Policing, Technology, and the Erosion of Constitutional Rights

*Terry Skolnik**

The relationship between technology and criminal procedure is typically described as follows. Technological innovation outpaces case law, statutes, and regulations. As technology evolves, judicial decisions that regulate its use may become outdated. Lawmakers and regulators typically react too slowly to new investigative technologies. Police officers exploit these jurisprudential, legislative, and regulatory vacuums. Law enforcement may deploy new investigative technologies that lack adequate transparency and oversight mechanisms, and that impact individuals' fundamental rights. Individuals cannot challenge secretive investigative tactics that are unknown to them. But technology not only outpaces case law, legislation, and regulation; emerging technologies progressively weaken constitutional norms.

This article argues that the cumulative effects of technological innovation and lax criminal procedure doctrines erode constitutional rights. It shows how two investigative strategies circumvent traditional constitutional protections: changing the normative quality of information gathering and changing the normative quality of information from private to public. To increase these strategies' effectiveness, officers use technology to leverage the criminal procedure doctrines of abandonment, waiver, and plain view searches—all of which weaken reasonable expectations of privacy. This article shows how the growth of these criminal procedure doctrines results in a one-way ratchet in criminal procedure, where the scope of police powers expands while the breadth of constitutional rights contracts or remains constant. It sets out how technology exacerbates this tendency.

The concluding parts of this article elucidate why three emerging investigative technologies—automated licence plate recognition, commercial DNA database searches, and facial recognition technology—risk eroding constitutional rights even further and must be regulated. It provides concrete proposals for how courts and lawmakers can safeguard individuals against these mass-surveillance technologies, and in doing so, restore the judiciary's role in protecting constitutional rights against state power.

* Associate Professor at the University of Ottawa's Faculty of Law and Co-Director of the uOttawa Public Law Centre. Visiting research fellow at the Academy for Justice and the Center for Constitutional Design at the Sandra Day O'Connor College of Law, Arizona State University. I thank Anna Maria Konewka, Vivek Krishnamurthy, and the anonymous reviewers for their helpful comments on prior drafts. I also thank the *Queen's Law Journal*'s editorial staff for their excellent feedback and edits that strengthened this article. All mistakes are my own.

Introduction

Typically, the relationship between technology and criminal procedure is characterized as follows. Technology's rapid evolution outpaces criminal procedure.[1] Lawmakers, regulators, and judges react too slowly to law enforcement's use of emerging investigative technologies.[2] Despite the rise of automated licence plate recognition, commercial DNA database searches, and facial recognition software, these technologies remain largely unregulated, and very few judicial decisions address their use.[3] Even when lawmakers or courts regulate certain technologies, these technologies may evolve so quickly that regulation loses its importance or becomes obsolete.[4]

1. Jessica Gabel Cino, "Tackling Technical Debt: Managing Advances in DNA Technology That Outpace the Evolution of Law" (2017) 54:2 Am Crim L Rev 373 at 377.

2. Gary E Marchant, "The Growing Gap Between Emerging Technologies and the Law" in Gary E Marchant, Braden R Allenby & Joseph R Herkert, eds, *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem* (New York: Springer, 2011) at 20–21.

3. Katelyn Ringrose & Divya Ramjee, "Watch Where You Walk: Law Enforcement Surveillance and Protester Privacy" (2020-2021) 11 Cal L Rev Online 349 at 355, 360; Samuel D Hodge, Jr, "Big Brother Is Watching: Law Enforcement's Use of Digital Technology in the Twenty-First Century" (2020) 89:1 U Cin L Rev 30 at 33–34.

4. Simon M Baker, "Unfriending the Stored Communications Act: How Technological Advancement and Legislative Inaction Have Rendered Its Protections Obsolete" (2011) 22:1 DePaul J Art Tech & IP L 75 at 78, 115.

There are other concerns. Individuals cannot contest secret investigative technologies that are unknown to them.[5] Furthermore, unregulated investigative technologies tend to lack adequate transparency and oversight mechanisms.[6] Increasingly, access to information requests—rather than statutory disclosure obligations or constitutional review—reveal how law enforcement uses investigative technologies unbeknownst to the public.[7] But there is another way to understand the relationship between technology and criminal procedure.

This article argues that the cumulative effects of technological innovation and lax criminal procedure doctrines expand police power while eroding constitutional rights.[8] It contends that police officers adopt two strategies to weaken these rights. First, officers change the normative quality of information gathering by acquiring data indirectly from databases rather than directly from individuals.[9] Second, officers change the normative quality of information from private to public, such that individuals lose a reasonable expectation of privacy that they would otherwise enjoy.[10] To facilitate these strategies, officers use technology to exploit three permissive criminal procedure doctrines: abandonment, waiver, and plain view searches.[11]

This article demonstrates how criminal procedure's evolution produced a one-way ratchet that expanded police power and limited constitutional rights.[12] It shows how criminal procedure results in legislative inertia and slippery slopes, both of which disadvantage defendants, and both of

5. Jonathan Manes, "Secrecy & Evasion in Police Surveillance Technology" (2019) 34:2 Berkeley Tech LJ 503 at 506.

6. Hannah Bloch-Wehba, "Access to Algorithms" (2020) 88:4 Fordham L Rev 1265 at 1283–88; Sarah Valentine, "Impoverished Algorithms: Misguided Governments, Flawed Technologies, and Social Control" (2019) 46:2 Fordham Urb LJ 364 at 376, 419.

7. Nicole Brockbank, "Toronto police used Clearview AI facial recognition software in 84 investigations", *CBC News* (23 December 2021), online: <cbc.ca> [perma.cc/Y7V7-FV9E].

8. Richard Jochelson, "Trashcans and Constitutional Custodians: The Liminal Spaces of Privacy in the Wake of *Patrick*" (2009) 72:2 Sask L Rev 199 at 221–22 [Jochelson, "Trashcans and Constitutional Custodians"].

9. Terry Skolnik, "Two Criminal Justice Systems" (2023) 56:1 UBC L Rev 285 at 302–04 [Skolnik, "Two Criminal Justice Systems"].

10. William MacKinnon, "Discarding Reasonable Expectations of Privacy: A Critique of *R. v. Patrick*" (2010) 47:4 Alta L Rev 1037 at 1039, 1044.

11. Kathleen Hammond, "Unnecessary and Redundant? Evaluating Canada's *Genetic Non-Discrimination Act*, 2017" (2020) 98:3 Can Bar Rev 480 at 497.

12. See e.g. William J Stuntz, "The Pathological Politics of Criminal Law" (2001) 100:3 Mich L Rev 505 at 507–09 (describing the concept of a one-way ratchet in criminal law and procedure) [Stuntz, "Pathological Politics"]. This argument was also advanced in Akwasi Owusu Bempah et al, *Ancillary Police Powers in Canada: Deep Roots and Current Challenges* (Vancouver: UBC Press), ch 7 [forthcoming in 2024].

which are exacerbated by technological innovation.[13] Its concluding parts set out why three emerging investigative technologies—automated licence plate recognition, commercial DNA databank searches, and facial recognition software—can erode constitutional rights even further and must be regulated to protect privacy, liberty, and equality.[14] It offers judicial and legislative oversight mechanisms to achieve that end, which leverage each branch of government's respective institutional competence.

The structure of this article is as follows. Sections II and III explain how officers adopt two strategies to weaken reasonable expectations of privacy: changing the normative quality of information gathering and modifying the normative quality of information. These sections elucidate how officers exploit technology and certain criminal procedure doctrines to make these strategies more effective. Sections IV and V show how these strategies produce a one-way ratchet in criminal procedure that technology aggravates. Section VI explains the need to regulate the three emerging investigative technologies mentioned above. Section VII concludes this article. It offers concrete proposals to safeguard individuals against mass-surveillance technologies, and ultimately, to help restore the judiciary's counter-majoritarian role within constitutional criminal procedure.[15]

I. Policing, Technology, and Information Gathering

A. Policing and Information Deficits

Police officers routinely face information deficits.[16] After explaining how constitutional norms prohibit officers from directly acquiring data to fix these deficits, this section shows how technology helps officers indirectly gather information in a manner that skirts constitutional norms. When officers initiate proactive police encounters or respond to calls, they often lack vital

13. James Stribopoulos, "The Limits of Judicially Created Police Powers: Investigative Detention after *Mann*" (2007) 52:3/4 Crim LQ 299 at 315–17 [Stribopoulos, "The Limits of Judicially Created Police Powers"].

14. Thomas Linder, "Surveillance Capitalism and Platform Policing: The Surveillant Assemblage-as-a-Service" (2019) 17:1/2 Surveillance & Society 76 at 76–79.

15. Terry Skolnik, "Rééquilibrer le rôle de la Cour suprême du Canada en procédure criminelle" (2022) 67:3 RD McGill 259 at 266 [Skolnik, "Rééquilibrer le rôle"].

16. This subsection's arguments were initially advanced in: Terry Skolnik, "Policing in the Shadow of Legality: Pretext, Leveraging, and Investigation Cascades" (2023) 60:3 Osgoode Hall LJ 505 at 518–19, 531–32 [Skolnik, "Policing in the Shadow of Legality"] and in Skolnik, "Two Criminal Justice Systems", *supra* note 9 at 291–99.

information that others possess.[17] During a traffic stop, officers do not know what drivers are hiding in their pockets, glove compartments, or trunks.[18] Similarly, when patrolling, officers do not know which individuals have warrants or bail conditions.[19] In each of these cases, the individual knows this information; they enjoy an informational advantage over law enforcement.[20]

This information asymmetry creates an important hurdle for police officers. The police have important statutory and common law duties to prevent crimes, protect people and property from harm, and maintain public order.[21] Yet, crime tends to be hidden, and individuals who commit crimes do not wish to be caught.[22] Officers have difficulty repressing crimes that they cannot see.[23] During police interactions, officers also want to have certain information for another reason: safety.[24] They want to know whether individuals are armed, which can influence how they respond to specific situations.[25]

Two interrelated factors explain why officers face information asymmetries that hamstring their investigative capacities—factors that in turn illustrate the value of investigative technologies. First, physical barriers—such as clothing, trunks, and housing—conceal criminality.[26] Second, constitutional norms prevent officers from removing these physical barriers to discover incriminating evidence.[27] Various constitutional rights illustrate this point.

Section 8 of the *Canadian Charter of Rights and Freedoms* (the *Charter*) prohibits officers from searching persons or their property unless the officer

17. *Ibid*.

18. Skolnik, "Two Criminal Justice Systems", *supra* note 9 at 293; John Hollway, Calvin Lee & Sean Smoot, "Root Cause Analysis: A Tool to Promote Officer Safety and Reduce Officer Involved Shootings Over Time" (2017) 62:5 Vill L Rev 883 at 887; Skolnik, "Policing in the Shadow of Legality", *supra* note 16 at 531–32.

19. Skolnik, "Two Criminal Justice Systems", *supra* note 9 at 293; Skolnik, "Policing in the Shadow of Legality", *supra* note 16 at 531–32.

20. Terry Skolnik, "R. v. Macdonald and the Illogicality of the Reasonable Belief Requirement for Safety Searches" (2015) 62:1/2 Crim LQ 43 at 49.

21. *Fleming v Ontario*, 2019 SCC 45 at paras 2, 69–70 [*Fleming*].

22. Skolnik, "Two Criminal Justice Systems", *supra* note 9 at 294.

23. *Ibid* at 293–94.

24. *R v MacDonald*, 2014 SCC 3 at paras 1, 40.

25. Paul L Taylor, "Dispatch Priming and the Police Decision to Use Deadly Force" (2020) 23:3 Police Q 311 at 316–17, 327.

26. Skolnik, "Two Criminal Justice Systems", *supra* note 9 at 293–94.

27. *Ibid*.

meets certain legal thresholds, obtains a warrant, or acts under exigent circumstances.[28] The section 9 *Charter* right to be free from arbitrary detention bars officers from intrusively questioning an individual unless the officer meets the reasonable suspicion requirement and informs the person of their *Charter* rights.[29] Together, sections 7 and 10 of the *Charter* require officers to inform detained and arrested individuals of their constitutional right to silence and their right to contact legal counsel.[30] Officers must then abstain from questioning them if they wish to speak with a lawyer.[31] When law enforcement violates these constitutional rights, section 24(2) of the *Charter* authorizes courts to exclude unconstitutionally obtained evidence whose admission would bring the administration of justice into disrepute.[32] These constitutional rights reduce officers' ability to fix information asymmetries, discover evidence, and extricate inculpatory confessions.[33]

Notice how these constitutional rights prohibit certain investigative tactics that officers use to gather information *directly* from suspects. Courts forbid unlawful detentions, interrogations, and searches because these information-gathering tactics can be oppressive, degrading, or unfair.[34] These same tactics can also exploit a defendant's vulnerability while in police custody.[35] Such tactics are barred because they both violate constitutional rights and

28. *Canadian Charter of Rights and Freedoms,* s 8, Part 1 of the *Constitution Act, 1982,* being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Canadian Charter*]; Kent Roach, "Twenty Years of the Charter and Criminal Justice: A Dialogue between a Charter Optimist, a Charter Realist and a Charter Sceptic" (2003) 19:2 SCLR 39 at 43.

29. *Canadian Charter*, *supra* note 28, s 9; Steven Penney & James Stribopoulos, "'Detention' under the Charter after *R. v. Grant* and *R. v. Suberu*" (2010) 51 SCLR (2d) 439 at 474; *R v Mann*, 2004 SCC 52 at para 45 [*Mann*].

30. *Canadian Charter*, *supra* note 28, ss 7 & 10; *R v Hebert*, [1990] 2 SCR 151, 1990 CanLII 118 at 164 (SCC) (explaining the right to silence); Steven Penney, "Triggering the Right to Counsel: 'Detention' and Section 10 of the Charter" (2008), 40 SCLR (2d) 271 at 272, 276 (at note 24).

31. *R v Manninen*, 1987 CanLII 67 at para 23 (SCC) [*Manninen*].

32. *Canadian Charter*, *supra* note 28, s 9; *R v Grant*, 2009 SCC 32 [*Grant*]; Richard Jochelson, Debao Huang & Melanie Murchison, "Empiricizing Exclusionary Remedies – A Cross Canada Study of Exclusion under s. 24(2) of the Charter, Five Years after *Grant*" (2016) 63 Crim LQ 206 at 206–07, 209–11.

