cc/KW49-UPXX].

104. *See* Danny Palmer, *Is 'Admin' Password Leaving Your IoT Device Vulnerable to Cyberattacks?*, ZDNET (Apr. 26, 2017, 3:10 PM), http://www.zdnet.com/article/is-admin-password-leaving-your-iot-device-vulnerable-to-cyberattacks/ [https://perma.cc/M5DK-SG4E].

105. *The Importance of User Authentication in Network Security*, BROOKHAVEN NAT'L LABABORATORY, https://www.bnl.gov/cybersecurity/networkaccess/strong-auth.php [https://perma.cc/WFL6-LJSU].

106. *See* CLOUD STANDARDS CUSTOMER COUNCIL, SECURITY FOR CLOUD COMPUTING TEN STEPS TO ENSURE SUCCESS 14 (2017), http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf [http://perma.cc/MZ5D-88B4].

107. BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3, at 19.

108. *Id.*

109. See CLOUD STANDARDS CUSTOMER COUNCIL, *supra* note 106, at 22–23.

back into the camera and storage system to iteratively improve security. Where police departments lack the institutional capacity to conduct such testing, they may contract for thorough testing from their vendors or third parties.[110]

2. "IoT Devices Should Follow Security & Cryptography Best Practices"[111]

BITAG recommends that IoT devices use security best practices when transmitting and storing data.[112] This recommendation includes using strong encryption, having unique credentials for every device, and disabling unnecessary devices and services.[113] The full list covers the following:

(a) Encrypt Configuration (Command & Control) Communications by Default
(b) Secure Communications to and from IoT Controllers
(c) Encrypt Local Storage of Sensitive Data
(d) Authenticate Communications, Software Changes, and Requests for Data
(e) Use Unique Credentials for Each Device
(f) Use Credentials That Can Be Updated
(g) Close Unnecessary Ports and Disable Unnecessary Services
(h) Use Libraries That Are Actively Maintained and Supported[114]

These best practices are tailored to IoT devices that collect and transmit sensitive data. Given the potentially sensitive nature of BWC footage (it may include violent crimes or video of individual homes),[115] they should apply to police BWCs as well. Camera footage and other sensitive information should be encrypted, which basically means that footage is electronically locked away.[116] Police

110. *See, e.g.*, *Security of the Axon Network*, AXON, https://www.axon.com/trust/security [https://perma.cc/3DZ5-GXNS].

111. BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3, at 19.

112. *Id.* at 20.

113. *Id.* at 20–21.

114. *Id.*

115. *See supra* notes 41–43 and accompanying text.

116. David Nield, *Why You Should Be Encrypting Your Devices and How to Easily Do It*, GIZMODO: FIELD GUIDE (Sept. 4, 2017, 9:00 AM), https://fieldguide.gizmodo.com/why-you-should-be-encrypting-your-devices-and-how-to-ea-1798698901 [http://perma.cc/YXH4-BDJS].

departments should consult with security experts and demand best practices from their vendors.

3. "IoT Devices Should Be Restrictive Rather Than Permissive in Communicating"[117]

"BITAG recommends [w]hen possible, devices should not be reachable via inbound connections by default."[118] This recommendation is designed to limit the number of potential vulnerabilities or means of attack (what the security community calls the "attack surface").[119] Creating additional, unnecessary points of entry creates more opportunities for attackers to hack into devices.[120]

Similarly, BWCs should only communicate with other devices when necessary. For example, BWCs will need to connect to the cloud directly or via the officer's squad car.[121] They may not need to connect to public Wi-Fi networks or Bluetooth devices that could open the devices up to attack, so such connections should exist only if clearly justified in a particular setting.[122]

4. "IoT Devices Should Continue to Function if Internet Connectivity is Disrupted"[123]

"BITAG recommends that an IoT device should be able to perform its primary function or functions (for example, a light switch or a thermostat should continue to function with manual controls), even if it is not connected to the Internet."[124] BITAG is concerned that connectivity outages will unnecessarily render devices useless.[125] Devices may lose connectivity for a variety of reasons such as "accidental misconfiguration or intentional attack (e.g. denial of service attack)."[126] Internet connectivity may add functions to light switches or thermostats, but the loss of connectivity should not

117. BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3, at 21.

118. *Id.*

119. *Id.*; Lily Hay Newman, *Hacker Lexicon: What is an Attack Surface?*, WIRED (Mar. 12, 2017, 8:00 AM), https://www.wired.com/2017/03/hacker-lexicon-attack-surface/ [http://perma.cc/57DX-NVVS].

120. Newman, *supra* note 119.

121. *See Axon Body 2*, AXON, https://www.axon.com/products/body-2 [https://perma.cc/P7MY-M4ST]; *supra* notes 29–30 and accompanying text.

122. *See Axon Body 2*, *supra* note 121.

123. BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3, at 21.

124. *Id.*

125. *See id.*

126. *Id.*

disable these devices entirely; they should just revert to being normal light switches or thermostats.[127]

This recommendation applies to BWCs, which should continue to function even when internet connectivity is lost. Police officers enter a wide variety of locations in the course of their work, including underground rooms and other places that may not receive a wireless signal. By continuing to function even in such places, BWCs can continue to serve the policy goals of transparency and accountability during temporary internet outages.[128] Footage may be recorded and uploaded at a later time, as with older generation cameras. In short, a BWC should still function as a regular camera even without internet connectivity.

5. "IoT Devices Should Continue to Function if the Cloud Back-End Fails"[129]

This recommendation is similar to the previous one. It recommends that if the cloud back-end (the computer server that stores and processes data from the IoT device)[130] fails, the device should continue to operate, even if its functionality is partially reduced as a result.[131] As with the previous recommendation, this should also apply to BWCs.

6. "IoT Devices Should Support Addressing and Naming Best Practices"[132]

BITAG recommends that IoT devices use the latest protocols—the "languages" by which devices communicate with one another[133]—to ensure that devices are secure and functional for as long as

127. *But see* Nick Bilton, *Nest Thermostat Glitch Leaves Users in the Cold*, N.Y. TIMES (Jan. 13, 2016), https://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html [https://perma.cc/QUK6-YK7X (dark archive)].

128. *See USSD Platform & Gateway – USSD+*, MYRIAD CONNECT, http://connect.myriadgroup.com/products/ussd/ [https://perma.cc/K3AV-JAM5] (detailing a software program allowing secure transfers of communications by mobile devices without internet connection).

129. BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3, at 22.

130. *Back-end and API Development*, LEMBERG SOLUTIONS, https://lemberg.co.uk/services/back-end-and-api-development [https://perma.cc/F5Z4-U8EB].

131. BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3, at 22.

132. *Id*.

133. Bradley Mitchell, *Network Protocols*, LIFEWIRE (Nov. 2, 2017), https://www.lifewire.com/definition-of-protocol-network-817949 [https://perma.cc/78G7-5ARG].

possible.[134] Specifically, BITAG refers to the internet protocol version 6 and the Domain Name System Security Extension.[135]

Like other IoT devices, BWCs will communicate with a cloud server and possibly other devices.[136] They should do so with up-to-date protocols to ensure security for as long as possible.

7. "IoT Devices Should Ship with a Privacy Policy That is Easy to Find & Understand"[137]

"BITAG recommends that IoT devices ship with a privacy policy, but that policy must be easy for a typical user to find and understand."[138] Although the privacy of the BWC user (the officer) is important, a major public policy concern for this Article is the privacy of the *subjects* of the camera, the general public.[139] Having a publicly available, plain language privacy policy on a website, physical signs, or mailers enables concerned citizens to remain informed and engaged with BWC privacy issues.[140]

8. "Disclose Rights to Remotely Decrease IoT Device Functionality"[141]

"BITAG recommends that if the functionality of an IoT device can be remotely decreased by a third party, such as by the manufacturer or IoT service provider, this possibility should be made clear to the user at the time of purchase."[142] This recommendation is aimed at consumer devices, where the concern is that companies will remotely decrease device functionality and deprive consumers of the service they paid for.[143] It may not be relevant to BWC privacy or cybersecurity because police officers are not the same kinds of consumers of commercial products—for one thing the individual officers do not pay for the device.[144] However, police departments

134. BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3, at 22.
135. *Id.*
136. *See supra* Section I.A.
137. BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3, at 22.
138. *Id.*
139. *See supra* Section I.B.
140. *See* FED. TRADE COMM'N, *supra* note 5, at 26–27, 39 n.159.
141. BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3, at 22.
142. *Id.*
143. *Cf.* Jason Perlow, *All Your IoT Devices Are Doomed*, ZDNET (July 12, 2016), http://www.zdnet.com/article/all-your-iot-devices-are-doomed/ [https://perma.cc/W685-4UBX].
144. *See* Press Release, U.S. Dep't of Justice, Department of Justice Awards Over $20 Million to Law Enforcement Body-Worn Camera Programs (Sept. 26, 2016), https://www.justice.gov/opa/pr/department-justice-awards-over-20-million-law-enforcement-

may wish to inquire of their vendors about the ability of third parties to remotely decrease BWC functionality. Some police departments have expressed frustration with how third-party vendors handle their data analytics functions for investigative and other purposes,[145] so departments may want to prevent similar frustration in the BWC context.

9. "The IoT Device Industry Should Consider an Industry Cybersecurity Program"[146]

BITAG recommends "an industry-backed program under which some kind of 'Secure IoT Device' logo or notation could be carried on IoT retail packaging."[147] As this Article is concerned with BWCs sold to police departments and not the general public, the usefulness of a mark or certification on retail packaging is not similarly applicable. It may be useful, however, for police departments to participate in an industry-wide set of best practices for BWCs as a check against possible business, privacy, and cybersecurity problems arising from relations with vendors. Developing an industry-wide set of best practices, for police departments to check their vendors' practices against, would still be useful. Hopefully, such an organization would help raise the bar for privacy and security across the BWC manufacturing industry. Organizations including PERF or the U.S. DOJ might encourage or promulgate such best practices and distribute them through existing networks.

10. "The IoT Supply Chain Should Play Their Part in Addressing IoT Security and Privacy Issues"[148]

BITAG notes that "[e]nd users of IoT devices depend upon the IoT supply chain to protect their security and privacy, and some or all parts of that IoT supply chain play a critical role throughout the entire lifecycle of the product."[149] The supply chain is important

body-worn-camera-programs [https://perma.cc/N7SN-6GMR]. *But see* Dan Sewell, *Cops Buying Body Cameras on Their Own*, POLICEONE (Apr. 23, 2015), https://www.policeone.com/police-products/body-cameras/articles/8531889-Cops-buying-body-cameras-on-their-own/ [https://perma.cc/E6HP-GBNQ].

145. Mark Harris, *How Peter Thiel's Secretive Data Company Pushed Into Policing*, WIRED (Aug. 9, 2017, 9:40 AM), https://www.wired.com/story/how-peter-thiels-secretive-data-company-pushed-into-policing/ [https://perma.cc/ER6U-MM2N].

146. BROADBAND INTERNET TECH. ADVISORY GRP., supra note 3, at 23**.**

147. *Id.*

148. *Id.*

149. *Id.*

because if it is vulnerable, malware may be introduced on the factory floor, or during shipping, or on the retail shelf.[150] Similarly, BWC manufacturers will play a large role in how their cameras ensure security and privacy. This is especially true if the device manufacturer also provides data processing and cloud management services to the police department.[151] Those manufacturers will have a great deal of control over both the device as it moves through the supply chain and the data once the camera is in the field.[152] BITAG recommends the following practices for the supply chain:

> (a) "a privacy policy that is clear and understandable;"
> (b) a reset mechanism to clear all configurations and delete or reset data;
> (c) "a bug reporting system;"
> (d) a "secure software supply chain;"
> (e) support for devices for their entire lifespan;
> (f) a method for consumers to contact the manufacturer as well as for manufacturers to inform consumers of vulnerabilities;
> (g) disclosure and remediation of software vulnerabilities; and
> (h) "a vulnerability reporting process" that is easy to find and use.[153]

Having a reset mechanism to easily delete data may not be advisable for police BWCs, due to legal reasons to preserve video footage for evidentiary or transparency purposes.[154] However, the other recommendations are apt. BWC manufacturers should maintain bug reporting systems and other methods to take feedback from users on bugs and security vulnerabilities. They should secure their supply chain to ensure that malware is not inserted into devices in the manufacturing process. Further, they should support BWCs with security patches and updates for the entire life of the camera.

150. *See* Tobias Naegele, *IOT Security Risks Begin with Supply Chains*, GOVTECHWORKS (July 12, 2017), https://www.govtechworks.com/iot-security-risks-begin-with-supply-chains/#gs.dnQYaBo [https://perma.cc/AP5A-2DQ5].

151. *See Choose the Network, Not the Camera*, AXON (Dec. 6, 2016), https://www.axon.com/company/news/choose-the-network-not-a-camera [https://perma.cc/GCK7-UD2U].

152. *See id.*

153. BROADBAND INTERNET TECH. ADVISORY GRP., *supra* note 3, at 23–24.

154. *See, e.g.*, Richard Lin, *Police Body Worn Cameras and Privacy: Retaining Public Benefits While Reducing Public Concerns*, 14 DUKE L. & TECH. J. 347, 363 (2016).

In summary, BITAG has created best practices based on expert experience with the privacy and cybersecurity threats that exist in connection with broadband services.[155] These broadband internet services exist for BWCs as well—sensors connected to the cloud through the high-bandwidth transmissions required for video footage.[156] The BITAG recommendations thus provide a useful checklist for issues that may arise for management of BWCs.

B. Microsoft: "Internet of Things [S]ecurity [B]est [P]ractices"[157]

As a leading technology company that has invested heavily in security and privacy over time,[158] Microsoft possesses a great deal of expertise on emerging technologies like IoT. This Article chooses to highlight this set of recommendations because of its focus on physical as well as digital security. Physical security is an important aspect of cybersecurity, as physical access may enable an attack to gain access to systems that would otherwise be difficult to crack.[159]

Microsoft classifies its recommendations based on the four IoT stakeholders.[160] The "hardware manufacturer[s]/integrator[s]" are those who build or assemble the physical devices.[161] The "solution developers" design the device functionality; they build the software.[162] The "solution deployer" installs the devices and connects them to each other and/or to the cloud.[163] Finally, the "solution operator" actually operates the devices in the long term.[164] For BWCs, the manufacturer and developer will likely be the vendor who supplies the cameras.[165] The deployer may be a third-party vendor, or that function may occur within the department. The operators will be the police department, possibly in cooperation with a third-party vendor. The issues identified in the Microsoft best practices expand on the

155. Wolff, *supra* note 83.

156. *See supra* Section I.A.

157. Bets & Diogenes, *supra* note 4.

158. John Viega, *Ten Years of Trustworthy Computing: Lessons Learned*, IEEE SECURITY & PRIVACY, Sept.–Oct. 2011, at 3, 3–4, https://www.computer.org/csdl/mags/sp/2011/05/msp2011050003.pdf [https://perma.cc/5LWX-FFKD].

159. Paul McCormack, *Why Physical Security Matters for Your Cybersecurity Efforts*, BOOST, ADP (Oct. 13, 2017), https://www.adp.com/boost/articles/why-physical-security-matters-for-your-cybersecurity-efforts-13-1745 [https://perma.cc/9U9F-6WHP].

160. Bets & Diogenes, *supra* note 4.

161. *Id.*

162. *Id.*

163. *Id.*

164. *Id.*

165. Wolff, *supra* note 83.

BITAG recommendations, such as those concerning the IoT supply chain.