33. Skolnik, "Two Criminal Justice Systems", *supra* note 9 at 295–99; Don Stuart, "Charter Standards for Investigative Powers: Have the Courts Got the Balance Right?" (2008) 40 SCLR (2d) 3 at 35.

34. *Mann*, *supra* note 29 at para 45; Stephen C Thaman, "Constitutional Rights in the Balance: Modern Exclusionary Rules and the Toleration of Police Lawlessness in the Search for Truth" (2011) 61 UTLJ 691 at 711–12.

35. *Grant*, *supra* note 32 at para 22.

undermine the fundamental interests that underpin these rights, such as liberty, dignity, equality, privacy, respect for persons, and more.[36]

Constitutional criminal procedure, therefore, proscribes investigative tactics that are used to directly gather information in a manner that sets back fundamental interests.[37] However, as discussed next, officers use investigative technologies to indirectly acquire information in a manner that lacks the typical hallmarks of unconstitutionality, such as oppressiveness, degradingness, and intrusiveness. As a result, officers can indirectly acquire the same information in a manner that skirts existing constitutional rights.

B. Technology and the Normative Quality of Information Gathering

Investigative technologies are crucial for police officers, but for reasons that we generally ignore. In criminal procedure, technology can convert the normative quality of information gathering from unlawful to lawful.[38] By using technology to acquire information, officers transform otherwise unconstitutional investigative tactics into constitutional ones.[39] They do so by lawfully gathering information indirectly that they cannot lawfully gather directly.[40]

Many areas of criminal procedure authorize such tactics. Take the example of Forward-Looking Infrared (FLIR) technology that measures the amount of heat that a dwelling emits.[41] Suppose officers want to determine whether an individual is growing marijuana in their home. Officers cannot trespass onto an individual's property, place their hand on a window, and gauge the level of heat that the house discharges.[42] Such tactics are impermissible. An individual's home—including its perimeter—attracts one of the strongest expectations of privacy in criminal law, and one that enjoys a very robust historical pedigree.[43] Some of the earliest common law decisions that involved

36. *R v Golden*, 2001 SCC 83 at paras 87, 98–99 [*Golden*]; Glen Luther, "Consent Search and Reasonable Expectation of Privacy: Twin Barriers to the Reasonable Protection of Privacy in Canada" (2008) 41:1 UBC L Rev 1 at 19–20.

37. Erik G Luna, "The Models of Criminal Procedure" (1999) 2:2 Buff Crim L Rev 389 at 473–74.

38. Skolnik, "Two Criminal Justice Systems", *supra* note 9 at 302–04.

39. *Ibid*.

40. *Ibid*.

41. *R v Tessling*, 2004 SCC 67 [*Tessling*]; Alan Young, "Search and Seizure in 2004: Dialogue or Dead-End?" (2005) 29 SCLR (2d) 351 at 355.

42. *R v Plant*, 1993 CanLII 70 (SCC) [*Plant*].

43. *Ibid*; *R v Feeney*, 1997 CanLII 342 at para 43 (SCC) [*Feeney*]; Benjamin Barros, "The Home as a Legal Concept" (2006) 46 Santa Clara L Rev 255 at 263–69.

searches and seizures analogize a home to a castle and limit the state's ability to trespass on a person's property without a warrant.[44]

Yet, officers can use technology to indirectly acquire the same information with none of the constitutional backlash.[45] The Supreme Court of Canada has decided that officers can lawfully fly an airplane over an individual's home and use FLIR technology to measure the dwelling's heat levels, without having to satisfy any legal threshold.[46] Although individuals have a strong expectation of privacy over their homes, they have no expectation of privacy over the amount of heat that their home releases.[47] The Court noted that a home's temperature attracts no reasonable expectation of privacy because it does not reveal personal information that goes to an individual's biographical core.[48] Through this process, officers acquire data indirectly that they cannot acquire directly.

The distinction between unlawful street-level interrogations and lawful police database checks are another example. Officers may want to know whether an individual has a criminal history, is sought by warrant, or is breaching their bail conditions.[49] Yet, unless officers meet the reasonable suspicion threshold and satisfy other requirements, they cannot ask invasive questions about the person's past or present involvement in crime.[50]

Here too, technology allows officers to acquire this information indirectly and lawfully. The law authorizes police officers to conduct random traffic stops.[51] They can also pull over drivers who commit motor vehicle offences.[52] Given the breadth of highway safety codes, most drivers will inevitably commit a traffic-related offence if they are observed for long

44. Barros, *supra* note 43 at 263–69; *Semayne's Case* (1604), 5 Co Rep 91a, 77 ER 194 (Eng KB).

45. Skolnik, "Two Criminal Justice Systems", *supra* note 9 at 302–04.

46. *Tessling*, *supra* note 41 at para 63.

47. *Ibid*.

48. *Ibid*; *Plant*, *supra* note 42; *R v Gomboc*, 2010 SCC 55 at paras 38, 40; Tim Quigley, "The Impact of the Charter on the Law of Search and Seizure" (2008) 40 SCLR (2d) 117 at 133–36 [Quigley, "The Impact of the Charter"].

49. Skolnik, "Two Criminal Justice Systems", *supra* note 9 at 293; Skolnik, "Policing in the Shadow of Legality", *supra* note 16 at 519.

50. *R v Le*, 2019 SCC 34 at paras 27–28.

51. *R v Ladouceur*, [1990] 1 SCR 1257 at 1287, 1990 CanLII 108 (SCC) [*Ladouceur*].

52. David A Sklansky, "Traffic Stops, Minority Motorists, and the Future of the Fourth Amendment" [1997] Sup Ct Rev 271 at 273.

enough by law enforcement.[53] Officers thus have the authority to pull over any vehicle irrespective of whether the driver violated some law.[54]

During a traffic stop, officers can order the driver to provide their driver's licence—a requirement that is justified by the need to ensure public safety on roads.[55] Officers can then verify the driver's information in one of several police databases, and lawfully acquire the very information that they cannot obtain through invasive questioning.[56] They can use centralized police databases—such as the Canadian Police Information Centre—to access a broad array of data about individuals, firearms, and vehicles, all of which are unavailable to the public.[57] Many police forces also have internal databases that contain even more information, such as individuals' photographs, prior occurrence reports, certain intelligence-related information, and more.[58] Like everyone else, officers can also run individuals' information through search engines and social media sites that reveal personal data about them.[59]

This data receives minimal constitutional protection. Courts have held that individuals lack a reasonable expectation of privacy over information that is contained in police databases or that is publicly available on social media.[60] In this way, criminal procedure allows officers to acquire drivers' information indirectly through databases that they cannot acquire directly through questioning.[61] And they do so without asking any invasive questions or infringing any constitutional rights.

53. Jordan Blair Woods, "Traffic Without the Police" (2021) 73:6 Stan L Rev 1471 at 1481.

54. Skolnik, "Policing in the Shadow of Legality", *supra* note 16 at 519.

55. *Ladouceur*, *supra* note 51 at 1285–86.

56. Steven Penney, "Driving While Innocent: Curbing the Excesses the 'Traffic Stop' Power" (2019) 24 CCLR 339 at 341 [Penney, "Driving While Innocent"].

57. *Ibid*; Jennifer Hegel, Karen D Pelletier & Mark E Olver, "Predictive Properties of the Ontario Domestic Assault Risk Assessment (ODARA) in a Northern Canadian Prairie Sample" (2022) 49:3 Crim Justice & Behavior 411 at 417–18.

58. For discussions of individuals' photos contained in Montreal police databases, Police Information Portal databases, and management of police occurrence reports and intelligence reports generally, see *R c Qiluqi*, 2020 QCCM 122 at paras 33, 37; *R c Viellot Blaise*, 2020 QCCM 26 at para 99; *R v Mooiman and Zahar*, 2016 SKCA 43 at para 7; *Toronto (Police Services Board) (Re)*, 2020 CanLII 33291 at para 18 (ONIPC); *R v Fowler*, 2021 ONSC 3180; cited in Skolnik, "Two Criminal Justice Systems", *supra* note 9 at 303.

59. Seth W Fallik et al, "Policing through social media: a qualitative exploration" (2020) 22:2 Intl J Police Science & Management 208 at 212.

60. Penney, "Driving While Innocent", *supra* note 56 at 355.

61. Skolnik, "Policing in the Shadow of Legality", *supra* note 16 at 518–19.

II. Criminal Procedure and the Public-Private Distinction

Officers not only use technology to change the normative quality of information gathering from unlawful to lawful. They also leverage permissive criminal procedure doctrines to transform the normative quality of *information* from private to public—a tactic that erodes individuals' reasonable expectations of privacy and weakens their constitutional rights.

To illustrate this point, consider first how the law of search and seizure conceptualizes privacy, and how officers take advantage of loopholes in privacy's normative framework (more on how technology exacerbates this tendency in the next section). Section 8 of the *Charter* confers a constitutional right to be free from unconstitutional search and seizure.[62] Yet, this section 8 *Charter* right only protects reasonable expectations of privacy, which is assessed according to subjective and objective standards.[63] Subjectively, the individual must sincerely believe that they had an expectation of privacy in the circumstances.[64] That subjective belief must also be objectively reasonable considering the totality of the circumstances.[65]

Search and seizure law adheres to a rough heuristic (or rule of thumb) to determine whether expectations of privacy are reasonable. Information, data, objects, or locations that are private in nature generally attract stronger expectations of privacy; those that are public in nature generally do not.[66] A person's body, home, vehicle, computer, and cellphone all attract robust expectations of privacy, given their inherently personal nature.[67] Conversely, individuals lack reasonable expectations of privacy over information that they post on social media, things that they abandon in public places, and objects

62. *Canadian Charter*, *supra* note 28, s 8.

63. *Hunter et al v Southam Inc*, [1984] 2 SCR 145 at 159, 1984 CanLII 33 (SCC) [*Hunter*]; Hamish Stewart, "Normative Foundations for Reasonable Expectations of Privacy" (2011) 54 SCLR (2d) 335 at 335.

64. Simon Stern, "Textual Privacy and Mobile Information" (2018) 55:2 Osgoode Hall LJ 398 at 411, 413–14; *R v Cole*, 2012 SCC 53 at para 40 [*Cole*].

65. *Cole*, *supra* note 64 at para 40.

66. Daniel J Solove, "Conceptualizing Privacy" (2002) 90:4 Cal L Rev 1087 at 1107; William J Stuntz, "Distribution of Fourth Amendment Privacy" (1999) 67:5 Geo Wash L Rev 1265 at 1265 [Stuntz, "Distribution of Fourth Amendment Privacy"].

67. *R v Stillman*, 1997 CanLII 384 (SCC) [*Stillman*]; *Feeney*, *supra* note 43; *R v Fearon*, 2014 SCC 77 [*Fearon*]; see also William J Stuntz, "Privacy's Problem and the Law of Criminal Procedure" (1995) 93:5 Mich L Rev 1016 at 1021–24.

that are plainly visible to the public.[68] Like elsewhere in the law, the public/private distinction is fundamental to criminal procedure.[69] And like elsewhere in the law, the public/private dichotomy can be manipulated to confer advantages to some individuals at the expense of others.[70]

For police officers, individuals' privacy is a bad thing. The private nature of information is an inconvenient constitutional barrier that hampers criminal investigations. However, information that is conceptualized as publicly visible or available—or simply non-private—throws up no such obstacles.[71] This explains why many investigative tactics attempt to convert private information to public information, so that individuals lose their reasonable expectation of privacy and its associated constitutional protection. Three criminal procedure doctrines facilitate such practices: abandonment, waiver, and plain view searches.

Consider abandonment first. Criminal procedure doctrine recognizes that individuals lose their reasonable expectation of privacy over information or objects that they abandon in public.[72] The doctrine is a convenient way to circumvent two constitutional safeguards: the prohibition against seizing bodily substances from the defendant without a warrant, and the prohibition against entering a home without a warrant to seize evidence.[73] Early *Charter* jurisprudence outlawed the police from warrantlessly seizing individuals' bodily substances.[74] It also forbade officers from warrantlessly seizing bodily substances that suspects inevitably shed while in police custody, such as hairs, saliva, or mucus.[75] Search and seizure law also bars officers from entering a suspect's private residence without a warrant to search for DNA evidence.[76]

68. *R v Marakah*, 2017 SCC 59 at paras 55, 116 (describing the lack of a reasonable expectation of privacy over information posted publicly on social media); *R v Patrick*, 2009 SCC 17 [*Patrick*] (discussing the doctrine of abandonment); *R v Boersma*, 1994 CanLII 99 (SCC) (explaining that individuals have no reasonable expectation of privacy over objects that are in plain view); Brian Mund, "Social Media Searches and the Reasonable Expectation of Privacy" (2017) 19:1 Yale JL & Tech 238 at 240.

69. David A Sklansky, "The Private Police" (1999) 46:4 UCLA L Rev 1165 at 1270.

70. Ruth Gavison, "Feminism and the Public/Private Distinction" (1992) 45:1 Stan L Rev 1 at 35.

71. *Hunter*, *supra* note 63 at 159.

72. *Patrick*, *supra* note 68; Jochelson, "Trashcans and Constitutional Custodians", *supra* note 8 at 212.

73. *Feeney*, *supra* note 43; *Stillman*, *supra* note 67.

74. *Stillman*, *supra* note 67; *R v Dyment*, 1988 CanLII 10 (SCC) [*Dyment*]; James Stribopoulos, "A Failed Experiment? Investigative Detention: Ten Years Later" 2003) 41:2 Alta L Rev 335 at 371 [Stribopoulos, "A Failed Experiment"].

75. *Stillman*, *supra* note 67 at paras 58–63; *D'Amico c R*, 2019 QCCA 77 at paras 99–104 [*D'Amico*].

76. *Feeney*, *supra* note 43.

The cumulative effects of the public/private distinction and the abandonment doctrine remedy these problems. In some contexts, undercover agents trick the defendant to chew gum or drink from a disposable cup in a public place.[77] The defendant then discards these objects and officers seize them for DNA analysis.[78] Courts have upheld this warrantless seizure as constitutional.[79] By discarding these objects in public, defendants lost whatever reasonable expectation of privacy they once had over the object.[80] The abandonment doctrine can circumvent warrant requirements by shifting the information's normative quality from private to public.