1. "IoT hardware manufacturer/integrator"[166]

a. "Scope hardware to minimum requirements"[167]

According to Microsoft, IoT "hardware design should include the minimum features required for operation of the hardware, and nothing more. An example is to include USB ports only if necessary for the operation of the device. These additional features open the device for unwanted attack vectors that should be avoided."[168]

Manufacturers should design BWCs to reduce vulnerabilities and attack vectors such as unnecessary USB ports.[169] The purpose of the camera is to capture video footage; creating additional methods to access the device creates more ways to introduce malicious software or otherwise tamper with the BWC.[170]

b. "Make hardware tamper proof"[171]

Microsoft recommends that IoT manufacturers "[b]uild in mechanisms to detect physical tampering, such as opening of the device cover or removing a part of the device. These tamper signals may be part of the data stream uploaded to the cloud, which could alert operators of these events."[172]

The need for tamper-proof IoT hardware is as great in the BWC context as it is with regular IoT devices.[173] BWCs implicate not only the integrity of personal data but potentially criminal evidence as well.[174] Manufacturers should design hardware to resist tampering by officers and third parties.

166. Bets & Diogenes, *supra* note 4.
167. *Id.*
168. *Id.*
169. *See* Andy Greenberg, *Why the Security of USB Is Fundamentally Broken*, WIRED (July 31, 2014, 3:00 AM), https://www.wired.com/2014/07/usb-security/ [https://perma.cc/G7LD-693G].
170. *See id.*
171. *Id.*
172. *Id.*
173. Ben Dickson, *Why IoT Security Is So Critical*, TECHCRUNCH (Oct. 24, 2015), https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/ [https://perma.cc/H7WM-E6K8].
174. *See supra* Section I.B.

c. "Build around secure hardware"[175]

Similar to BITAG,[176] Microsoft recommends using encryption to secure data storage and IoT devices themselves.[177] This recommendation applies to BWCs.

d. "Make upgrades secure"[178]

Not only do IoT devices need regular patching to remain secure, but the process for patching itself must not be compromised.[179] For example, the NotPetya attack that hit Ukraine in 2017 infiltrated systems through an unsecured software update.[180] Police departments should consult security experts and require their vendors to use secured update systems.

2. "IoT solution developer"[181]

a. "Follow secure software development methodology"[182]

This recommendation is similar to the BITAG recommendation to use software best practices.[183] As stated above, it should apply to police BWCs.

b. "Choose open-source software with care"[184]

Microsoft recommends that "[w]hen choosing open-source software, consider the activity level of the community for each open-source component."[185] Open-source software, where the source code is publicly available, is community-driven by nature, so more active communities are more likely to find and update software

175. Bets & Diogenes, *supra* note 4.
176. *See supra* text accompanying note 116.
177. Bets & Diogenes, *supra* note 4.
178. *Id.*
179. *See* Roger A. Grimes, *Why Patching Is Still a Problem—And How to Fix It*, CSO (Jan. 26, 2016, 3:00 AM), https://www.csoonline.com/article/3025807/data-protection/why-patching-is-still-a-problem-and-how-to-fix-it.html [https://perma.cc/4L5R-RVMB].
180. Andy Greenberg, *The Petya Plague Exposes the Threat of Evil Software Updates*, WIRED (July 7, 2017, 10:00 AM), https://www.wired.com/story/petya-plague-automatic-software-updates/ [https://perma.cc/VRW4-6R9U].
181. Bets & Diogenes, *supra* note 4.
182. *Id.*
183. *See supra* Section II.A.1.
184. Bets & Diogenes, *supra* note 4.
185. *Id.*

vulnerabilities.[186] This recommendation illustrates how the best practices from sources including Microsoft can provide questions that police departments can pose to vendors during the BWC procurement process.

c. "Integrate with care"[187]

Microsoft suggests that software developers integrate different capabilities into their IoT devices carefully.[188] Creating additional functionality introduces greater complexity, which creates more opportunities for a vulnerability.[189] The benefits of new features should be weighed against the increased attack surface.[190] This recommendation applies to police BWCs and related software vendors.

3. "IoT solution deployer"[191]

a. "Deploy hardware securely"[192]

"IoT deployments may require hardware to be deployed in unsecure locations, such as in public spaces or unsupervised locales. In such situations, ensure that hardware deployment is tamper-proof to the maximum extent. If USB or other ports are available on the hardware, ensure that they are covered securely."[193]

Police BWCs will, by their very nature, be deployed in public.[194] It is important that they be deployed securely.[195] For example,

186. *See* Maria Korolov, *Open Source Software Security Challenges Persist, but the Risk Can Be Managed*, CSO (Jan. 10, 2018, 3:24 AM), https://www.csoonline.com/article/3157377/application-development/report-attacks-based-on-open-source-vulnerabilities-will-rise-20-percent-this-year.html [https://perma.cc/A9YQ-W7EE].

187. Bets & Diogenes, *supra* note 4.

188. *Id.*

189. *See, e.g.*, Jane Chong, *Why Is Our Cybersecurity So Insecure?*, NEW REPUBLIC (Oct. 11, 2013), https://newrepublic.com/article/115145/us-cybersecurity-why-software-so-insecure [https://perma.cc/MC8L-D8GJ].

190. *See* Newman, *supra* note 119.

191. Bets & Diogenes, *supra* note 4.

192. *Id.*

193. *Id.*

194. *See* NAT'L INST. OF JUSTICE, A PRIMER ON BODY WORN CAMERA TECHNOLOGIES 6 (2012), https://www.ncjrs.gov/pdffiles1/nij/grants/250382.pdf [https://perma.cc/D9D5-TN8R].

195. *See* Padraig Scully, *Understanding IoT Security – Part 1 of 3: IoT Security Architecture on the Device and Communication Layers*, IOT ANALYTICS (Nov. 29, 2016), https://iot-analytics.com/understanding-iot-security-part-1-iot-security-architecture/ [http://perma.cc/26KG-CGHE].

cameras should not be left unattended in the open where they may be tampered with.[196]

b. "Keep authentication keys safe"[197]

"During deployment, each device requires device IDs and associated authentication keys generated by the cloud service. Keep these keys physically safe even after the deployment. Any compromised key can be used by a malicious device to masquerade as an existing device."[198]

Police departments must maintain and keep track of BWCs like any other hardware. If the cameras have unique device IDs and authentication keys (as recommended), then those keys should be physically secured and secluded.[199] Most people know intuitively not to leave their physical keys out in the open—the same logic applies to digital keys.[200] As police departments move toward uploading BWC footage in real time, it becomes even more important to trust the identification and authentication of individual BWCs.

4. "IoT solution operator"[201]

a. "Keep the system up to date"[202]

Although automatic updates are a best practice in IoT, as noted above by BITAG,[203] if updates do not come automatically the device user will need to ensure software is up to date.[204]

With BWCs, each device must be patched and updated.[205] Police departments must develop a system to do so, and decide whether responsibility for patching devices falls on the individual officer or a centralized information technology ("IT") or quartermaster service.

196. *Cybersecurity and IoT: Where Do We Go From Here?*, SIA PARTNERS (Oct. 18, 2017), http://en.finance.sia-partners.com/20171018/cybersecurity-and-iot-where-do-we-go-here [https://perma.cc/FAS9-FYPP].

197. *Id.*

198. *Id.*

199. *See id.*

200. *See Physical Measures to Amp Up Your Digital Security*, WIRED (Dec. 9, 2017), https://www.wired.com/story/physical-security-measures/ [https://perma.cc/XS5Q-TNVK].

201. Bets & Diogenes, *supra* note 4.

202. *Id.*

203. *See supra* text accompanying notes 95–96.

204. *Cf. Updating Device Firmware*, AXON, https://help.axon.com/hc/en-us/articles/226850208-Updating-device-firmware [https://perma.cc/AX6R-UNGA].

205. *See supra* text accompanying note 100.

b. "Protect against malicious activity"[206]

Microsoft recommends that, where possible, IoT devices should run the latest software, including antivirus software.[207]

Whether BWCs are able to run antivirus software will depend on design choices by the manufacturer.[208] There is currently active research on how to secure IoT devices with antivirus measures,[209] which may or may not apply to BWCs. In any case, this recommendation illustrates the importance of updated and secure software, including for other parts of the IoT infrastructure that connect to BWCs such as the cloud servers.[210]

c. "Audit frequently"[211]

Microsoft says that frequent audits are "key when responding to security incidents. Most operating systems provide built-in event logging that should be reviewed frequently to make sure no security breach has occurred. Audit information can be sent as a separate telemetry stream to the cloud service where it can be analyzed."[212] BWC manufacturers and police departments should explore similar capabilities for automatic auditing in their devices.[213]

d. "Physically protect the IoT infrastructure"[214]

In the IOT context, "[t]he worst security attacks . . . are launched using physical access to devices."[215] Therefore, an "important safety practice is to protect against malicious use of USB ports and other

206. Bets & Diogenes, *supra* note 4.

207. *Id.*

208. *Cf.* Liam Tung, *Samsung: Here's How We're Securing Your Smart TV*, ZDNET (May 17, 2017, 10:44 AM), http://www.zdnet.com/article/samsung-heres-how-were-securing-your-smart-tv/ [https://perma.cc/CZH9-JXJ6].

209. *See, e.g.*, Dawn Lim, *Startup Offers to Protect Printers, Phones, and Other Devices from Hackers*, MIT TECH. REV. (Feb. 21, 2013), https://www.technologyreview.com/s/511331/startup-offers-to-protect-printers-phones-and-other-devices-from-hackers/ [https://perma.cc/3W7E-ZUSB].

210. *E.g.*, Mike Borza, *Hardware Roots of Trust for IoT Security*, TECH DESIGN F. (July 29, 2016), http://www.techdesignforums.com/practice/technique/hardware-roots-of-trust-for-iot-security/ [https://perma.cc/QXR3-S3QL].

211. Bets & Diogenes, *supra* note 4.

212. *Id.*

213. *See, e.g.*, *Change Auditor*, QUEST, https://www.quest.com/change-auditor/ [https://perma.cc/727N-WXRH].

214. Bets & Diogenes, *supra* note 4.

215. *Id.*

physical access. One key to uncovering breaches that might have occurred is logging of physical access, such as USB port use."[216]

In the BWC context, the IoT infrastructure includes the device, the cloud servers, and any intermediate transmitting devices such as the officer's squad car.[217] Each aspect of the infrastructure must be physically as well as digitally protected.[218] All the security in the world for the camera itself becomes meaningless if an attacker can simply walk into the server room where footage is stored and tamper with the footage.

e. "Protect cloud credentials"[219]

According to Microsoft, the passwords used to log in, configure, and operate the IoT cloud "are possibly the easiest way to gain access and compromise an IoT system."[220] The company recommends users "change[] the password frequently, and refrain from using these credentials on public machines."[221] Password management is a basic part of cybersecurity[222] and remains important for BWCs.

In summary, the Microsoft and BITAG sets of best practices are generally consistent, but each contains a number of specific recommendations not listed by the other. Taken together, they provide a thorough set of recommendations for police departments to consider when deploying BWCs.

C. The Federal Trade Commission

The FTC is the leading U.S. regulator for consumer privacy across sectors.[223] It is a leading proponent of privacy best practices generally and IoT privacy best practices more specifically.[224] This Section will discuss the FTC report *Internet of Things: Privacy &*

216. *Id.*

217. *See supra* Section I.A.

218. *See* Julian Lovelock, *Aligning Physical and Digital Security in the Cloud*, SOURCE SECURITY, https://www.sourcesecurity.com/insights/aligning-physical-digital-security-today-increasingly-connected-world-co-823-ga.22604.html [https://perma.cc/ML6U-Y2UX].

219. *Id.*

220. *Id.*

221. *Id.*

222. *See* Kenneth Olmstead & Aaron Smith, *Password Management and Mobile Security*, PEW RES. CTR. (Jan. 26, 2017), http://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security/ [http://perma.cc/A3WF-TLYX].

223. *See* HOOFNAGLE, *supra* note 80, at 73–81.

224. GEORGE CORSER ET AL., INTERNET OF THINGS (IOT) SECURITY BEST PRACTICES 2 (2017), https://internetinitiative.ieee.org/images/files/resources/white_papers/internet_of_things_feb2017.pdf [https://perma.cc/LT8M-X8R9].

Cybersecurity in a Connected World[225] to identify recommendations based on the FTC's IoT expertise. It will also discuss some of the more general FTC Privacy by Design recommendations that could apply to IoT and BWCs. Broadly, the FTC recommends "data security," "data minimization," "notice and choice," and "privacy by design."[226] The FTC has highlighted the role of administrative controls, in addition to the technical and physical measures stressed by BITAG and Microsoft.

1. Data Security

Like other leading organizations, the FTC stresses the importance of cybersecurity to protect the data generated by IoT devices.[227] The report makes recommendations that are similar to BITAG and Microsoft, such as access controls and patching.[228] It emphasizes "security by design," where developers build "security into their devices at the outset, rather than as an afterthought,"[229] and "defense-in-depth," where "security measures are considered at several levels" such as using a combination of network passwords and encryption.[230] All of the FTC's security recommendations apply to BWCs, but the recommendation to "retain service providers that are capable of maintaining reasonable security"[231] is particularly applicable. Local police departments may lack deep cybersecurity expertise, but they should demand good security from their vendors. IoT's reliance on the cloud can help in this regard, as cloud servers can allow for secure storage at scale by organizations with cybersecurity expertise.[232]

The full list of FTC IoT cybersecurity recommendations is largely similar to the BITAG and Microsoft recommendations above:

(a) Security by Design[233];

225. FED. TRADE COMM'N, *supra* note 5.
226. *See id.* at 27–35, 39–46.
227. *Id*. at 27–32.
228. *Id.* at 28–30.
229. *Id.* at 28–30.
230. *Id.* at 30.
231. *Id.*
232. *See, e.g.*, *Device Security*, GOOGLE CLOUD PLATFORM, https://cloud.google.com/iot/docs/concepts/device-security [http://perma.cc/SM27-97M9] (providing an example of storage offerings from a well-known cloud service provider). On the other hand, a possible downside of cloud storage is that it may concentrate large pools of data in one place, creating a more attractive target. *See also* FED. TRADE COMM'N, *supra* note 5, at 33.
233. FED. TRADE COMM'N, *supra* note 5, at 28.

(b) Ensure personnel practices promote good security[234];
(c) Retain service providers that are capable of maintaining reasonable security[235];
(d) Defense-in-depth[236];
(e) Reasonable access controls[237]; and
(f) Monitor and patch throughout the product's life cycle.[238]

2. "Data Minimization"[239]

The FTC recommends companies apply a principle of data minimization by developing "policies and practices that impose reasonable limits on the collection and retention of consumer data."[240] Data minimization means limiting the collection and retention of data to only what is necessary to accomplish a particular task, rather than operating under a default that more data is always better.[241] Data minimization has been an important privacy principle for over thirty years and has been promoted by entities like the Organization for Economic Cooperation and Development ("OECD") and the Obama White House.[242] The FTC says that minimization helps protects against two distinct privacy harms: (1) it creates smaller data sets, which present a less attractive target for hackers and expose less information in the event of a breach; and (2) it reduces the risk that data will be used in a way that violates the data subject's reasonable expectations.[243] The FTC makes more detailed recommendations on how to implement minimization in IoT, which this Article examines below.