Second, the waiver doctrine functions similarly. Criminal procedure permits individuals to waive their rights, and allows some form of police action that would ordinarily be unconstitutional.[81] Officers may request to search an individual's pockets, bags, or trunk—all of which normally attract a reasonable expectation of privacy.[82] Yet, once individuals waive their rights, they waive the reasonable expectation of privacy that these rights provide.[83] When this happens, the law generally treats the evidence as if it were non-private; consent modifies the normative quality of the information from private to public.[84]

Consent also modifies the normative quality of conduct in other areas of the law, such as criminal law or tort law.[85] Consider the defence of consent in these legal domains. Normally, the law treats physical force against others as presumptively wrong.[86] Non-consensual physical contact can constitute a physical or sexual assault, or give rise to the tort of battery.[87] Yet, an individual can lawfully consent to being touched by others.[88] In both criminal law and

77. *D'Amico*, *supra* note 75 at paras 321, 391; *R v Delaa*, 2009 ABCA 179 at para 19 [*Delaa*].

78. *Delaa*, *supra* note 77 at para 19.

79. *Ibid*.

80. *Ibid*.

81. William J Stuntz, "Waiving Rights in Criminal Procedure" (1989) 75:4 Va L Rev 761 at 762; Steven Penney, "Consent Searches for Electronic Text Communications: Escaping the Zero-Sum Trap" (2018) 56:1 Alta L Rev 1 at 7 [Penney, "Consent Searches"].

82. *Cloutier v Langlois*, [1990] 1 SCR 158 at 182, 185, 187, 1990 CanLII 122 (SCC) [*Cloutier*]; *R v Caslake*, 1998 CanLII 838 at paras 3, 15 (SCC) [*Caslake*].

83. Luther, *supra* note 36 at 4.

84. *Ibid*.

85. Vera Bergelson, "The Meaning of Consent" (2014) 12:1 Ohio St J Crim L 171 at 171–72; Terry Skolnik, "Use of Force and Criminalization" (2022) 85:3 Alb L Rev 663 at 665–66.

86. Hamish Stewart, "The Limits of Consent and the Law of Assault" (2011) 24:1 Can JL & Jur 205 at 206–07 [Stewart, "The Limits of Consent"].

87. *Ibid*.

88. *Ibid* at 208–09.

tort law, consent modifies the normative character of the physical contact from something that was wrong into something that is acceptable.[89] In search and seizure law, consent searches shift the normative character of information from private to public by removing one's reasonable expectation of privacy.

Consent is crucial for police officers because they can bypass normal constraints that protect defendants' privacy. Police officers have the common law power to search a defendant's cellphones incidental to arrest in certain circumstances.[90] Although officers can more easily search cellphones that are not passcode protected, they may be unable to search a passcode-protected phone. In many cases, officers obtain a search warrant and an assistant order so that a third party may unlock the phone.[91] But officers may also ask the defendant whether they will agree to waive their section 8 *Charter* right and consensually disclose their passcode.[92] Waiver is particularly effective for police officers. Empirical studies tend to show that many individuals consent to searches when they have no obligation to do so.[93] Moreover, a high percentage of individuals—including those who have done nothing wrong—also permit others to search through their phones.[94]

To be clear, the law imposes a relatively high threshold for a defendant to lawfully waive their constitutional right to be free from unreasonable search and seizure.[95] The defendant must be truly aware of the consequences of waiving

89. Bergelson, *supra* note 85 at 1712; Peter Schaber, "Consent and Wronging a Person" in Andreas Müller & Peter Schaber, eds, *The Routledge Handbook of the Ethics of Consent* (New York: Routledge, 2018) 61 at 61; Felix Koch, "Consent as a Normative Power" in Andreas Müller & Peter Schaber, eds, *The Routledge Handbook of the Ethics of Consent* (New York: Routledge, 2018) 32 at 32.

90. *Fearon*, *supra* note 67.

91. *Re: section 487.02 of the Criminal Code*, 2019 NLCA 6 at para 106 (providing an overview of these decisions).

92. *R v SL*, 2019 ONCJ 101 at paras 81–97. Note that officers must re-inform a person of their right to counsel in such contexts. See e.g. *R v Boutros*, 2018 ONCA 375. Yet individuals may waive both their right to counsel and their reasonable expectation of privacy.

93. Illya Lichtenberg, *Voluntary Consent or Obedience to Authority: An Inquiry into the Consensual Police-Citizen Interaction* (PhD Dissertation, Rutgers University, 1999) at 260–75; David K Kessler, "Free to Leave? An Empirical Look at the Fourth Amendment's Seizure Standard" (2008) 99:1 J Crim L & Criminology 51 at 65, 74–79; LAPD, *Arrest, Discipline, Use of Force, Field Data Capture and Audit Statistics Covering Period of January 1, 2006 – June 30, 2006* (Los Angeles: 2006) at 8, cited in Oren Bar-Gill & Barry Friedman, "Taking Warrants Seriously" (2012) 106:4 Nw UL Rev 1609 at 1662. These articles are cited in Skolnik, "Policing in the Shadow of Legality", *supra* note 16 at 526–27.

94. Roseanna Sommers & Vanessa K Bohns, "The Voluntariness of Voluntary Consent: Consent Searches and the Psychology of Compliance" (2019) 128:7 Yale LJ 1962 at 1987.

95. Luther, *supra* note 36 at 5.

their right and must be informed that they can refuse a waiver request.[96] Furthermore, the prosecution must prove that a waiver is informed and voluntary.[97] Yet, as discussed above, many defendants still waive their rights despite the exacting threshold.[98] Furthermore, courts do not assess the lawfulness of many waivers, given the low visibility of police encounters and the high guilty plea rate in criminal trials.[99]

Third, the plain view doctrine also helps officers shift the normative quality of information from private to public. Individuals lack a reasonable expectation of privacy over objects or information that is visible to the public, such as drugs or weapons on the centre console of one's vehicle.[100] Officers do not need a warrant or reasonable and probable grounds to seize things that are in plain view.[101] However, even when individuals strive to confer themselves greater privacy, officers can use the plain view doctrine to thwart such attempts.

For instance, officers cannot see through a vehicle's tinted windows—an additional physical barrier that confers greater privacy to the individual. Yet, officers can shine a flashlight through the vehicle's tinted windows to illuminate its interior and discover illegal objects. Courts have decided that this tactic is lawful and does not constitute a search.[102] Or, officers may pull over a vehicle, speak with the driver, request their licences, and look through the vehicle's window during this exchange. They can use whatever inculpatory evidence they see or smell—such as narcotics or drug paraphernalia, illegal objects, signs of impairment, or the scent of marijuana—to conduct a more intrusive

96. *Ibid*; see e.g. *Clarkson v The Queen*, 1986 CanLII 61 at para 18 (SCC) (discussing the requirements for a valid waiver).

97. Penney, "Consent Searches", *supra* note 81 at 16; Ryan Liss, "Whose Right is it Anyway? Adjudicating Charter Rights in the Context of Multiple Rights Holders" (2020) 94 SCLR (2d) 271 at 276.

98. Lichtenberg, *supra* note 93.

99. See e.g. James Stribopoulos, "Packer's Blind Spot: Low Visibility Encounters and the Limits of Due Process versus Crime Control" in François Tanguay-Renaud & James Stribopoulos, eds, *Rethinking Criminal Law Theory: New Canadian Perspectives in the Philosophy of Domestic, Transnational, and International Criminal Law* (Oxford: Hart Publishing, 2012) 193 at 209 (describing the low visibility of police encounters).

100. *R v Boersma*, 1994 CanLII 99 (SCC).

101. James A Fontana & David Keeshan, *The Law of Search and Seizure in Canada*, 11th ed (Toronto: LexisNexis, 2019) at 1061–75.

102. *R v Grunwald*, 2010 BCCA 288 at paras 37–55 [*Grunwald*]; *R v Mitchell*, 2019 ONSC 2613 at para 109 [*Mitchell*]; *R v Wilson*, 2015 ONSC 4135 at paras 23–37 [*Wilson*], and accompanying cases; *R v Ceballos*, 2014 ONSC 2281 at paras 73–79 [*Ceballos*].

investigation or to arrest the individual.[103] In both contexts, the law conceptualizes the objects that officers saw and the information that they acquired as if it were in plain view.[104] A flashlight's technology may be primitive, but it is still technology that leverages the plain view search doctrine to officers' benefit.

These examples illustrate how law enforcement chips away at individuals' reasonable expectations of privacy by converting private information into public information. These same examples also show how police officers can use technology to exploit weaknesses in criminal procedure doctrines. As discussed more below, certain features of constitutional criminal procedure, technology, and adjudication further erode defendants' constitutional rights and reduce individuals' privacy even more.

III. Criminal Procedure as a One-Way Ratchet

Technology is inseparable from the two above-mentioned policing strategies that weaken constitutional norms: changing the normative quality of information gathering and converting the normative quality of information from private to public. But this is only half the story. The other half has less to do with policing tactics, and more to do with how criminal procedure's democratic design—and political dynamics—disadvantage defendants and decrease individuals' privacy.[105] These democratic and political realities, in turn, further strengthen the effectiveness of these two policing strategies and further weaken defendants' constitutional rights.

Consider first constitutional criminal procedure's democratic design and political dynamics. Constitutional criminal procedure's worst-kept secret is that Parliament rarely enacts new police powers, codifies existing ones, or proactively regulates emerging technologies.[106] Courts tend to create new police powers through the judicially created ancillary powers doctrine, which

103. Skolnik, "Policing in the Shadow of Legality", *supra* note 16 at 520, 532. Note how such searches would satisfy the requirements of the plain view search doctrine. See *R v Spindloe*, 2001 SKCA 58 at para 36. Officers may also seize evidence in plain view when they arrest an individual in their dwelling house incidental to arrest. See e.g. *R v Stairs,* 2022 SCC 11 at para 23 [*Stairs*].

104. *Grunwald*, *supra* note 102 at paras 37–55; *Mitchell*, *supra* note 102 at para 109; *Wilson*, *supra* note 102 at paras 23–37, and accompanying cases; *Ceballos*, *supra* note 102 at paras 73–79.

105. Terry Skolnik, "Racial Profiling and the Perils of Ancillary Police Powers" (2021) 99:2 Can Bar Rev 429 at 434 [Skolnik, "Racial Profiling"].

106. *Ibid*; James Stribopoulos, "In *Search* of Dialogue: The Supreme Court, Police Powers and the *Charter*" (2005) 31:1 Queen's LJ 1 at 73–74 [Stribopoulos, "In Search of Dialogue"].

allows judges to craft new law enforcement powers to fill legislative gaps.[107] Today, many street-level police powers have been created by judges rather than by Parliament.[108] Examples include the police power to set up a roadblock, detain and search persons incidental to investigative detention, strip search individuals, and search persons, vehicles, and cellphones incidental to arrest, amongst others.[109]

Typically, scholars argue that these powers are objectionable for three reasons.[110] Some contend that these powers lack democratic legitimacy because they were created by judges who are nominated rather than democratically elected lawmakers.[111] Others note that, compared to courts, Parliament has better institutional competence to create police powers through the democratic process.[112] Others still argue that judicially created police powers contribute significantly to racial and social profiling.[113] They remark that judges have upheld police powers that can be exercised arbitrarily, and that fail to impose proper measures to promote law enforcement transparency and accountability.[114]

However, the fact that judges create certain police powers rather than lawmakers raises other objections that scholars typically overlook. More specifically, the judicial creation of police powers—and Parliament's reluctance to regulate investigative technologies—contributes to a one-way ratchet in criminal procedure.[115] In other words, courts have considerably expanded police powers in a manner that progressively limits constitutional rights.[116]

This current trend marks a significant shift from how criminal procedure initially developed following the *Charter*'s enactment and continuing

107. *Fleming*, *supra* note 21 at para 42.

108. Richard Jochelson, "Crossing the Rubicon: Of Sniffer Dogs, Justifications, and Preemptive Deference" (2008) 13:2 Rev Const Stud 209 at 212–19 [Jochelson, "Crossing the Rubicon"].

109 *Ibid*.

110. Skolnik, "Racial Profiling", *supra* note 105 at 430–31 (discussing the following objections and the accompanying footnotes).

111. Tim Quigley, "Brief Investigatory Detentions: A Critique of *R. v. Simpson*" (2004) 41:4 Alta L Rev 935 at 950.

112. Martin L Friedland, "Criminal Justice in Canada Revisited" (2004) 48:4 Crim LQ 419 at 446, 448–50.

113. Skolnik, "Racial Profiling", *supra* note 105 at 430–31.

114. *Ibid*.

115. Aziz Z Huq, "Fourth Amendment Gloss" (2018) 113:4 Nw UL Rev 701 at 739–40; Stuntz, "Pathological Politics", *supra* note 12 at 509. I first advanced this argument and this section's arguments in Owusu-Bempah et al, *supra* note 12, ch 7.

116. Skolnik, "Rééquilibrer le rôle", *supra* note 15 at 261, 277, 293.

into the 1990s.[117] During that time, the Supreme Court of Canada ruled that certain police powers were unconstitutional if they were exercised without a warrant.[118] Examples include warrantless arrests in dwelling houses, warrantlessly videotaping individuals within their dwelling houses, and installing tracking devices on persons or vehicles without a warrant.[119] Parliament responded accordingly and modified the *Criminal Code*.[120] Lawmakers created an entry warrant, a general warrant, and a tracking-device warrant.[121]

From the late 1990s onwards, the Supreme Court of Canada also created a litany of new police powers through the ancillary powers doctrine discussed above.[122] Between 2002 and 2017, for instance, the Supreme Court of Canada created a new police power in every case where the government argued that such a common law investigative power existed.[123]

Though the breadth of street-level police powers has expanded significantly within the past two decades, the scope of constitutional rights generally has not.[124] Consider two examples: search and seizure law and the law governing arbitrary detentions and imprisonment. Courts have recognized that police officers have the authority to warrantlessly search individuals, their vehicles, their cellphones, and parts of their home incidental to arrest.[125] Officers can strip search individuals or take a penile swab incidental to arrest

117. Alexandre Boucher, François Lacasse & Thierry Nadon, "La création de la détention pour enquête en common law : dérive jurisprudentielle ou évolution nécessaire ? Un point de vue pragmatique" (2009) 50:3/4 C de D 771 at 795–96.

118. Quigley, "The Impact of the Charter", *supra* note 48 at 126–28.

119. See e.g. *Feeney*, *supra* note 43; *R v Wong*, 1990 CanLII 56 (SCC) [*Wong*]; *R v Wise*, 1992 CanLII 125 (SCC) [*Wise*].

120. *Criminal Code*, RSC 1985, c C-46; Stribopoulos, "The Limits of Judicially Created Police Powers", *supra* note 13 at 316–17 (discussing 1990s amendments to the *Criminal Code*).

121. See *An Act to Amend the Criminal Code and the Interpretation Act* (*powers to arrest and enter dwellings*), SC 1997, c 39, s 2 (creating a warrant to enter a dwelling-house to effect an arrest); *An Act to Amend the Criminal Code, the Crown Liability and Proceedings Act and the Radiocommunication Act*, SC 1993, c 40, s 15 (creating a general warrant to authorize the use of any investigative technique); and *ibid*, s 18 (creating a warrant to place electronic tracking devices on vehicles).

122. Terry Skolnik & Vanessa MacDonnell, "Policing Arbitrariness: *Fleming v. Ontario* and the Ancillary Powers Doctrine" (2021) 100 SCLR (2d) 187 at 187, 192–94.

123. Richard Jochelson et al, "Generation and Deployment of Common Law Police Powers by Canadian Courts and the Double-Edged Charter" (2020) 28:1 Crit Criminol 107 at 116.

124. Skolnik, "Rééquilibrer le rôle", *supra* note 15 at 285.

125. *Cloutier*, *supra* note 82 at 182, 185, 187; *Caslake*, *supra* note 82 at paras 3, 15; *Fearon*, *supra* note 67; *Stairs*, *supra* note 103 at para 23.

without a warrant in either case.[126] They can use undercover officers to ensnare suspects in a ruse and trick them into abandoning their DNA.[127] Officers can also informally question individuals or ask them for identification without informing them of their rights.[128] They can lawfully pull over vehicles at random, set up roadblocks, and identify and question drivers and passengers, all without having to inform individuals of their constitutional rights.[129] These examples illustrate how the growth of police powers erode the section 8 and 9 constitutional rights to be free from unreasonable searches and seizures and to be free from arbitrary detentions and imprisonment.

The same is true for other constitutional rights that apply to police investigations. Consider how the right to counsel evolved during the 1980s and 1990s. Initially, the Supreme Court of Canada recognized that police officers have the constitutional duty to inform detained and arrested persons of their right to counsel and to provide them with certain information.[130] The Court affirmed a police duty to abstain from questioning defendants until they contact their lawyer and confirmed officers' duty to implement the right to counsel.[131]

But since then, the scope of the constitutional right to counsel has evolved little. The Supreme Court of Canada has rejected a constitutional right to have a lawyer present during police interrogations.[132] Many courts reject a constitutional right to contact counsel from one's cellphone, and officers have no duty to provide their own cellphones to detained or arrested persons so that they can call their lawyer.[133] In one pertinent case, the Court ruled that the defendant's confession remained free and voluntary despite having asserted their right to silence eighteen times during an interrogation.[134] Although constitutional criminal procedure produces a one-way ratchet that expands police power and restricts individual rights, technology worsens this trend.

---

126. *Golden*, *supra* note 36; *R v Saeed*, 2016 SCC 24 [*Saeed*].

127. *D'Amico*, *supra* note 75 at paras 321, 391; *Delaa*, *supra* note 77 at para 19.

128. *R v Suberu*, 2009 SCC 33 at paras 28–29 [*Suberu*]. See also *Grant*, *supra* note 32 at para 47; Jennifer Woollcombe, "*Grant, Suberu* and *Harrison*: Detention, the Right to Counsel and a New Analysis under Section 24(2): Some Practical Impacts" (2010) 51 SCLR (2d) 479 at 484.

129. *Ladouceur*, *supra* note 51; *R v Humphrey*, 2011 ONSC 3024 at para 130; *R v Robertson*, 2018 ABQB 658 at paras 58–65; *Dedman v The Queen*, 1985 CanLII 41 (SCC).

130. *Manninen*, *supra* note 31 at para 21.

131. *Ibid* at para 23; *R v Evans*, [1991] 1 SCR at 869 at 890, 1991 CanLII 98 (SCC).

132. *R v Sinclair*, 2010 SCC 35.

133. See e.g. *R v Montgomery*, 2009 BCCA 41. For the opposite conclusion, see *R v Landry*, 2020 NBCA 72. For a decision holding that officers have no duty to provide their own cellphones to defendants upon detention or arrest, see *R v Taylor*, 2014 SCC 50.

134. *R v Singh*, 2007 SCC 48 at paras 13, 53.

IV. How Technology Worsens Criminal Procedure's One-Way Ratchet

Two interrelated phenomena help explain why technology exacerbates criminal procedure's one-way ratchet tendency: legislative inertia and slippery slopes. Consider legislative inertia first. As discussed above, within the past twenty years, Parliament rarely legislates new police powers, codifies existing ones, or regulates emerging technologies.[135] There are various reasons for this. For one, since courts increasingly create police powers rather than Parliament, there is little incentive for lawmakers to legislate in this area.[136] The force of precedent—and its capacity to create path dependency—reinforces this dynamic.[137] The Supreme Court of Canada understands that lawmakers rarely enact new investigative powers, and lawmakers grasp that the Supreme Court is the primary institution that creates them instead.[138] Each new judicially created police power further legitimizes the ancillary powers doctrine and justifies the judicial creation of police powers in future cases.[139]

Lawmakers may also be reluctant to create new police powers because it can be politically costly.[140] Politicians are self-interested in certain respects.[141] They seek re-election and may favour the enactment of laws and policies that achieve this aim.[142] Insofar as crime control is a winning electoral strategy, lawmakers may be reluctant to rein in police powers too significantly, especially if they risk being portrayed as soft on crime.[143] Paradoxically, lawmakers can also be accused of overreaching if they create new police powers that are too intrusive.[144] They may experience major political

135. Skolnik, "Racial Profiling", *supra* note 105 at 430–31.

136. Stribopoulos, "In Search of Dialogue", *supra* note 106 at 34.

137. Skolnik, "Racial Profiling", *supra* note 105 at 430–31; Oona A Hathaway, "Path Dependence in the Law: The Course and Pattern of Legal Change in a Common Law System" (2001) 86:2 Iowa L Rev 601 at 605 [Hathaway, "Legal Change in a Common Law System"].

138. Skolnik, "Racial Profiling", *supra* note 105 at 456.

139. *Ibid*.

140. *Ibid*.

141. Cass R Sunstein, "The Most Knowledgeable Branch" (2016) 164:7 U Pa L Rev 1607 at 1617 [Sunstein, "The Most Knowledgeable Branch"].

142. *Ibid*.

143. Don Stuart, "The Charter Balance against Unscrupulous Law and Order Politics" (2012) 57 SCLR (2d) 13 at 13.

144. Pollyanna Sanderson, "Balancing Public Health and Civil Liberties: Privacy Aspects of Contact-Tracing Technologies" (2021) 19:4 IEEE Security & Privacy 65 at 66.

blowback if they attempt to enact police powers that are associated with mass surveillance, invasiveness, or authoritarianism.[145] The judicial creation of police powers is a win-win for lawmakers because it avoids this problem. When courts create police powers rather than legislators, lawmakers bear none of the political costs associated with legislating too mildly or too aggressively.

There is another reason why lawmakers may be disincentivized from regulating new investigative technologies: secret technologies are more effective.[146] Police officers seek a first-mover advantage. The police are more effective when criminals do not understand how they can be caught.[147] Secrecy maximizes law enforcement's capabilities. Criminals shift their behaviour to avoid detection; secrecy prevents that shift. Regulatory vacuums maximize law enforcement's effectiveness by deploying technology clandestinely and opaquely.[148]

Legislative inertia within criminal procedure is bad in various respects. Courts may lack the necessary institutional competence to regulate certain technologies adequately.[149] Compared to other branches of government, judges lack the information-gathering capacities that the legislative and executive branches possess.[150] When Parliament enacts laws, the bills go through specialized committees and sub-committees, appeal to professional expertise, are subject to democratic debate, and incorporate public commentary throughout the legislative process.[151] The executive branch collaborates with stakeholders, interacts through notice and comment procedures, and proactively seeks out technocratic and bureaucratic expertise.[152] The judicial creation of police powers, on the other hand, involves none of these democratic processes.[153]

The judiciary's lack of institutional competence to control emerging investigative technologies produces negative consequences. Courts have authorized certain routine street-level police powers—such as random traffic

145. Benjamin J Goold, "How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy" in DW Schartum, ed, *Surveillance in a Constitutional Government* (Bergen: Fagbokforlaget, 2010) 38 at 46.

146. *Ibid* at 38; Manes, *supra* note 5 at 507.

147. Andrew Guthrie Ferguson, "Surveillance and the Tyrant Test" (2021) 110:2 Geo LJ 205 at 218 [Ferguson, "Surveillance and the Tyrant Test"].

148. *Ibid*.

149. Orin S Kerr, "The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution" (2004) 102:5 Mich L Rev 801 at 858–59 [Kerr, "The Fourth Amendment"].

150. Sunstein, "The Most Knowledgeable Branch", *supra* note 141.

151. Terry Skolnik, "Hot Bench: A Theory of Appellate Adjudication" (2020) 61:4 Boston College L Rev 1271 at 1306 [Skolnik, "Hot Bench"].

152. Sunstein, "The Most Knowledgeable Branch", *supra* note 141 at 1620–21.

153. Skolnik, "Racial Profiling", *supra* note 105 at 456.

stops and stop-and-frisk—that lack transparency, do not impose oversight mechanisms, and do not require police officers to gather data on how these powers are used.[154] Due to this shortcoming, these powers have been disproportionately exercised against Indigenous and racialized persons.[155] Even when courts have attempted to regulate some new technology—for instance, with warrantless cellphone searches incident to arrest—judges failed to impose basic oversight measures.[156] For instance, when the Supreme Court of Canada created that power, it did not impose a duty on police officers to inform defendants that their cellphone was searched.[157] Defendants—especially intoxicated ones—may not realize that officers searched their phones and cannot challenge the constitutionality of that action.[158] Given technology's rapid evolution and the disparate impact of algorithmic decision-making on racialized persons, legislative inertia poses important risks for civil rights.

The second phenomenon that contributes to criminal procedure's one-way ratchet tendency—and that technology exacerbates—is slippery slopes. A slippery slope occurs when judges initially reject an outcome perceived as extreme or dangerous, yet the cumulative effects of incremental decisions produce that same outcome over time.[159] In other words, the gulf between decisions *A* and *D* may be extreme.[160] Yet, outcome *D* appears less extreme when the law incrementally expands *A*'s application to *B,* and *B*'s application to *C*, and then *C*'s application to *D*.[161] Through this process, outcome *D* is construed as no more than an incremental expansion of the law, even though it would be seen as a drastic departure from outcome *A*.[162]

Criminal procedure is unique in that it produces unidirectional slippery slopes. As discussed above, constitutional rights do not generally expand to produce extreme outcomes over time; police powers do. Many constitutional rights progressively contract rather than expand. As discussed above, the evolution of search and seizure law, the law governing arbitrary detentions, and the right to counsel are examples.

154. *Ibid* at 430, 448, 451.

155. *Ibid* at 436–38. See e.g. Terry Skolnik & Fernando Belton, "*Luamba* et la fin des interceptions routières aléatoires" (2023) 101 RB Can 671.

156. Skolnik, "Racial Profiling", *supra* note 105 at 452, citing Terry Skolnik, "Improving the Current Law of Warrantless Cellphone Searches After *R v Fearon*" (2015) 49:3 RJTUM 825 at 830–31.

157. *Ibid*.

158. *Ibid*.

159. Eugene Volokh, "The Mechanisms of the Slippery Slope" (2003) 116:4 Harv L Rev 1026 at 1100–01.

160. *Ibid*.

161. *Ibid*.

162. *Ibid*.

Police powers produce the opposite tendency, and their scope tends to broaden incrementally. To illustrate this point, consider the common law's expansion of the power to search incidental to arrest. Initially, courts recognized that police officers can lawfully search a person who is placed under arrest.[163] That power was later extended to cover searches incidental to arrest of a person's vehicle, cellphone, and home.[164] Despite the common law's aversion to invasive personal search and the seizure of bodily samples, courts incrementally authorized officers to strip search defendants and take penile swabs without a warrant.[165] The gulf between searching a person incidental to arrest and a penile swab incidental to arrest would have been construed as judicial maximalism and a major departure from precedent. Yet, the legal distance between authorizing strip searches incidental to arrest and authorizing penile swabs incidental to arrest was not.

Investigative technologies contribute to similar slippery slopes. Recall how courts affirmed a police power to ask individuals preliminary questions without informing them of their constitutional rights, including requests for identification.[166] Courts subsequently decided that officers can query individuals', drivers', and passengers' identities in police databases—the content of which individuals lack a reasonable expectation of privacy.[167] Although cellphones attract very strong expectations of privacy, courts eventually permitted warrantless cellphone searches incidental to arrest.[168] As discussed more below, automated licence plate recognition, commercial DNA database searches, and facial recognition software represent the next potential phase of criminal procedure's slippery slope. These concerns, in turn, justify a new approach to protecting individuals' privacy against mass-surveillance technologies—one that restores constitutional dialogue, discourages legislative inertia, and reduces the likelihood of slippery slopes in criminal procedure.

V. Emerging Technologies and the Need for Oversight

Increasingly, emerging investigative technologies combine the two policing strategies discussed above. The following subsections show how these technologies attempt to change the normative quality of information gathering and the normative quality of information from private to public. They do so to exploit weak points in criminal procedure and to circumvent constitutional norms. These technologies are automated licence plate recognition (ALPR),

163. *Cloutier*, *supra* note 82 at 187.

164. *Caslake*, *supra* note 82 at para 15; *Fearon*, *supra* note 67; *Stairs*, *supra* note 103 at para 23.

165. *Golden*, *supra* note 36; *Saeed*, *supra* note 126.

166. *Suberu*, *supra* note 128 at paras 28–29. See also *Grant*, *supra* note 32 at para 47.