234. *Id.* at 29.
235. *Id.* at 30.
236. *Id.*
237. *Id.* at 31.
238. *Id.*
239. *Id.* at 33.
240. *Id.*at 34.
241. *See* Bernard Marr, *Why Data Minimization Is An Important Concept In The Age of Big Data*, FORBES (Mar. 16, 2016, 3:24 AM), https://www.forbes.com/sites/bernardmarr/2016/03/16/why-data-minimization-is-an-important-concept-in-the-age-of-big-data/#11dc6dc11da4 [http://perma.cc/86YH-5FW9].
242. FED. TRADE COMM'N, *supra* note 5, at 34.
243. *Id.*at 34–35

a. "Impose reasonable limits on the collection and retention of consumer data"[244]

The FTC states that "the data minimization principle remains relevant and important to the IoT."[245] Its report notes that "if a company collects and retains large amounts of data, there is an increased risk that the data will be used in a way that departs from consumers' reasonable expectations," which would harm user privacy.[246] It cites a hypothetical example of a wearable patch to assess a user's skin condition; the device manufacturer does not need to collect precise geolocation data to perform its main function, but it may want to do so in the future to enable a new feature.[247] The report suggests the manufacturer wait to collect location data until it decides to launch the new feature and consider using less information (zip code instead of precise location).[248]

This recommendation applies to BWCs. As discussed below, in many cases BWC policies already impose limits on recording, such as prohibitions on recording in bathrooms or locker rooms to protect officer privacy.[249] Setting shorter retention periods on camera footage also achieves data minimization, where the specific footage is no longer needed for the original law enforcement purposes.[250] Other minimization opportunities may exist in particular police systems as well.

b. "[T]ake reasonable steps to de-identify the data"[251]

The FTC suggests that when companies decide to retain data, "they should also consider whether they can do so while maintaining data in de-identified form."[252] "De-identified" data is data which has been stripped of personally identifiable information or data fields that

244. *Id.* at 34.
245. *Id.* at 33.
246. *Id.* at 35.
247. *Id.* at 36–37.
248. *Id* at 36.
249. *See supra* text accompanying notes 42–43; *see also* CHARLOTTE-MECKLENBURG POLICE DEP'T, CMPD DIRECTIVES § 400-006 (2015), https://www.bwcscorecard.org/static/policies/2016-06-08%20Charlotte-Mecklenburg%20-%20BWC%20Policy.pdf [http://perma.cc/5XDZ-BWZR].
250. *See, e.g.*, CHARLOTTE-MECKLENBURG POLICE DEP'T, *supra* note 249, at § 400-006.
251. FED. TRADE COMM'N, *supra* note 5, at 38.
252. *Id.* at 37.

link to an individual.[253] The FTC gives the example of a smartphone health-tracking application that collects consumer information like geolocation.[254] Such an application could "maintain and post information in anonymous and aggregate form, which can benefit public health authorities and the public, while at the same time maintaining consumer privacy."[255] The FTC warns, however, that companies must take care that data is not re-identified and may wish to take various measures to reduce that risk, such as by employing a de-identification expert similar to procedures under the Health Insurance Portability and Accountability Act ("HIPAA").[256] De-identification also means "keeping up with technological developments" that may threaten the privacy de-identified data down the line.[257]

This recommendation may apply to BWCs in some contexts. Video footage held for evidentiary purposes will naturally require identifying information to be useful. However, video that departments release to the public for other purposes, such as in response to Freedom of Information Act ("FOIA") requests, may warrant de-identification.[258] In some cases, departments blur the faces of bystanders in videos, which is a form of de-identification.[259] In those instances, de-identification or redaction may serve the dual purpose of transparency and privacy better than either displaying the un-blurred faces or simply withholding footage.

253. *Cf. Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP'T HEALTH & HUMAN SERVICES, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html [https://perma.cc/3FMW-Z856] (providing methods of de-identification to meet the requirements of the HIPAA Privacy Rule).

254. FED. TRADE COMM'N, *supra* note 5, at 37.

255. *Id.*

256. *Id.*

257. *Id.* at 38.

258. Michael Lickstein, *Police Body Cameras and Public Records Requests: Another Privacy Frontier*, COLUM. SCI. & TECH. L. REV. (Mar. 30, 2016), http://stlr.org/2016/03/30/police-body-cameras-and-public-records-requests-another-privacy-frontier/ [http://perma.cc/R77U-6UTX].

259. *See* Alex Pasternack, *Police Body Cameras Will Do More Than Just Record You*, FAST COMPANY (Mar. 3, 2017), https://www.fastcompany.com/3061935/police-body-cameras-livestreaming-face-recognition-and-ai [http://perma.cc/KD4X-VZ5Z].

c. Make a public commitment "not to re-identify" data[260]

The FTC calls on companies to "publicly commit not to re-identify . . . data."[261] A public promise by a private company allows the FTC to enforce that promise, because if the company does otherwise it is an unlawful "deceptive act," in commerce.[262] Police departments are outside of the scope of FTC enforcement, which applies to commercial actors.[263] By contrast, the FTC may be able to enforce such promises by third-party commercial vendors of BWCs and the associated cloud services. In addition, public promises not to re-identify BWC footage may help build public trust in this technology. This recommendation may therefore still be applicable in the BWC context.

d. Have enforceable contracts with third parties not to re-identify[264]

The FTC recommends companies "have enforceable contracts in place with any third parties with whom they share the data, requiring the third parties to commit not to re-identify the data."[265] Because digital data is easily copied or transferred, privacy protections must extend to third parties that handle that data in order to be meaningful. If a company de-identifies their data sets but then hands the data to a company that immediately re-identifies individuals, that protection was ineffective. This recommendation applies to BWCs to the extent police departments de-identify their footage. Many police departments rely on third parties such as Axon (formerly Taser) to process and store their BWC footage. Thus, police departments can

260. FED. TRADE COMM'N, *supra* note 5, at 38.

261. *Id.*

262. 15 U.S.C. § 45 (a)(1) (2012) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby deemed unlawful."); *see* Stephanie L. Kroeze, *The FTC Won't Let Me Be: The Need for a Private Right of Action Under Section 5 of the FTC Act*, 50 VAL. U. L. REV. 227, 234–36 (2015) ("Any person who violates one the FTC's trade regulation rules with actual knowledge, or knowledge that can be implied based on objective circumstances, is liable for civil penalties . . . provided the act is unfair or deceptive . . . . [A] deceptive act occurs where a representation, omission, or practice misleads the consumer, the consumer interprets the characteristic in a reasonable manner, and the misleading characteristic is material.").

263. Federal law empowers the FTC to regulate "persons, partnerships, or corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(2).

264. FED. TRADE COMM'N, *supra* note 5, at 38.

265. *Id.*

require such vendors not to re-identify through contract, backed by FTC, state attorney general, or other enforcement against the vendor for violation.[266]

3. Notice and Choice

While noting the difficulties of providing notice and choice in IoT, the FTC report says "that providing notice and choice remains important, as potential privacy and security risks may be heightened due to the pervasiveness of data collection inherent in the IoT."[267] The FTC incorporates a "use-based" model into its approach to providing notice and choice to consumers.[268] This means that notice is not required when a company collects and uses consumer data in a way that is "consistent with the context of a transaction or the company's relationship with the consumer."[269] On the other hand, data uses that are inconsistent with the consumer's reasonable expectations should require notice and choice.[270]

The FTC uses the example of a smart oven to illustrate its point.[271] The oven might be paired with a smartphone app that allows the user to remotely control temperature and baking time. In that case, using the consumer's oven-usage data to improve the device's performance would not require consumer choice because consumers would reasonably expect such usage.[272] However, sharing that data with a data broker or advertiser "would be inconsistent with the context of the consumer's relationship with the manufacturer," so the company should provide notice and choice.[273]

This "use-based" approach may or may not be applicable to BWCs. It is likely that if video footage is recorded in one context (say

266. The FTC may bring enforcement actions against companies that break publicly made promises as "deceptive practices." 15 U.S.C. § 45(a). State attorneys general, depending on state law, generally have enforcement power under state unfair and deceptive acts and practices statutes. *See* CAROLYN L. CARTER, NAT'L CONSUMER LAW CTR., CONSUMER PROTECTION IN THE STATES: A 50-STATE REPORT ON UNFAIR AND DECEPTIVE ACTS AND PRACTICES STATUTES 6 (2009), https://www.nclc.org/images/pdf/udap/report_50_states.pdf [https://perma.cc/S59A-B2KS]. Police departments that enter into contracts with vendors such as Axon may also bring a civil suit for breach of contract by the vendor.

267. FED. TRADE COMM'N, *supra* note 5, at 39.

268. *Id.* at 43.