167. Penney, "Driving While Innocent", *supra* note 56 at 355.

168. *Fearon*, *supra* note 67; *R v Vu*, 2013 SCC 60 at para 63.

commercial DNA database searches, and automated facial recognition (AFR). These investigative methods raise significant concerns regarding discriminatory policing tactics, secrecy, invasions of privacy, and slippery slopes—all of which militate in favour of proper legislative and judicial oversight of these technologies.

A. Automated Licence Plate Recognition

Begin with automated licence plate recognition (ALPR). ALPR can be installed in a fixed location—for instance, on a pole at a roadway intersection—or can be portable—for example, mounted onto a police vehicle.[169] ALPR can verify up to 5,000 licence plates per hour and offer a wealth of information to law enforcement.[170] Some readers also capture an image of the driver.[171] The technology automatically scans licence plates and identifies whether the vehicle or its owner are on a hotlist.[172] Typically, a hotlist comprises a list of vehicles that are stolen, under investigation, or have a suspended or expired licence plate or registration.[173] Hotlists can also indicate whether the vehicle's owner is sought by warrant, prohibited from driving, or under criminal investigation.[174] Since ALPR can produce errors (more on this below), officers must then confirm that the vehicle or person identified in the hotlist matches the vehicle or person captured by the ALPR.[175] To do so, officers can manually verify the vehicle or driver's information in a police database.[176]

Automated licence plate recognition is useful for various reasons. For one, ALPR promotes investigative efficiency. Officers can only manually investigate a certain number of vehicles at the same time. And they can only query the licence plates that they see. The time that officers spend manually

169. Hannah Bloch-Wehba, "Visible Policing: Technology, Transparency, and Democratic Control" (2021) 109:3 Cal L Rev 917 at 919 [Bloch-Wehba, "Visible Policing"].

170. Information and Privacy Commissioner of Ontario (IPCO), "Guidance on the Use of Automated License Plate Recognition Systems by Police Services" (Toronto: Government of Ontario, 2017) at 12; Ottawa Police Service, "Automated License Plate Recognition" (last visited 2021) online: <ottawapolice.ca> [perma.cc/L65P-3WB9].

171. Julia M Brooks, "Drawing the Lines: Regulation of Automatic License Plate Readers in Virginia" (2019) 25:3 Rich JL & Tech 1 at 3; Electronic Frontier Foundation (EFF), "Automated License Plate Readers" (28 August 2017), online: <eff.org> [perma.cc/3BS2-VN79].

172. Stephanie Foster, "Should the Use of Automated License Plate Readers Constitute a Search After *Carpenter v. United States*?" (2019) 97:1 Wash U L Rev 221 at 221.

173. IPCO, *supra* note 170 at 12; Meg Young, Michael Katell & PM Krafft, "Municipal surveillance regulation and algorithmic accountability" (2019) 6:2 Big Data & Society 1 at 5.

174. *Ibid*.

175. IPCO, *supra* note 170 at 12.

176. *Ibid*.

investigating one vehicle may come at the expense of a more revelatory search. Furthermore, ALPR serves as a vital screening tool for law enforcement. Suspended driver's licences, unpaid vehicle tags, driving prohibitions, and outstanding warrants all narrow the scope of potential targets for police officers.[177]

ALPR also raises significant concerns. For one, ALPR can be used to surveil individuals rather than for traffic safety purposes.[178] Automated licence plate readers store the date, time, and GPS location when a licence plate was scanned.[179] Law enforcement can aggregate the data to determine movement patterns or to actively surveil criminal suspects.[180] By analyzing this aggregated data, officers are able to determine, with significant accuracy, where individuals live, shop, and work.[181] Empirical evidence shows that police forces use ALPR for a multitude of purposes beyond traffic safety, such as counter-terrorism, investigating criminal suspects, detecting violent crimes or property offences, and monitoring gang-related activities.[182] By examining ALPR data, officers can determine which vehicles entered or exited a certain perimeter during a particular period.[183] If a crime was committed within that perimeter, officers can review the ALPR data to narrow the scope of potential suspects.[184] Some note that in response to such investigative tactics, individuals may alter their movements or not engage in certain activities, if they know or believe that they are being tracked.[185]

ALPR may also decrease public trust in law enforcement. Studies indicate that many individuals—up to ninety per cent of persons in some

177. Skolnik, "Two Criminal Justice Systems", *supra* note 9 at 299–302.

178. Elizabeth E Joh, "The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing" (2016) 10:1 Harvard L & Pol'y Rev 15 at 22 [Joh, "The New Surveillance Discretion"]; the authors refer to the term "re-invention" rather than ratcheting. See James J Willis, Christopher Koper & Cynthia Lum, "The Adaptation of License-plate Readers for Investigative Purposes: Police Technology and Innovation Re-invention" (2018) 35:4 Justice Q 614 at 631–33.

179. Joh, "The New Surveillance Discretion", *supra* note 178 at 22.

180. Foster, "Should the Use of Automated License Plate Readers", *supra* note 172 at 221.

181. *Ibid* at 227.

182. Cynthia Lum et al, *The Rapid Diffusion of License Plate Readers in U.S. Law Enforcement Agencies: A National Survey* (Fairfax, Va: George Mason University Center for Evidence-Based Crime Policy, 2016) at 25; Christopher S Koper & Cynthia Lum, "The Impacts of Large-Scale License Plate Reader Deployment on Criminal Investigations" (2019) 22:3 Police Q 305 at 307.

183. Joh, "The New Surveillance Discretion", *supra* note 178 at 23–24.

184. *Ibid*.

185. IPCO, *supra* note 170 at 3; Andrew G Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York: New York University Press, 2017) at 184.

studies—do not know whether their police service uses ALPR technology.[186] Some studies indicate that individuals are more distrustful of law enforcement that uses ALPR and retains its associated data for long time periods.[187] Yet, this trust is crucial because the criminal justice system requires the public's assistance to report, detect, prevent, and prosecute crimes.[188] Highly-invasive uses of ALPR may be counterproductive by discouraging that cooperation.[189]

Beyond surveillance-related preoccupations, ALPR also generates broader privacy concerns. In some contexts, information gathered by ALPR —including photographs of drivers—have been successfully hacked, resulting in major privacy breaches.[190] ALPR can have significant security vulnerabilities, rendering them susceptible to being hacked or hijacked.[191] Security researchers have documented that some ALPR can be accessed relatively easily, while others have default passwords provided in their technical support guides.[192]

ALPR is minimally regulated despite its capacity to track individuals. To date, provincial privacy commissioner reports are the primary source that recommend how the technology should be used and how its data should be retained.[193] Few judicial decisions provide meaningful constitutional oversight over ALPR, other than to state that officers must manually confirm that the technology accurately identified the relevant licence plate, and that the Crown must deposit ALPR images into evidence.[194] No *Criminal Code* provisions directly govern the technology's use.

---

186. Linda M Merola, Cynthia Lum & Ryan P Murphy, "The Impact of License Plate Recognition Technology (LPR) on Trust in Law Enforcement: A Survey-Experiment" (2019) 15 J Experimental Criminology 55 at 62.

187. *Ibid* at 63.

188. Tom R Tyler, Phillip Atiba Goff & Robert J MacCoun, "The Impact of Psychological Science on Policing in the United States: Procedural Justice, Legitimacy, and Effective Law Enforcement" (2015) 16:3 Psychological Science in Public Interest 75 at 85.

189. Merola, *supra* note 186 at 63.

190. Catharine Tunney, "CBSA launches investigation after licence plate reader linked to U.S. hack", *CBC News* (12 June 2019), online: <cbc.ca> [perma.cc/H3E4-8M7C]; Zolan Kanno-Youngs & David E Sanger, "Border Agency's Images of Travelers Stolen in Hack", *The New York Times* (10 June 2019), online: <nytimes.com> [perma.cc/D4VQ-6UFS].

191. Zack Whittaker, "Police license plate readers are still exposed on the internet", *TechCrunch* (22 January 2019), online: <techcrunch.com> [perma.cc/AF92-76J7].

192. *Ibid*.

193. Elizabeth Denham, *Use of Automated Licence Plate Recognition Technology by the Victoria Police Department* (Victoria: Office of the Information and Privacy Commissioner for British Columbia, 2012); IPCO, *supra* note 170.

194. *Ville de Montréal c Philibert*, 2020 QCCM 125 at paras 55–71; *Ville de Laval c Fokou*, 2021 QCCM 83 at paras 9–14; *Ville de Montréal c Kaoukji*, 2020 QCCM 129 at paras 17–25.

ALPR is pernicious because it can potentially bypass constitutional norms. Courts have decided that police officers require a warrant to track vehicles or individuals.[195] Officers must request a production order to obtain cell-phone data in the possession of third parties—such as GPS information held by telecommunications companies—which discloses an individual's past movements.[196] Or, if officers wish to search an individual's phone to access previous GPS data, that too requires a warrant.[197] Yet, officers may secretly use ALPR to gather an individual's past location data—or track them in real time—without any warrant whatsoever.

Notice how ALPR deploys the two strategies discussed above.[198] First, much like manual licence plate verifications, ALPR accesses information indirectly through police databases rather than directly through defendants. Second, certain uses of ALPRs convert the private nature of information into public information. The technology can document a person's movements, which normally attract a reasonable expectation of privacy.[199] However, the technology also captures a person's licence plate in a public place much like a security camera or physical surveillance, such that individuals may have no reasonable expectation of privacy over that data.[200] Indeed, some courts have determined that the data captured by ALPR does not trigger a reasonable expectation of privacy, since licence plates are publicly visible and could be queried by police officers.[201] Courts have also recognized that compared to individuals, the state can more justifiably surveil vehicles because driving is a highly regulated activity that can endanger others' lives.[202] ALPR exemplifies a slippery slope in criminal procedure that can expand police powers and may evade constitutional norms.

---

195. *Wise*, *supra* note 119 at 538.

196. See *Criminal Code*, *supra* note 120, s 487.017; Colton Fehr, "Criminal Law and Digital Technologies: An Institutional Approach to Rule Creation in a Rapidly Advancing and Complex Setting" (2019) 65:1 McGill LJ 67 at 88 [Fehr, "Criminal Law and Digital Technologies: An Institutional Approach"].

197. *Criminal Code*, *supra* note 120, s 487; *R v TI*, 2021 ONSC 2608 at paras 56–61.

198. Elizabeth E Joh, "Discretionless Policing: Technology and the Fourth Amendment" (2007) 95:1 Cal L Rev 199 at 227 (advancing a similar argument).

199. *Wise*, *supra* note 119 at 538–39; Fehr, "Criminal Law and Digital Technologies: An Institutional Approach", *supra* note 196 at 78, 86.

200. Robert W Hubbard, Susan Magotiaux & Matthew Sullivan, "The State Use of Closed-Circuit TV: Is There a Reasonable Expectation of Privacy in Public?" (2004) 49:2 Crim LQ 222 at 224–30.

201. *An Application for a General Warrant, s. 487.01 and a Sealing Order, s. 487.3*, 2020 MBPC 62 at paras 24–25.

202. *Wise*, *supra* note 119 at 538–39.

B. Commercial DNA Database Searches

Second, commercial DNA database searches may also give rise to a slippery slope in criminal procedure that weakens constitutional rights. Law enforcement increasingly uses commercial DNA databases to identify suspects in the following way.[203] Officers upload crime scene DNA to a commercially available DNA database, such as GEDmatch.[204] Investigators then verify whether the crime scene DNA sample matches that of another individual who voluntarily submitted their DNA to the database.[205] Where there is a positive match, investigators work with a genealogist to construct a family tree of the individual who produced that match.[206] The investigators then narrow down their family members by age, gender, location, and proximity to the crime scene to determine which of them is a potential suspect.[207]

Commercial database searches carry certain advantages. These searches have helped police officers identify suspects in high-profile crimes—especially homicides and sexual assaults—that had gone unsolved for years.[208] They have been used to exonerate individuals who were wrongfully convicted of crimes.[209] These commercial databases can also help officers identify human remains.[210]

But these databases also raise various concerns. For one, some commercial database searches have led to false positives, which resulted in innocent persons being mistakenly identified as suspects and interrogated by police officers.[211] Individuals may suffer significant stress—and reputational

203. Evan Frohman, "23PolicemenAndMe: Analyzing the Constitutional Implications of Police Use of Commercial DNA Databases" (2020) 22:5 U Pa J Const L 1495 at 1495–96.

204. Hannah Parman, "The Thickness of Blood: Article I, Section 7, Law Enforcement, and Commercial DNA Databases" (2020) 95:4 Wash L Rev 2057 at 2058–59.

205. Nina F de Groot, Britta C van Beers & Gerben Meynen, "Commercial DNA Tests and Police Investigations: A Broad Bioethical Perspective" (2021) 47 J Medical Ethics 788 at 788–89.

206. *Ibid*; Patrick White, "Genetic Genealogy Helps Toronto Police Crack Landmark 1984 Christine Jessop Cold Case in Ontario", *The Globe and Mail* (16 October 2020), online: <theglobeandmail.com> [perma.cc/364G-XD8W].

207. *Ibid*.

208. Rebecca Gold, "From Swabs to Handcuffs: How Commercial DNA Services Can Expose You to Criminal Charges" (2019) 55:2 Cal WL Rev 491 at 498–500; White, *supra* note 206..

209. Virginia Hughes, "Two New Laws Restrict Police Use of DNA Search Method", *The New York Times* (31 May 2021), online: <nytimes.com> [perma.cc/K74Y-Q4E5]; Heather Murphy, "The Jury Said He Killed Her Daughter. She Helped Clear His Name.", *The New York Times* (18 June 2019), online: <nytimes.com> [perma.cc/9YQQ-LJD6].

210. Hughes, *supra* note 209.

211. Frohman, *supra* note 203 at 1512–13.

harm—while they wait to be cleared as a suspect.[212] Furthermore, laws and policies minimally regulate the use and retention of information that is gathered as part of a commercial database analysis.[213] There is little transparency regarding the type of information that officers gather from such searches and who is investigated, which also reduces police accountability.[214] Commercial database searches were initially used for the most serious crimes, such as homicides.[215] Yet, they have more recently been used to solve lower-level offences, such as assaults.[216] This expansion risks normalizing the use of commercial database searches, especially where there is insufficient judicial or legislative oversight.[217]

Commercial DNA database searches can circumvent constitutional norms that protect individuals against the seizure and analysis of their bodily substances. Constitutional law recognizes that a person's body—including their bodily substances—attracts one of the strongest expectations of privacy.[218] Courts have decided that the seizure of bodily substances can violate one's interests in bodily integrity, privacy, human dignity, and autonomy.[219] Several early *Charter* decisions involved the unlawful search and seizure of bodily substances.[220] Courts decided that police officers required warrants to seize blood samples, take dental impressions, remove a person's hair for DNA analysis, and so on.[221] In cases where officers seized this type of evidence without a warrant and without the defendant's consent, the Supreme Court of Canada judged these constitutional violations as particularly serious and excluded the evidence.[222] These earlier decisions sent a relatively strong message to police officers: if an individual's bodily substances are seized without a warrant, there is a very strong chance that the evidence will be excluded at trial.

---

212. Christi J Guerrini et al, "Four misconceptions about investigative genetic genealogy" (2021) 8:1 J L & Biosciences 1 at 11.

213. Rana Muhammad Mateen et al, "Familial DNA analysis and criminal investigation: Usage, downsides and privacy concerns" (2021) 318 Forensic Science Intl 1 at 4.

214. Erin Murphy, "Law and policy oversight of familial searches in recreational genealogy databases" (2018) 292 Forensic Science Intl e5 at e7.

215. De Groot, van Beers & Meynen, *supra* note 205 at 793–794.

216. *Ibid*.

217. *Ibid*; Erin Murphy & Jun Tong, "The Racial Composition of Forensic DNA Databases" (2020) 108 Cal L Rev 1847 at 1908–09.

218. *Stillman*, *supra* note 67 at 639–40.

219. *Ibid* at 643–44.

220. *Ibid*; *Dyment*, *supra* note 74.

221. *Stillman*, *supra* note 67; *Dyment*, *supra* note 74.

222. *Stillman*, *supra* note 67.

But commercial DNA databank searches skirt these same constitutional norms that typically protect defendants. For law enforcement, commercial databank searches are valuable because they leverage the doctrines of abandonment and waiver to diminish the defendant's reasonable expectation of privacy. First, defendants lose their reasonable expectation of privacy over their own DNA that they abandon at a crime scene.[223] Second, defendants also lack a reasonable expectation of privacy over their family member's decision to voluntarily provide a DNA sample to a commercial databank, an act that resembles a waiver over certain usages of one's DNA.[224]

Much like how police database searches circumvent constitutional norms by acquiring data indirectly from computers rather than directly from individuals, commercial database searches indirectly gather information from relatives who consent to DNA samples rather than directly from suspects.

Some courts have upheld the constitutionality of warrantless public DNA database searches based on similar considerations. In *R v Wright*, the defendant was charged with second degree murder.[225] Police officers uploaded DNA that was found under the victim's fingernails to a public DNA database that was used by genealogy enthusiasts.[226] Officers aimed to match the defendant's DNA with relatives that had potentially uploaded their own DNA to the database.[227] This technique produced a match.[228] As a result, the officers established the relevant individuals' family tree using information that was publicly available, and interviewed members of that family.[229] They narrowed the scope of the investigation to the defendant and some of his family members.[230] Officers subsequently gathered discarded DNA from these individuals, the results of which could not exclude them as suspects.[231] The officers then obtained warrants to obtain a DNA sample from the defendant, which produced a match with the discarded DNA.[232] The officers later arrested

223. Amy Conroy, "Combining Familial Searching and Abandoned DNA: Potential Privacy Outcomes and the Future of Canada's National DNA Data Bank" (2014) 12:2 CJLT 171 at 179.

224. See e.g. Meghan McLoughlin, "Solving Crimes with 23andMe: DNA Databases and the Future of Law Enforcement" (2021) 34:3 J Civ Rights & Econ Development 317 at 342. Although McLoughlin analyzes the legal context in American law, similar justifications apply in Canadian law.

225. 2022 ONSC 6756 [*Wright*].

226. *Ibid* at para 1.

227. *Ibid*.

228. *Ibid* at para 2.

229. *Ibid*.

230. *Ibid* at paras 2–3.

231. *Ibid* at paras 3–4.

232. *Ibid*.

the defendant and obtained a warrant to take his fingerprints.[233] His fingerprint matched the fingerprint found on the crime scene.[234]

The Court concluded that the warrantless DNA database search was lawful.[235] In the Court's view, the defendant lacked a reasonable expectation of privacy over the information contained in the public database, and lacked standing to challenge the search's constitutionality.[236] The Court noted that the defendant provided no evidence that he had a subjective expectation of privacy over genetic markers that he shared with other individuals and that they uploaded to the database.[237] Moreover, the Court decided that individuals who uploaded their DNA to the public database lacked a similar expectation of privacy because their goal was to find other individuals with whom their genetic profile matched.[238]

C. Automated Facial Recognition

Third, automated facial recognition (AFR) also circumvents constitutional rights. Police forces tend to employ facial recognition technology in two main contexts: "face surveillance" and "face identification". The term face surveillance implies that a camera in a public location captures an individual's face, measures its features and geometric quality, and compares it to pictures or videos of faces contained within a database.[239] The technology can capture and store images for use in subsequent criminal investigations.[240] Face surveillance has been used in a variety of public locations: streets, public squares, parks, sports stadiums, and more.[241] The cameras capture individuals' faces, irrespective of whether they are suspected of wrongdoing.[242] Face identification, on the other hand, is used to identify suspects or persons of interest whose faces were captured by a camera, such as a surveillance camera or cellphone camera.[243] Like face surveillance,

233. *Ibid* at paras 4–5.

234. *Ibid*.

235. *Ibid* at paras 39–41.

236. *Ibid*.

237. *Ibid* at paras 17–20.

238. *Ibid* at paras 39–41.

239. Andrew Guthrie Ferguson, "Facial Recognition and the Fourth Amendment" (2021) 105:3 Minn L Rev 1105 at 1116 [Ferguson, "Facial Recognition"].

240. *Ibid*.

241. Pete Fussey, Bethan Davies & Martin Innes, "'Assisted' Facial Recognition and the Reinvention of Suspicion and Discretion in Digital Policing" (2021) 61:2 Brit J Crim 325 at 331.

242. Ferguson, "Facial Recognition", *supra* note 239 at 1116–18.

243. *Ibid* at 1119–20. The author also uses the term "face identification".

face identification also compares the geometry of a person's face captured by AFR to images of persons contained within a database.[244] Facial recognition databases can contain governmental images—such as health card or driver's licence photos—as well as images scraped from publicly accessible websites —such as social media accounts, professional profiles on an employer's website, or photographs in media.[245] Both governments and private entities establish facial image databases, and the latter may share these databases with the former.[246]

Beyond its privacy implications, facial recognition technology raises other fundamental concerns. For one, AFR can result in biased and discriminatory outcomes.[247] Numerous studies highlight how facial recognition technology results in higher false-positive rates for racialized persons than for white persons—a reality that exacerbates existing discrimination in the criminal justice system.[248] These studies also show that females, elderly persons, and children produce a disproportionate number of false positives.[249] Furthermore, facial recognition technology can produce errors.[250] Individuals have been wrongfully arrested and needlessly subjected to police use of force due to false positives associated with AFR.[251] Certain climatic conditions may also increase error rates.[252] Lastly, facial recognition technology has been

244. *Ibid*.

245. *Ibid* at 1116–19.

246. Elizabeth E Joh, "Policing the Smart City" (2019) 15:2 Intl JL in Context 177 at 179.

247. Peter NK Schuetz, "Fly in the Face of Bias: Algorithmic Bias in Law Enforcement's Facial Recognition Technology and the Need for an Adaptive Legal Framework" (2021) 39:1 Minn JL & Inequality 221 at 222–29.

248. Jacqueline Cavazos et al, "Accuracy Comparison Across Face Recognition Algorithms: Where Are We on Measuring Race Bias?" (2021) 3:1 IEEE Transactions on Biometrics, Behaviour, and Identity Science 101 at 103; Mary D Fan, *Camera Power: Proof, Policing, Privacy, and Audiovisual Big Data* (Cambridge, UK: Cambridge University Press, 2019) at 154.

249. Patrick Grother, Mei Ngan & Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (Washington, DC: National Institute of Standards and Technology, 2019) at 6–8.

250. Steve Lohr, "Facial Recognition Technology is Accurate, if You're a White Guy", *The New York Times* (9 February 2018), online: <nytimes.com> [perma.cc/8V3X-6352].

251. Gabrielle M Haddad, "Confronting the Biased Algorithm: The Danger of Admitting Facial Recognition Technology Results in the Courtroom" (2021) 23:4 Vanderbilt J Entertainment & Tech L 891 at 892–93.

252. Shawn Singh, "Algorithmic Policing Technologies in Canada" (2021) 44:6 Man LJ 246 at 272–73.

used by law enforcement clandestinely.[253] Following access to information requests, journalists discovered that Canadian police services secretly used facial recognition technology to identify suspects in numerous criminal investigations.[254] Certain police forces initially denied using facial recognition technology but subsequently admitted that they had used it.[255]

The cumulative effect of the two strategies discussed above—changing the normative quality of information and of information gathering—explain why AFR can circumvent constitutional norms. First, AFR changes the normative quality of biometric information by capturing the image of a person's face in public rather than in private.[256] Recall how, in certain contexts, individuals lack a reasonable expectation of privacy over images captured in public places, such as security camera footage or photographs taken by a police surveillance team.[257] The problem is that courts may determine that the act of taking a person's picture on public property does not violate section 8 of the *Charter*. Second, AFR then modifies the normative quality of information gathering by comparing the image that was captured in public to information contained in a database.[258] However, information contained within a police database does not give rise to a reasonable expectation of privacy.[259] For this reason, courts may decide that individuals lack a reasonable expectation of privacy when a camera captures a person's image in public and compares it with non-private information contained in a police database.

* * *

The three investigative technologies discussed above—automated licence plate readers, commercial DNA databank searches, and automated facial recognition software—all risk circumventing constitutional norms in similar ways. These technologies attempt to change the normative quality of information gathering and to modify the normative quality of information from private to public, both of which decrease reasonable expectations of privacy. And they leverage permissive criminal procedure doctrines to make

253. *Joint investigation of Clearview AI, Inc by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta*, 2021 CanLII 9227 (PCC).

254. Brockbank, *supra* note 7.

255. *Ibid*; Kate Robertson, Cynthia Khoo & Yolanda Song, *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada* (Toronto: Citizen Lab, 2020) at 63.

256. Mariko Hirose, "Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology" (2017) 49:5 Conn L Rev 1591 at 1595.

257. Hubbard, Magotiaux & Sullivan, *supra* note 200 at 224–30.

258. Ferguson, "Facial Recognition", *supra* note 239 at 1116–18.

259. Penney, "Driving While Innocent", *supra* note 56 at 355.

these strategies more effective, which both contributes to slippery slopes and exacerbates criminal procedure's one-way ratchet tendency.

The lack of legislative and judicial oversight of these technologies highlights a crucial shortcoming in constitutional criminal procedure and a commonality between these seemingly unrelated technologies. Currently, statutory law and constitutional criminal procedure fail to protect individuals adequately against mass-surveillance technologies. But this need not be the case. As discussed next, lawmakers and courts can regulate these technologies to better safeguard individuals' privacy, dignity, and equality.

VI. Investigative Technologies: Legislative and Judicial Oversight

A. Diminishing Reasonable Expectations of Privacy

Although criminal procedure functions as a one-way ratchet that expands police powers, technology also produces a one-way ratchet that incrementally diminishes privacy interests.[260] Individuals enjoy far less privacy today than they did previously, both in life and in law.[261] Surveillance cameras are present in many public spaces.[262] Companies routinely sell individuals' data to third parties.[263] Cellphones allow individuals to surreptitiously record audio or video, which can then be shared with the public.[264] Confidential conversations can be leaked into the public domain, and individuals cannot effectively control their disclosure.[265] As discussed above, the doctrines of

260. Jim Harper, "Reforming Fourth Amendment Privacy Doctrine" (2008) 57:5 Am UL Rev 1381 at 1382; Jerry Kang, "Cyberspace Privacy: A Primer and Proposal" (1999) 26:1 Hum Rts J 3 at 6; Douglas A Fretty, "Face-Recognition Surveillance: A Moment of Truth for Fourth Amendment Rights in Public Places" (2011) 16:3 Va JL & Tech 430 at 440.

261. Anita L Allen, "Coercing Privacy" (1999) 40:3 Wm & Mary L Rev 723 at 729–730; Shaun B Spencer, "Reasonable Expectations and the Erosion of Privacy" (2002) 39:3 San Diego L Rev 843 at 870–90 (noting the decline in privacy protections).

262. Benjamin Goold, Ian Loader & Angélica Thumala, "The Banality of Security: The Curious Case of Surveillance Cameras" (2013) 53:6 Brit J Crim 977 at 980.

263. Max N Helveston, "Reining in Commercial Exploitation of Consumer Data" (2019) 123:3 Penn St L Rev 667 at 668.

264. Tyler Finn, "Qualified Immunity Formalism: 'Clearly Established Law' and the Right to Record Police Activity" (2019) 119:2 Colum L Rev 445 at 446.

265. William E Scheuerman, "Digital Disobedience and the Law" (2016) 38:3 New Political Science 299 at 308–09.

abandonment, waiver, and plain view searches have all watered down the notion of reasonable expectations of privacy in law.

The incremental erosion of privacy, both in life and in law, generates perverse consequences within constitutional criminal procedure. Subjective and objective expectations of privacy shape one another.[266] As privacy norms continue to erode within society, individuals' subjective expectations of privacy may incrementally decrease as well.[267] Reduced subjective expectations of privacy that are widespread in society, in turn, diminish the reasonableness of an expectation of privacy.[268]

Part of the problem is that the threshold for reasonable expectations of privacy is constantly lowered by various forces. Certain privacy incursions may become normalized and expected within society.[269] Over time, individuals may no longer expect their information to remain private.[270] Furthermore, individuals may incrementally accept that law enforcement uses certain technologies that invade their privacy.[271] They may progressively lose a reasonable expectation of privacy that they once enjoyed.[272] In some circumstances, courts may conclude that individuals have no reasonable expectation of privacy regarding the use of technologies that are primitive and that do not initially disclose core biographical information.[273] However, these technologies may evolve rapidly or be used in new ways that courts did not anticipate.[274] Judges may fail to control these developments.[275] The force of precedent may discourage lower court

266. Matthew Tokson, "Knowledge and Fourth Amendment Privacy" (2016) 111:1 Nw UL Rev 139 at 139 [Tokson, "Knowledge"].

267. Teri Dobbins Baxter, "Low Expectations: How Changing Expectations of Privacy Can Erode Fourth Amendment Protection and a Proposed Solution" (2012) 84:3 Temp L Rev 599 at 610.