269. *Id.* at 40.

270. *See id.*

271. *Id.*

272. *Id.*

273. *Id.*

a routine traffic stop), and later becomes relevant to another context (say a murder investigation), the police should not need to seek the video subject's (i.e., the suspect's) consent to use the video. The interest in solving and prosecuting a crime are too great in such a case. If the context shifts to something other than evidentiary use in a criminal prosecution, however, it may make more sense to seek renewed consent. Police departments may wish to provide notice or seek consent before releasing videos to the public, for instance, although doing so surfaces the tension between privacy and transparency.

The FTC recommends other specific methods of providing notice and choice in IoT devices. Many of these recommendations likely do not apply to BWCs, because the FTC assumes that the device's user will have some access to an interface to modify privacy settings, even if that interface is not on the device itself.[274] BWCs operate in a different context however. While the privacy of the BWC user (the police officer) is important, the subjects of the video footage (the public) will not have access to such an interface. Therefore, some of the recommendations like QR codes on devices, consumer choice during set up, management portals or dashboards, or general privacy menus do not apply and have been omitted from the discussion.[275] Nevertheless, some of the other best practices may still apply or be informative for addressing privacy and cybersecurity concerns, so they are included below.

a. Choices at point of sale

The FTC advocates, with regard to individual consumers, "opt-in choices at the time of purchase in '[p]lain language and multiple choices of levels.'"[276] The concept of a "point of sale," when police departments purchase cameras from their vendors, is not necessarily relevant to BWCs. But if the "point of sale" is the point at which officers interact with citizens, then this recommendation could make sense. Some police department policies instruct officers to obtain consent to record when they interact with the public.[277]

274. *See id.* at 40–41.

275. *Id.* at 41–42.

276. *Id.* at 41.

277. *Police Body Worn Cameras: A Policy Scorecard*, UPTURN (Nov. 2017), https://www.bwcscorecard.org/ [https://perma.cc/UX8J-BWTD].

b. Tutorials

The FTC suggests that IoT manufacturers offer tutorial videos to consumers on how to control privacy settings on their devices.[278] This recommendation could be useful to inform police officers about their privacy vis-à-vis BWCs. Police departments may also provide tutorials to the public about privacy and cybersecurity aspects of BWC and camera footage.

c. Icons

The FTC says that "[d]evices can use icons to quickly convey important settings and attributes, such as when a device is connected to the Internet."[279] This suggestion can apply to BWCs and is currently being employed in cameras with a visible light to indicate recording.[280] Some cameras even deploy a front-facing screen that shows members of the public how they are being recorded.[281]

d. "Out of band" communications

The FTC suggests "[w]hen display or user attention is limited, it is possible to communicate important privacy and security settings to the user via other channels," such as text or email.[282] Similar techniques may apply to BWCs, although they would need to adapt to the unique circumstances of policing. For instance, it could be plausible to imagine a smart phone app or other portable device that automatically tagged an individual when they appear in BWC footage and notify that person so they can review the footage after the fact. Assuming such a system does not compromise the integrity of footage or safety of officers, technology could be a means to give individuals notice and choice.[283]

278. FED. TRADE COMM'N, *supra* note 5, at 41.

279. *Id.* at 42.

280. *See, e.g.*, *Public Awareness Light on Police Body Cameras*, WOLFCOM ENTERPRISES, http://www.policebodycameras.com/police-bodyworn-camera-articles/police_public_awarness_indicator.htm [https://perma.cc/SXG7-NPX9].

281. *D-Series*, REVEAL MEDIA, https://www.revealmedia.com/products/d-series [https://perma.cc/TY4G-RWWU]. The manufacturer promotes this feature by saying it "has a proven calming effect on people being recorded and maximises transparency with the public." *Id.*

282. FED. TRADE COMM'N, *supra* note 5, at 42.

283. This approach would raise its own privacy issues, however, due to the automated identification of persons included in the video.

e. A user experience approach

The FTC suggests that "companies could consider an approach that applies learning from consumer behavior on IoT devices, in order to personalize choices."[284] Many members of the public will not interact with police officers often enough to form a personalized choice, so this suggestion would not seem directly relevant. On the other hand, further research may be useful concerning citizen preferences on privacy with relation to BWCs, such as whether they wish bystanders' faces to be blurred or whether and when officers should turn off the camera.

4. Administrative Privacy Controls

Another major report by the FTC, *Protecting Consumer Privacy in an Era of Rapid Change*, lays out the FTC's recommendations for Privacy by Design and administrative privacy controls.[285] Although the report does not focus on IoT specifically, Privacy by Design is an important concept for IoT because it seeks to build privacy into both the device itself and the organizational processes that handle camera footage and other personal data. This Article therefore includes a brief discussion of the FTC's Privacy by Design recommendations below to complement its IoT-specific work.

a. "Data Security: Companies Must Provide Reasonable Security for Consumer Data"[286]

The FTC report states "[i]t is well settled that companies must provide reasonable security" as an aspect of Privacy by Design.[287] The Microsoft and BITAG reports discussed above explain security best practices for IoT and their application to police BWCs.

284. *Id.*

285. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESS AND POLICYMAKERS 22–23 https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/T3U5-WDWR].

286. *Id.* at 24.

287. *Id.*

b. "Reasonable Collection Limitation: Companies Should Limit Their Collection of Data"[288]

The FTC recommends that companies "limit data collection to that which is consistent with the context of a particular transaction or the consumer's relationship with the business, or as required or specifically authorized by law."[289] This recommendation articulates a "data minimization" similar to the one discussed above.

This recommendation applies to police BWCs. Recall PERF's warning that always-on recording may interfere with community policing interactions or witness interviews.[290] Policies dictating that officers turn off their cameras in certain situations are a form of data minimization.

c. "Sound Data Retention: Companies Should Implement Reasonable Data Retention and Disposal Policies"[291]

The FTC recommends that companies "implement reasonable restrictions on the retention of data and should dispose of it once the data has outlived the legitimate purpose for which it was collected."[292] The FTC notes, however, that retention periods may be flexible and allowed to adapt to the needs of the organization and type of data.[293]

This recommendation clearly applies to BWCs as well. The ACLU recommends that retention of BWC footage "be measured in weeks not years, and video should be deleted after that period unless a recording has been flagged."[294] Retaining footage for shorter periods of time is seen as a data minimization technique that reduces privacy risk.[295] That BWCs are a type of IoT device lends further support for adopting reasonable data retention policies from the IoT literature.

288. *Id.* at 26.
289. *Id.* at 27.
290. MILLER & TOLIVER, *supra* note 41, at 12.
291. FED. TRADE COMM'N, *supra* note 285, at 27.
292. *Id.* at 28.
293. *Id.*
294. STANLEY, *supra* note 7, at 4.
295. *See id.* at 3–5.

d. "Accuracy: Companies should maintain reasonable accuracy of consumers' data"[296]

The FTC recommends "reasonable steps to ensure the accuracy of the data they collect and maintain, particularly if such data could cause significant harm or be used to deny consumers services."[297] The Commission also emphasizes here that measures to ensure accuracy should be flexible and "scaled to the intended use and sensitivity of the information."[298]

BWC footage is potentially very sensitive and therefore may warrant strict measures to ensure accuracy. This is especially true if the footage has the potential to be released to the public or used in a criminal prosecution. Maintaining the accuracy and integrity of this data may require tagging and auditing as well as strict cybersecurity measures like those discussed above.

e. "Companies should maintain comprehensive data management procedures throughout the life cycle of their products and services"[299]

For data management, the Commission recommends the following measures:

(a) "designation of personnel responsible for the privacy program;"
(b) "a risk assessment that, at a minimum, addresses employee training and management and product design and development;"
(c) "implementation of controls designed to address the risks identified;"
(d) "appropriate oversight of service providers;" and
(e) "evaluation and adjustment of the privacy program in light of regular testing and monitoring."[300]

Each of these measures apples to police BWCs. It is likely that police departments already have administrative procedures to safeguard gathered information on the public, for example training on how to handle evidence. Given the large volume of sensitive data the BWCs may generate, police departments may need to expand these procedures and formulate new ones. They should consider programs

296. FED. TRADE COMM'N, *supra* note 285, at 29.
297. *Id.*
298. *Id.* at 30.
299. *Id.*
300. *Id.* at 31.

that focus specifically on privacy, incorporating the measures listed above. Oversight of service providers is particularly important if departments use outside parties to handle the BWC footage.

D. Operationalizing Best Practices from the Expert IoT Literature

We hope the discussion here can speed up the transfer of insight from IoT privacy and security experts to police departments implementing BWC programs. Each police department is different, and policies must respond to local conditions. Further, we have not done field research on the institutional practices of the police. Nevertheless, we offer three points about how departments can operationalize these recommendations, then discuss the relevance of "smart city" developments, and conclude with comments on the importance of having technical, physical, and administrative safeguards for privacy and cybersecurity.

We first stress the importance of the contractual terms when police departments procure BWCs and related services. As is true in the private sector,[301] these contracts often provide the clearest legal source for requiring effective cybersecurity and privacy protection. Professor Jan Whittington and co-authors have written that local governments have the ability to be "market makers," not market takers" who must unquestionably accept contractual terms from their vendors.[302] Notably, state and local governments can provide by law that BWC procurements be done consistently with strong cybersecurity and privacy requirements. Bargaining power will vary based on the size of the department and other factors such as local procurement regulations, but police departments quite likely are better positioned to demand privacy and security best practices than the average consumer in the commercial IoT space.

Second, police departments can draw on their experience handling analog evidence to inform how they treat digital evidence. While digital evidence presents some unique challenges, some of which we explore above, departments should have experience

301. FED. FIN. INSTS. EXAMINATION COUNCIL, FFIEC CYBERSECURITY ASSESSMENT TOOL 49 (2017), https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017.pdf [https://perma.cc/VC7Q-X4GX].

302. Jan Whittington et al., *Push, Pull, and Spill: A Transdisciplinary Case Study in Municipal Open Government*, 30 BERKELEY TECH. L.J. 1899, 1954 (2015). *But see* Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. 101, 112–17 (2017) (documenting the power of surveillance technology companies, including BWC manufacturers, to influence policy) .

securing physical evidence to preserve the chain of custody and procedures to protect the privacy of victims. Departments will need to adapt to the digital age, but their old practices and principles will still be useful.

Third, police departments lack the institutional resources or experience to implement these best practices and should therefore consider seeking outside assistance. Such assistance could come from a variety of sources, such as the U.S. DOJ, industry associations such as PERF, or outside consultants. The U.S. DOJ and PERF have already studied BWC issues in depth and have preexisting channels through which to spread that research.[303] A key point of this Article is that there are challenging issues of privacy and cybersecurity that apply to BWCs, which merit systematic attention and adoption of best practices. These issues are also a fruitful area of ongoing research.[304]

One useful way to see the connection of BWCs to the IoT literature is to think of BWCs as a "smart city" application. Smart cities are cities "that integrate information and communication technologies ("ICTs") and the Internet of Things (IoT) to manage the city's assets and delivery of services."[305] Because smart cities rely heavily on IoT devices,[306] smart city research overlaps with IoT research. Cities have done extensive work implementing privacy and security best practices and policies that can inform the work of police departments. The cities of Seattle and San Francisco have public documents detailing their privacy and cybersecurity practices.[307] Localities have been enacting local ordinances that govern implementation of new surveillance technologies, including in Seattle, Oakland, and Santa Clara County (California).[308] Whether from

303. *See*, *e.g.*, BUREAU OF JUSTICE ASSISTANCE, *supra* note 37; MILLER & TOLIVER, *supra* note 41.

304. For one example of research on how police departments handle digital evidence, see Sheona A. Hoolachan & William B. Glisson, *Organizational Handling of Digital Evidence*, 2010 ADFSL CONF. ON DIGITAL FORENSICS, SECURITY, & L. 33, 41–43 (2010).

305. Woo, *supra* note 59, at 956.

306. *Id.* at 955.

307. *See* CITY OF SEATTLE, CITY OF SEATTLE PRIVACY PROGRAM 1, 23–33 (Oct. 2015), http://ctab.seattle.gov/wp-content/uploads/2015/10/COS-Privacy-Program.pdf [https://perma.cc/9MFS-KUBY]; ERICA FINKLE, DATASF: RESOURCES, OPEN DATA RELEASE TOOLKIT: PRIVACY EDITION 4–7 https://docs.google.com/document/d/1MhvEuGKFuGY2vLcNqiXBsPjCzxYebe4dJicRWe6gf_s/edit [https://perma.cc/C8CS-VC4Q].

308. Kevin Schofield, *Council Passes Surveillance Technology Ordinance*, SCC INSIGHT (July 31, 2017) https://sccinsight.com/2017/07/31/council-passes-surveillance-technology-ordinance/ [https://perma.cc/BT7M-HPHL]; *Privacy Advisory Commission*, CITY OF OAKLAND, http://www2.oaklandnet.com/OAK057463 [https://perma.cc/D7J9-

smart cities or the broader IoT literature, there is a wealth of information to help police departments implement BWCs while addressing privacy and cybersecurity concerns.

In mining previous cybersecurity and privacy sources for lessons for BWCs, this Article concludes with discussion of the importance of a system that addresses the full range of technical, physical, and administrative controls. The discussion here has examined three sources of recommendations, which significantly emphasized technical controls (BITAG), physical safeguards (Microsoft, emphasizing hardware risks), and administrative/organizational controls (the FTC). This framework of technical, physical, and administrative controls is longstanding and useful way to think about privacy and cybersecurity. The three categories of controls are set forth in a leading law and regulation—the Privacy Act of 1974[309] and the HIPAA Privacy Rule.[310] Police departments and policy makers should examine risks and controls for all three of these realms as they proceed with their BWC programs.

III. LESSONS FOR IOT FROM BWCS

Part II discussed lessons from IoT for BWCs. This Part considers two lessons that BWCs may offer for privacy and cybersecurity in the IoT. The first lesson is recognizing that IoT devices are not "always on." Instead, there are important issues to consider about when the IoT devices should record or not, depending on time and context. The second lesson is the potentially crucial role of transparency and accountability for determining when to provide information from an IoT device to various audiences. In these two respects, BWCs highlight issues that apply more generally to IoT, but where the BWC context makes the two issues more salient than in other IoT settings studied to date.

The implicit assumption in many smart cities and other IoT deployments is that the sensors are "always on." For instance, it

3MWV]; *Cutting-edge Surveillance Ordinance Approved for Santa Clara County*, CTY. SANTA CLARA (June 7, 2016), https://www.sccgov.org/sites/d5/newsmedia/press-releases/Pages/SurveillanceOrdinance.aspx [https://perma.cc/NPE6-6MHX].

309. 5 U.S.C. § 522(e)(10) (2012) (requiring "each agency" to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained").

310. 45 C.F.R. §§ 164.308–.312 (2017) (describing administrative, physical, and technical safeguard standards for the privacy of electronic protected health information).

makes sense for weather sensors to report atmospheric conditions on a 24/7 basis, for smart utility meters to measure usage continuously, and for sensors that detect urban gunshots to pick up sounds any time of the day or night. In the BITAG and Microsoft list of recommendations discussed in Part II, the issue of "always on" or "when to have the sensor on" does not appear explicitly in any of the recommendations. The FTC makes general recommendations about data minimization but does not focus on the data minimization technique of regularly turning the device off entirely.

By contrast, a significant issue for BWC governance is when the camera should be running. Work by Professor Fan and the digital rights group Upturn notes that in many cases the policies governing BWC use prohibit recording in bathrooms or locker rooms.[311] Scholars and advocacy groups suggest that officers should turn cameras off either at the request of victims or witnesses,[312] or in some cases should default to an opt-in regime.[313] The ACLU originally advocated something close to an "always on" model but eventually modified its position to recognize clear limits on recording to respect privacy.[314] This is in recognition that even in a context where ubiquitous recording is the norm, certain types of data are so sensitive that "always on" collection is inappropriate. Certain locations where people have a heightened expectation of privacy, or certain people who may be extra sensitive from trauma or other reasons, warrant clear limits on recording.