268. Tokson, "Knowledge", *supra* note 266 at 139; Matthew M Meacham, "The Perfect Storm: How Narrowing of the State Action Doctrine, Inconsistency in Fourth Amendment Caselaw, and Advancing Security Technologies Converge to Erode Our Privacy Rights" (2019) 55:3 Idaho L Rev 309 at 330.

269. Richard Sobel, Barry Horwitz & Gerald Jenkins, "Fourth Amendment Beyond *Katz*, *Kyllo* and *Jones*: Reinstating Justifiable Reliance as a More Secure Constitutional Standard for Privacy" (2013) 22:1 BU PILJ 1 at 20–21.

270. *Ibid*.

271. *Ibid* at 20–21, 23.

272. *Ibid*.

273. *Tessling*, *supra* note 41 at para 63.

274. Brian J Serr, "Great Expectations of Privacy: A New Model for Fourth Amendment Protection" (1988) 73:3 Minn L Rev 583 at 586–87.

275. *Ibid*.

judges from overturning precedents that authorized the relevant technology in previous cases.[276]

The increasing use of mass surveillance—and its progressive normalization within society—presents unique challenges for the doctrine of reasonable expectations of privacy in constitutional criminal procedure. The less we can protect our privacy, the less we can reasonably expect our privacy to be protected in certain cases.[277] Mass-surveillance technologies worsen this trend because individuals cannot generally opt out of a surveillance scheme that gathers information about them in public.[278] Immovability is one of real property's core features.[279] Individuals must use public property to travel from point *A* to point *B* to live their lives, make purchases, work, play, associate with others, and more.[280]

The problem is that innocent individuals can limit their freedom and bear high costs to attempt to opt out of technological mass-surveillance schemes (and these attempts may fail). Consider, for instance, how individuals altered their behaviour in response to more intense baggage-screening policies following the terrorist attacks of September 11th, 2001.[281] Economic studies show that a greater number of persons opted to drive rather than fly to avoid this screening, which resulted in increased vehicle traffic and more motor vehicle fatalities.[282] Yet, individuals may alter their routine behaviours in other ways. They may conceal their face to thwart facial recognition technology.[283] Or, they may take public transit so that ALPR does not track their vehicle's movements. In each of these contexts, individuals sacrifice their liberty to protect their privacy.

The gradual reduction of reasonable expectations of privacy, the inability to opt out of mass-surveillance schemes, and the need to trade-off freedom for privacy all militate in favour of stronger safeguards against mass-surveillance technologies within criminal procedure. The following section highlights how judges and lawmakers can provide such protection given their respective institutional competence.

---

276. Hathaway, "Legal Change in a Common Law System", *supra* note 137 at 605.

277. Baxter, *supra* note 267 at 610.

278. Lotte Houwing, "Stop the Creep of Biometric Surveillance Technology" (2020) 6:2 European Data Protection L Rev 174 at 174.

279. Arthur Ripstein, *Force and Freedom: Kant's Legal and Political Philosophy* (Cambridge, Mass: Harvard University Press, 2009) at 246.

280. *Ibid* at 246–48.

281. L Rush Atkinson, "The Bilateral Fourth Amendment and the Duties of Law-Abiding Persons" (2011) 99 Geo LJ 1517 at 1522–24.

282. *Ibid*, citing Garrick Blalock, Vrinda Kadiyali & Daniel H Simon, "Driving Fatalities After 9/11: A Hidden Cost of Terrorism" (2009) 41:14 Applied Econs 1717.

283. Meredith Van Natta et al, "The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic" (2020) 7:1 JL & Biosciences 1 at 11.

B. Mass-Surveillance Technologies and Institutional Competence

Together, courts and legislators can catalyze a new era of constitutional criminal procedure that better protects individuals against technologies that are used—or can be used—for mass surveillance. However, the legislative and judicial branches of government possess different levels of expertise, institutional competence, and information-gathering capacities.[284] The institutional competence of courts and lawmakers—and the institutional limitations of these branches of government—raise unique challenges for the regulation of mass-surveillance technologies.[285]

The institutional competence of courts and legislatures can be summarized as follows.[286] Begin with courts. Judges have difficulty crafting rules and establishing tests that govern new surveillance technologies because these technologies evolve rapidly.[287] Although courts may establish flexible tests to accommodate technological change, the malleability of these tests may provide inadequate guidance to lower courts, police officers, and individuals.[288] Judges may not understand the various ways in which emerging technologies impact privacy, and how these technologies can be deployed for new purposes that judges do not consider.[289] Furthermore, it may take years for courts to revisit a legal test that goes awry or generates unexpected negative consequences.[290] Apex courts must wait until a case that involves a surveillance technology winds its way through the appeals process to establish rules or tests that govern its

284. See e.g. Colton Fehr, "Digital Evidence and the Adversarial System" (2016) 16:2 CJLT 437 at 439–42 [Fehr, "Digital Evidence"]; Kerr, "The Fourth Amendment", *supra* note 149 at 857–59; Fehr, "Criminal Law and Digital Technologies: An Institutional Approach", *supra* note 196 at 69–71; Colton Fehr, "Criminal Law & Digital Technologies: Drawing Lessons from the Canadian and American Experiences" (2021) 53:3 UBC L Rev 653 at 653–55 [Fehr, "Criminal Law & Digital Technologies: Drawing Lessons"].

285. See e.g. Patricia L Bellia, "Designing Surveillance Law" (2011) 43:2 Ariz St LJ 293 at 296.

286. Kerr, "The Fourth Amendment and New Technologies", *supra* note 149 at 858. Note that each of these features are discussed by Kerr. He highlights that many of these factors apply in civil contexts rather than in the context of criminal procedure. However, this subsection also discusses his distinct concerns regarding institutional competence in the context of criminal procedure.

287. *Ibid*.

288. *Ibid*.

289. *Ibid* at 858–59; James Orenstein, "Judicial Engagement with Surveillance Technology" (2017) 49:5 Conn L Rev 1719 at 1727.

290. Kerr, "The Fourth Amendment and New Technologies", *supra* note 149 at 858–59; Skolnik, "Hot Bench", *supra* note 151 at 1310.

use.[291] Lastly, judges lack information gathering capacity and are bound by the evidence that the parties present.[292] But the litigation process distorts the presentation of evidence.[293] Given the adversarial nature of proceedings, each party has a self-interest to present information that best supports their position.[294] Judges may craft overly broad rules and legal tests that are based on incomplete information, and that are prone to misfire.[295]

Despite these limitations, courts enjoy the institutional competence to regulate technologies in ways that lawmakers cannot. While lawmakers enact rules that apply to a broad class of cases, judges can develop the law incrementally and assess its constitutionality in a discrete case.[296] Although certain judicial decisions may be predominantly concerned with the impact of mass-surveillance technologies on individual rights, statutory oversight of these technologies may reflect lawmakers' self-interest in re-election.[297]

The legislative branch, on the other hand, has a certain degree of institutional competence that the judicial branch lacks. Lawmakers can, in theory, regulate emerging technologies proactively and more quickly because they are not required to wait until an appeals process winds its course.[298] They can also craft rules or tests that are based on a broader and more complete array of information.[299] As discussed above, when regulating technology, lawmakers may seek out expert evidence, implement a notice-and-comment procedure, resort to legislative committees and subcommittees, refine a bill through multiple readings, and respond to academic and media scrutiny of a bill—a democratic process that courts do not employ.[300] Compared to judicial

291. Kerr, "The Fourth Amendment and New Technologies", *supra* note 149 at 868.

292. *Ibid* at 875; Sunstein, "The Most Knowledgeable Branch", *supra* note 141 at 1613.

293. Sunstein, "The Most Knowledgeable Branch", *supra* note 141 at 1614.

294. *Ibid*.

295. See e.g. Cass R Sunstein, *One Case at a Time: Judicial Minimalism on the Supreme Court* (Cambridge, Mass: Harvard University Press, 1999) at 49–50.

296. Kerr, "The Fourth Amendment", *supra* note 149 at 859. See also Orin S Kerr, "An Equilibrium-Adjustment Theory of the Fourth Amendment" (2011) 125:2 Harv L Rev 476 at 528 [Kerr, "An Equilibrium-Adjustment Theory"].

297. Steven Penney, "Unreasonable Search and Seizure & Section 8 of the *Charter*: Cost-benefit Analysis in Constitutional Interpretation" in Errol Mendes & Stéphane Beaulac, eds, *Canadian Charter of Rights and Freedoms*, 5th ed (Toronto: LexisNexis, 2013) 748 at 758.

298. Kerr, "The Fourth Amendment", *supra* note 149 at 870; Sunstein, "The Most Knowledgeable Branch", *supra* note 141 at 1608, 1614.

299. Kerr, "The Fourth Amendment", *supra* note 149 at 875.

300. *Ibid*; Skolnik, "Hot Bench", *supra* note 151 at 1306.

oversight mechanisms, the legislative process may regulate emerging technology in a more balanced and effective manner.[301]

Yet, the legislative process also suffers from certain shortcomings. Lawmakers may be reluctant to authorize or regulate mass-surveillance technologies because they fear significant backlash from their constituents.[302] Elected officials are particularly vulnerable to regulatory capture and lobbying pressures that result in laws and policies that skew in favour of groups that are more politically powerful.[303] Furthermore, even when lawmakers *do* attempt to regulate emerging technologies, legislative responses may be slow, incomplete, or incoherent.[304] Colton Fehr has shown that Parliament has been reluctant to regulate such technologies despite the legislative branch's purported institutional competence in such contexts.[305]

In contrast, judges exercise a counter-majoritarian role that can protect the interests of minority groups better than lawmakers.[306] Furthermore, unlike lawmakers, judges are generally insulated against these pressures because of the opaque and secretive nature of their deliberative process.[307] Yet, this lack of transparency in the deliberative process also raises democratic legitimacy concerns, especially in contexts where judges authorize new common law police powers that authorize surveillance.[308]

Given these strengths and weaknesses, scholars have suggested that lawmakers and courts should regulate certain investigative technologies based on their respective institutional competence. Orin Kerr argues that courts should create rules, principles, and tests in contexts where the relevant investigative

301. Kerr, "The Fourth Amendment", *supra* note 149 at 875.

302. See e.g. Catherine Crump, "Surveillance Policy Making by Procurement" (2016) 91:4 Wash L Rev 1595 at 1616–28 (providing an overview of how the authorization of mass surveillance technology in Oakland led to significant public backlash).

303. Kerr, "The Fourth Amendment", *supra* note 149 at 859; Fehr, "Criminal Law and Digital Technologies", *supra* note 196 at 101.

304. Fehr,"Criminal Law and Digital Technologies: An Institutional Approach", *supra* note 196 at 89–91.

305. *Ibid*.

306. See e.g. Steven Penney, "National Security Surveillance in an Age of Terror: Statutory Powers & *Charter* Limits" (2010) 48:2 Osgoode Hall LJ 247 at 266–68.

307. Scott Dodson, "The Making of the Supreme Court Rules" (2022) 90:4 Geo Wash L Rev 866 at 907–08.

308. See e.g. Richard Jochelson & Mark Doerson, "The Supreme Court of Canada Presents: The Surveillant Charter and the Judicial Creation of Police Powers in Canada" in Randy K Lippert et al, eds, *National Security, Surveillance and Terror: Canada and Australia in Comparative Perspective* (London, UK: Palgrave MacMillan, 2016) 75 at 78.

tool's use remains stable and where judges are familiar with its underlying facts.[309] Lawmakers, on the other hand, are better suited to regulate technologies whose use can evolve and where judges lack familiarity with its underlying facts.[310] Notably, the legislative branch can amend these laws and policies more frequently, correct errors more easily, and devise tests and norms that involve a greater degree of democratic and stakeholder input.[311] Furthermore, judicial review can ensure that the statutory regulation of surveillance technologies respect individuals' constitutional rights.

In response, scholars have contested this division of labour on various grounds. First, some note that legislative attempts to regulate emerging technologies may result in fierce opposition by various groups—civil society organizations, privacy commissioners, academics, other political parties—that block legislative oversight of these technologies.[312] Second, the public should not rely on lawmakers to proactively regulate certain investigative techniques because they have failed to do so in various contexts.[313] Rather, lawmakers tend to legislate when a court strikes down some law or police conduct as unconstitutional, or in response to a highly mediatized and salient event.[314] Third, statutes that govern emerging technologies may still have important gaps or produce errors.[315] Fourth, statutory regimes may confer less protection against surveillance technologies than courts tend to provide.[316] Fifth, although lawmakers can revise statutes more frequently than courts, the legislative branch may not do so.[317]

Given the institutional capacities and limitations of each branch of government, scholars have advanced different proposals to regulate emerging

309. Kerr, "The Fourth Amendment", *supra* note 149 at 863.

310. *Ibid*.

311. *Ibid*.

312. Fehr, "Criminal Law and Digital Technologies: An Institutional Approach", *supra* note 196 at 101.

313. Erin Murphy, "The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions" (2013) 111:4 Mich L Rev 485 at 490, 502–03 (providing the example of police interrogations). However, a similar argument applies in various other contexts in Canada, including the judicial regulation of investigative detentions, stop-and-frisk searches, searches incidental to arrest, police surveillance operations, and more.

314. *Ibid* at 498–99.