The need for transparency has also been a much more prominent issue for BWCs than for IoT generally. Transparency has been a principle reason cited by BWC advocates to adopt the technology.[315] For those supporting transparency, the rationale is that transparency will deter bad behavior and engender trust between officers and the communities they serve.[316] The value of transparency to detect bad behavior and foster future deterrence is illustrated by a high-profile 2017 incident of police officers caught planting drugs at a crime

311. Fan, *supra* note 10, at 429; UPTURN, *supra* note 277.

312. *See* MILLER & TOLIVER, *supra* note 41, at 12–13; STANLEY, *supra* note 7, at 3; UPTURN, *supra* note 277.

313. Fan, *supra* note 10, at 429.

314. STANLEY, *supra* note 7, at 3.

315. *See, e.g.*, *id.* at 2; UPTURN, *supra* note 277, at 4.

316. The ACLU lists policy goals for BWCs as "providing oversight, reducing police abuses, and increasing community trust." *Police Body Cameras*, AM. C.L. UNION, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/police-body-cameras [https://perma.cc/HSE3-3AHH].

scene.[317] Support for transparency has led commentators to worry that efforts to block release of BWC footage under state FOIAs will undermine transparency.[318] Advocates have opposed FOIA exemptions for BWC footage, showing the high value placed on transparency and accountability in the BWC context.[319]

Transparency has not been nearly as prominent a feature in the IoT literature more generally. There has indeed been attention to transparency in a somewhat different sense, such as where the FTC calls for greater transparency in company data practices through better privacy notices, consumer access to their data, and better consumer education.[320] The Online Trust Alliance, an industry group promoting best practices in IoT, similarly calls for transparency in the form of increased disclosure of data practices.[321] This meaning of "transparency," however, applies to transparency about an organization's policies and practices. In contrast, the core meaning of transparency in the BWC context has been about what is sometimes called "open data"—when and whether to release the actual video and accompanying audio to the general public.

This sort of "open data" issue has come up in the context of smart cities and other collection of information by the government. The Obama administration, for instance, had open data initiatives such as release of data on data.gov.[322] Authors including David Brin

317. Bill Chappell, *Baltimore Police Caught Planting Drugs in Body-Cam Footage, Public Defender Says*, NAT'L PUB. RADIO (July 20, 2017), http://www.npr.org/sections/thetwo-way/2017/07/20/538279258/baltimore-police-caught-planting-drugs-in-body-cam-footage-public-defender-says [https://perma.cc/2L5E-X84G].

318. Brian Liebman, *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); Joseph Wenner, *Who Watches the Watchman's Tape? FOIA's Categorical Exemptions and Police Body-Worn Cameras*, 2016 U. CHI. LEGAL F. 873, 874–75.

319. *See, e.g.,* JOSH DEVINE ET AL., POLICE BODY CAM FOOTAGE: JUST ANOTHER PUBLIC RECORD 16–17 (2015), https://isp.yale.edu/sites/default/files/publications/police_body_camera_footage-_just_another_public_record.pdf [https://perma.cc/4WCQ-CVL6]; Liebman, *supra* note 318, at 368; Wenner, *supra* note 318, at 905–06.

320. FED. TRADE COMM'N, *supra* note 285, at 60–72.

321. ONLINE TR. ALL., IOT SECURITY & PRIVACY TRUST FRAMEWORK V2.0, at 1 (2017), https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework2.1.pdf [https://perma.cc/DS78-2E9S].

322. *See* Alexis Madrigal, *Data.gov Launches to Mixed Reviews*, WIRED (May 21, 2009), https://www.wired.com/2009/05/datagov-launches-to-mixed-reviews/ [https://perma.cc/LX9T-QLEU]; *Open Government Data, Out of the Box*, ECONOMIST (Nov. 21, 2015), https://www.economist.com/news/international/21678833-open-data-revolution-has-not-lived-up-expectations-it-only-getting [https://perma.cc/3NYN-M4CQ]; John Podesta, *Big Data and Privacy: 1 Year Out*, THE WHITE HOUSE: PRESIDENT BARACK OBAMA (Feb. 5,

have also advocated for greater release of video feeds and other data in the name of transparency and accountability.[323] In practice, however, privacy concerns and the risk of re-identification have often resulted in data being released publicly than supporters had initially hoped. One important feature of BWCs is that full video is being released in many instances, despite concerns from the privacy side that bystanders, victims, or others are suffering a privacy violation due to such release.

These lessons from BWCs can inform best practices for IoT more generally. Best practice guides, such as those created by BITAG and Microsoft, quite possibly should consider more explicitly when to have an "always on" model, and when instead to minimize or stop data collection based on time of day or other criteria. Restrictions on BWC recording in bathrooms suggests that the location of recording may be an important guidepost. Limits on recording bystanders or witnesses implies that certain categories of people require greater sensitivity. U.S. law already recognizes heightened privacy interests of children and of data in the healthcare and financial fields.[324] We suggest that the IoT literature could explore application of limits based on place, person, or time. The IoT literature could also take note of the emphasis on transparency and open data in the BWC literature. BWCs are seen as a tool to hold powerful actors (police officers) to account. The value of transparency for data feeds from BWCs may provide broader lessons for how transparency could become a greater priority in other IoT settings.

CONCLUSION

A first conclusion of this Article is that BWCs are indeed an instance of IoT. The cameras and microphones are sensors, and the video and audio feeds characteristically go to storage in the cloud,

2015), https://obamawhitehouse.archives.gov/blog/2015/02/05/big-data-and-privacy-1-year-out [https://perma.cc/V26P-BZ72].

323. *See* DAVID BRIN, THE TRANSPARENT SOCIETY: WILL TECHNOLOGY FORCE US TO CHOOSE BETWEEN PRIVACY AND FREEDOM? 8–15, 326–29 (1998). Brin argues that "accountability is no side benefit .... Without the accountability that derives from openness—enforceable upon even the mightiest individuals and institutions—how can freedom survive?" *Id.* at 13. Further, Brin argues, "[a]ccountability is the only defense that ever adequately protected free speech." *Id.* at 327.

324. Federal law specifically regulates privacy in each of these areas. Children's Online Privacy Protection Act, 15 U.S.C. § 6502 (2012); Health Information Portability and Accountability Act, 42 U.S.C. § 1320d-6; Gramm-Leach-Bliley Act, 15 U.S.C. § 6801.

thus matching the standard IoT definition of sensors with cloud storage.

Understanding this technological equivalence of BWCs and IoT assists those seeking to manage the privacy and cybersecurity risks of BWCs. Police departments may understandably find that managing those risks is an expensive and daunting task. A principle goal of this Article has been to provide rich sources of best practices to assist those deploying and administering BWCs and the accompanying data services. One related outcome is to highlight the role of the procurement contract in governing privacy and cybersecurity risks. Under state or local law, or negotiation of individual contracts, cities and police departments have an opportunity to set requirements for how privacy and cybersecurity will be managed by the third-party vendors who are so important to the deployment of BWCs and related services.

Another outcome of the Article is to provide insights from the BWC experience for IoT more generally. An implicit assumption for many IoT deployments is that the sensors are "always on." For BWCs, this is typically not the case, and IoT best practices can do more to highlight the opportunity to toggle off sensors, achieving data minimization goals. In addition, BWCs are an example of "open data" where the full data feed is often available to the public. Those who have been debating the benefits of open data efforts, and the privacy and other associated risks, can learn from the extensive discussions about when transparency and open release of the video is appropriate for BWC footage.

Privacy and cybersecurity risks will continue to evolve for both IoT generally and BWCs more specifically. Recognizing the overlap of these two usually distinct discourses can offer assistance to those in both realms as they face the new risks.