315. *Ibid*; Daniel J Solove, "Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference" (2005) 74:2 Fordham L Rev 747 at 763–64 [Solove, "Fourth Amendment Codification"]

316. Solove, "Fourth Amendment Codification", *supra* note 315 at 765–66.

317. David Alan Sklansky, "Two More Ways Not to Think about Privacy and the Fourth Amendment" (2015) 82:1 U Chicago L Rev 223 at 227.

technologies. Some contend that the legislative and judicial branches of government can each play a complementary role in regulating emerging technologies.[318] Lawmakers can regulate emerging technologies by submitting a constitutional reference to an appellate or apex court.[319] Or, lawmakers can also enact legislation that incorporates a sunset clause, which ensures that the legislative branch must revisit statutory oversight mechanisms that become outdated.[320] These proposals leverage the institutional competence of each branch of government. Yet, lawmakers may still be reluctant to regulate these technologies due to inertia or because they fear backlash. Furthermore, such regulation may still contain gaps or confer inadequate protection against mass surveillance.

C. Anti-Mass-Surveillance Norms in Criminal Procedure

There are other ways in which courts and lawmakers can expand constitutional protection against mass-surveillance technologies in a manner that leverages their respective institutional competence. As discussed more below, lawmakers tend to regulate surveillance technologies when courts conclude that an investigative technique is unconstitutional or requires greater legislative oversight. However, the reasonable expectation of privacy test may fail to provide adequate protection against mass surveillance given how technology progressively erodes constitutional norms, and because surveillance takes place on public property where individuals enjoy a lower expectation of privacy.

Yet, courts could recognize that individuals enjoy a distinct constitutional interest in being protected against mass-surveillance technologies—recognition that can stimulate constitutional dialogue and promote better legislative oversight over these technologies.[321] This judicially recognized constitutional interest can provide additional safeguards that the reasonable expectation of privacy test does not, especially as private information becomes increasingly available in the public domain, and as expectations of privacy incrementally decrease. Courts could invoke this interest to conclude that mass-surveillance technologies are unconstitutional insofar as they fail to satisfy certain conditions or lack adequate oversight mechanisms. In doing so,

318. Orin S Kerr, "Digital Evidence and the New Criminal Procedure" (2005) 105:1 Colum L Rev 279 at 308.

319. Fehr, "Criminal Law and Digital Technologies: An Institutional Approach", *supra* note 196 at 109.

320. *Ibid*.

321. For an article advancing a similar argument that applies to the internet of things, see Andrew Guthrie Ferguson, "The Internet of Things and the Fourth Amendment of Effects" (2016) 104:4 Cal L Rev 805 at 866–67; Kerr, "An Equilibrium-Adjustment Theory", *supra* note 296 at 501, citing Posner J's approach in *US v Garcia*, 474 F (3d) 994 at 998 (7th Cir 2007).

courts would encourage dialogue between the judicial and legislative branches of government. The recognition of a constitutional interest in being protected against mass-surveillance technologies could catalyze legislative action in a way that leverages lawmakers' institutional competence and helps ensure that statutory oversight mechanisms are subject to judicial review. Moreover, this proposal could overcome the traditional problem of legislative inertia that hinders the legislative regulation of emerging surveillance technologies.

The distinct constitutional interest in being protected against mass-surveillance technology can be justified on various grounds. For instance, mass-surveillance technologies significantly increase governmental power, are prone to abuse, and can be exercised tyrannically in ways that other types of searches cannot.[322] Many of these technologies can be deployed surreptitiously, such that individuals do not know whether they were surveilled, and thus cannot challenge abusive exercises of state power.[323] In contrast to the execution of a search warrant at a particular time, mass surveillance empowers the government to gather and store information for years.[324] Many of these technologies may be cheaper to use than other investigative tools—such as acquiring search warrants or conducting physical surveillance—which facilitates their use and abuse.[325] Individuals may also self-censor or modify their conduct because they cannot ascertain whether the government is watching them constantly.[326] A distinct constitutional interest in being protected against mass surveillance captures how these technologies give rise to unique risks of tyranny and abuse.

This standalone section 8 *Charter* interest is justified by the gradual erosion of reasonable expectations of privacy, the blanket use of surveillance technologies, and the increasing inability to opt out of mass surveillance.[327] A distinct privacy interest against mass surveillance can strengthen section 8 *Charter* protection more robustly compared to the conventional analysis of whether expectations of privacy are reasonable.[328]

---

322. Ferguson, "Surveillance and the Tyrant Test", *supra* note 147 at 212, 262–63.

323. Bloch-Wehba, "Visible Policing", *supra* note 169 at 962.

324. Matthew Tokson, "The Next Wave of Fourth Amendment Challenges after *Carpenter*" (2020) 59:1 Washburn LJ 1 at 8, n 60, citing *United States v Jones,* 565 US 400 at 415–16 (2012).

325. Rachel Levinson-Waldman, "Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public" (2017) 66:3 Emory LJ 527 at 567.

326. Elizabeth Stoycheff et al, "Privacy and the Panopticon: Online Mass Surveillance's Deterrence and Chilling Effects" (2019) 21:3 New Media & Society 602 at 603, 612.

327. Levinson-Waldman, *supra* note 325 at 550–55.

328. David Gray & Danielle Citron, "The Right to Quantitative Privacy" (2013) 98:1 Minn L Rev 62 at 101.

Constitutional criminal procedure already acknowledges individuals' interests in being protected against mass surveillance.[329] Three examples illustrate this point. To begin, in *R v Duarte,* the Supreme Court of Canada decided that law enforcement must obtain a warrant to intercept individuals' private communications.[330] The Court's decision was justified by the threat that the technology could be used for mass surveillance purposes.[331] Similarly, in *R v Wong,* the Supreme Court of Canada held that the state cannot surreptitiously film individuals in their dwelling house without a warrant.[332] The Court observed that individuals have an interest in being protected against Orwellian forms of mass surveillance in the private sphere—a justification that can be extended equally to the public sphere.[333] The federal government responded to the Court's decision in *Wong* by creating the *Criminal Code*'s general warrant provision.[334] Lastly, in *R v Wise,* the Supreme Court of Canada decided that the police must obtain a warrant to track an individual or their vehicle except in exigent circumstances.[335] The Court remarked that the technology created a significant risk of mass surveillance which justified the prior judicial authorization requirement.[336] Here too, Parliament responded by creating a new warrant provision—the tracking warrant—in the *Criminal Code*.[337] Concerns about mass surveillance underpinned the Court's reasoning in these three decisions.

A privacy interest against mass surveillance is advantageous for several reasons. For one, this privacy interest aligns with the common law's recognition that warrantless searches are presumptively unreasonable.[338] Second, this same interest counteracts the state's capacity to gather highly personal information in public spaces that individuals cannot generally avoid entirely.[339] This privacy interest acknowledges that individuals should not be required to trade their

329. Derek Lai, "Public Video Surveillance by the State: Policy, Privacy Legislation, and the *Charter*" (2007) 45:1 Alta L Rev 43 at 67.

330. 1990 CanLII 150 (SCC) [*Duarte*].

331. *Ibid* at 44.

332. *Wong*, *supra* note 119.

333. *Ibid* at 45–47.

334. *Criminal Code*, *supra* note 120, s 487.01; Kent Roach, "Constitutional and Common Law Dialogues Between the Supreme Court and Canadian Legislatures" (2001) 80:1/2 Can Bar Rev 481 at 520.

335. *Wise*, *supra* note 119.

336. *Ibid* at 558.

337. *Criminal Code*, *supra* note 120, s 492.1; James Stribopoulos, "A Failed Experiment", *supra* note 74 at 367.

338. *R v Collins*, 1987 CanLII 84 at para 25 (SCC); *Hunter*, *supra* note 63 at 161.

339. Houwing, *supra* note 278 at 174.

liberty to safeguard their privacy.[340] Third, courts have already affirmed that individuals do not necessarily waive their section 8 *Charter* rights simply because they are in public.[341] A privacy interest against mass surveillance is both consistent with a purposive interpretation of section 8 of the *Charter* and would bolster existing constitutional safeguards.

Concretely, recognizing a privacy interest against mass surveillance could generate several consequences within criminal procedure. Courts could affirm that the state cannot employ technologies that can be used for mass surveillance without prior judicial authorization that limits the scope and duration of their use—an approach that the Supreme Court of Canada has adopted in the three cases discussed above.[342] Courts could also mandate that such technologies can only be justified if lawmakers implement certain oversight requirements.[343] These oversight measures can include clear laws and policies that govern the acquisition, retention, and destruction of data that these technologies acquire, which privacy commissions already impose. Oversight mechanisms can also include reporting obligations that compel law enforcement to document their use of investigative technologies that can be used for mass surveillance.[344]

The judiciary could impose other requirements that would govern police investigations. To counteract mass surveillance, courts could decide that investigative technologies—such as collecting abandoned objects that contain DNA—can be used only against individuals who are reasonably suspected of having committed a particular crime.[345] Courts could also limit the scope of some investigative techniques, such as public DNA database searches, to major crimes identified by Parliament—an approach that fosters constitutional dialogue.[346] Courts could prohibit certain technologies that violate the privacy interest against mass surveillance, such as facial recognition or ALPR, and which may encourage Parliament to regulate them more thoroughly. Subsequent laws that permit the use of such technologies would be subject to constitutional scrutiny.

340. Terry Skolnik, "How and Why Homeless People Are Regulated Differently" (2018) 43:2 Queen's LJ 297 at 316–19.

341. John Burchill, "Tale of the Tape: Policing Surreptitious Recordings in the Workplace" (2017) 40:3 Man LJ 247 at 248, 282, citing *R v Spencer*, 2014 SCC 43 at para 44.

342. *Wong*, *supra* note 119; *Wise*, *supra* note 119; *Duarte*, *supra* note 330; Robin McLachlen, "Reasonable Expectations Make Unreasonable Inferences: The Reasonable Expectation Threshold is a Legal Doctrine Unequal to the Menace to Privacy Posed by Mass Surveillance and Algorithmic Analysis" (2022) 45:6 Man LJ 172 at 190.

343. Skolnik, "Racial Profiling", *supra* note 105 at 459.

344. *Ibid*.

345. See e.g. *D'Amico*, *supra* note 75 at para 321, per Thibault J.

346. Solana Lund, "Ethical Implications of Forensic Genealogy in Criminal Cases" (2020) 13:2 J Bus Entrepreneurship & L 185 at 206.

Admittedly, greater statutory oversight may result in some of the problems discussed in the previous subsection. Legislative attempts to regulate emerging technologies may still be subject to significant backlash by academics, political opposition, or civil society organizations, amongst others. To be clear, such opposition and disagreement are vital in a democracy. Yet, lawmakers could collaborate more closely with an independent institution—such as a privacy commission—to devise these statutory oversight mechanisms, leverage the independent institution's expertise, and reduce errors that provoke unnecessary backlash that tends to hinder legislative action.[347]

These mechanisms would also help re-establish the proper constitutional dialogue between courts and Parliament that has deteriorated over the past two decades, and would promote the rule of law by ensuring that police powers are legislated rather than judicially created after the fact.[348] By mandating prior judicial authorization, the judiciary would help recalibrate the respective roles of lawmakers and courts and leverage their respective institutional competence.[349] The Supreme Court of Canada's recognition of a constitutional interest to be protected against mass surveillance—and the need for legislative oversight over emerging surveillance technologies—would incentivize Parliament to legislate in the field of criminal procedure and overcome legislative inertia. These laws, in turn, would be subject to constitutional scrutiny by courts.[350] This proposed approach would not be revolutionary. Much of constitutional criminal procedure resembled this dynamic prior to the ancillary powers doctrine's growth in the 2000s.[351]

Together, a judicially recognized privacy interest against mass surveillance, a warrant requirement for investigative tools with mass surveillance potential, and rigorous legislative oversight mechanisms can better safeguard individuals' privacy. This same approach can also help restore a more democratic dynamic between the various branches of government and counteract criminal procedure's one-way ratchet tendency.

347. Fehr, "Digital Evidence", *supra* note 284 at 454–55.

348. Skolnik, "Racial Profiling", *supra* note 105 at 459–62; James Stribopoulos, "Has Everything Been Decided? Certainty, the Charter and Criminal Justice" (2006) 34 SCLR (2d) 381 at 405–06.

349. Skolnik, "Racial Profiling", *supra* note 105 at 459–62.

350. *Ibid*.

351. Boucher, Lacasse & Nadon, *supra* note 117 at 795–96.

Conclusion

This article argued that police officers employ two strategies to circumvent constitutional norms: changing the normative quality of information gathering and changing the normative quality of information from private to public. It demonstrated how the criminal procedure doctrines of abandonment, waiver, and plain view searches facilitate these tactics and erode reasonable expectations of privacy. It explained how technology worsens this tendency. And it showed how legislative inertia and slippery slopes further chip away at constitutional rights.

The concluding parts of this article advanced concrete proposals that offer better judicial and legislative oversight of mass-surveillance technologies. More specifically, courts should recognize that individuals enjoy a distinct privacy interest against mass surveillance, an interest to which the Supreme Court of Canada has alluded in several cases.[352] This privacy interest would justify prior judicial authorization for mass-surveillance technologies, and mandate legislative oversight measures that govern data retention, notice requirements, and disclosure obligations. Ultimately, this approach would also recalibrate the respective roles of Parliament and the Supreme Court of Canada in a manner that optimizes their institutional competence.

More fundamentally, this article highlights why criminal procedure's one-way ratchet tendency justifies a new normative approach to privacy in constitutional law. It explained why the rise of mass-surveillance technologies presents a unique challenge to the traditional concept of reasonable expectations of privacy inherent to section 8 of the *Charter*. Although this article discussed why three specific technologies justify a distinct privacy interest against mass surveillance, other emerging technologies further reinforce this justification: surveillance drones, stingray technology that tracks cellphone use, body-worn police cameras that can incorporate facial recognition software, spyware, and more.[353]

This article also lays the groundwork for future scholarship that analyzes how a distinct privacy interest against mass surveillance can impact other areas of the law, such as tort law, health law, tax law, administrative law, and more. The recognition of this interest not only holds the potential to better safeguard individuals' liberty, dignity, and privacy in these other spheres. The consequences of a judicially recognized privacy interest against mass surveillance—warrant requirements, legislative oversight, and robust data protection policies—also help ensure that each branch of government helps protect individuals against mass surveillance, and ultimately, tyranny.

352. *Wong*, *supra* note 119; *Wise*, *supra* note 119; *Duarte*, *supra* note 330.

353. Ringrose & Ramjee, *supra* note 3 at 350–51, 357; Roya Butler, "Stingray Stung? Analyzing Cellphones as Effects Provides Fourth Amendment Treatment" (2021) 34:2 Harv JL & Tech 733 at 734–36.