From Horseback to the Moon and Back: Comparative Limits on Police Searches of Smartphones Upon Arrest

BRYCE CLAYTON NEWELL† AND BERT-JAAP KOOPS†

The search of a smartphone by the police in connection with an arrest carries the potential to intrude into the very core of an arrestee's private life. Indeed, such a search has been compared to providing a "window[] to our inner private lives," including aspects of our lives completely disconnected from the reasons for the arrest. In recent years, the supreme courts of the United States, Canada, and the Netherlands (as well as Dutch legislators) have handed down rules about how, and whether, police may search an arrestee's smartphone upon arrest without first obtaining a warrant or other court order. These responses can be categorized as either container-based or content-based approaches, depending on whether the court (or legislature) focuses on protecting the privacy-sensitive content (for example, personal information) as such or, rather, the container (for example, the smartphone) as a proxy for protecting privacy-sensitive content contained within the device. After analyzing and comparing the approaches adopted in each of these three countries, we argue that both approaches have advantages and disadvantages, and we suggest a combination of the two as a fruitful path forward, balancing the important privacy and law enforcement interests at stake.

† J.D., PhD., Assistant Professor of Media Law and Policy, School of Journalism and Communication, University of Oregon.

† Professor of Regulation and Technology, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, the Netherlands. The research for this Article was made possible by a grant from the Netherlands Organisation for Scientific Research (NWO), project number 453-14-004. All translations in this Article are by the authors, except where otherwise indicated. We thank Aldo Sghirinzetti for his research assistance.

TABLE OF CONTENTS

> The [government] asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches of these sorts of physical items [such as cigarette packs, wallets, or address books]. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together.
>
> — Chief Justice John Roberts, United States Supreme Court[1]

INTRODUCTION

If a traditional police search of an arrestee's pockets, purse, or wallet for investigatory purposes can be characterized as a simple "ride on horseback," then, comparatively, a similar search of an arrestee's smartphone is "a flight to the moon."[2] The two searches, although both relevant to law enforcement investigations, are fundamentally distinguishable from each other in character—as noted by Chief Justice John Roberts of the Supreme Court of the United States, "[b]oth are ways of getting from point A to point B, but little else justifies lumping them together."[3] The distinction, according to the Court in its unanimous 2014 decision in *Riley v. California*,[4] is compelled by the underlying interest in personal privacy that limits unreasonable police searches of private persons and their property. While "inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself," the search of the person's cellphone constitutes a qualitatively and quantitatively different (and much greater) intrusion into personal privacy.[5] And, the Supreme Court's holding is not limited to the most modern smartphones. Indeed, the ruling extends to both smartphones and not-so-smart phones, as the Court found that even a "flip phone" exhibiting "a smaller range of features than a smart phone . . . [is] based on technology nearly inconceivable just a few decades ago."[6] As put by one Canadian court, "[s]earches of these devices engender privacy concerns that have no analogue."[7] Additionally, questions about the proper scope of searches conducted incident to arrest are important, in part, because, "[t]he power to search incident to arrest not only permits searches

1. Riley v. California, 573 U.S. 373, 393 (2014) (citation omitted).

2. *Id.* In *Riley*, the search of two different types of cellphones were at issue: a "smart phone"—defined by the court as "a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity"—and a "flip phone" exhibiting "a smaller range of features than a smart phone." *Id.* at 379–80. Although the Court focused much of its reasoning on the advanced capabilities of modern smartphones, the holding covered both. In the Court's words, "[b]oth phones are based on technology nearly inconceivable just a few decades ago." *Id.* at 385. As such, although we focus in this Article on modern smartphones, we also discuss where doctrine might make distinctions between different mobile phones based on their (broad or limited) capabilities.

3. *Id.* at 393.

4. *Id.* at 373.

5. *Id.* at 375.

6. *Id.* at 379–80, 385.

7. R. v. Nero (2016), 345 O.A.C. 282, para. 157 (Can. Ont. C.A.).

without a warrant, but does so in circumstances in which the grounds to obtain a warrant do not exist."[8]

Only a few months after the Supreme Court of the United States (SCOTUS) decided *Riley*, the Supreme Court of Canada (SCC) was confronted with a similar question: whether "the general common law framework for searches incident to arrest needs to be modified in the case of cell phone searches incident to arrest."[9] Additionally, in the Netherlands, courts have also grappled with this question in recent years—and while lower courts had been split on the issue, the Dutch Supreme Court (*Hoge Raad*) finally addressed the issue in 2017.[10]

In each of these lines of cases, courts have had to weigh law enforcement interests against suspects' interests in privacy and to determine whether existing legal frameworks for regulating searches incident to arrest should be modified to account for the fact that these searches can constitute a "much more significant invasion of privacy"[11] than the sorts of searches envisioned by those who promulgated these frameworks. Similar challenges apply to the ability of law enforcement to search other types of computing devices, including, for example, digital cameras,[12] laptop computers, or computers embedded in automobiles.[13]

Indeed, the power to search the vast amount of information that modern smartphones might contain would allow the police to overcome prior limitations (or "physical realities") that existed in the pre-smartphone environment.[14] In effect, this is a situation where

> [c]ourts and legislators have had to deal with questions about how the law relating to atoms applies to cases involving bits (in the absence of bits-specific law), facing the fact that bits and atoms have different properties and finding that the law is not adequately suited to cope with relevant differences.[15]

And, as demonstrated by the fact that courts and legislators in multiple countries have been grappling with this issue for years, these cases pose

8. R. v. Fearon, [2014] 3 S.C.R. 621, para. 16 (Can.).

9. *Id.* at para. 58.

10. HR 4 april 2017, ECLI:NR:HR:2017:584 (Neth.).

11. *Fearon*, 3 S.C.R. at para. 58.

12. *See, e.g.*, Commonwealth v. Mauricio, 80 N.E.3d 318, 324 (Mass. 2017) (holding, on state constitutional grounds, that "the search of data contained in digital cameras falls outside the scope of the search incident to arrest exception to the warrant requirement").

13. *See, e.g.*, Mobley v. State, 816 S.E.2d 769, 770–71 (Ga. Ct. App. 2018) (holding that the defendant did not have a reasonable expectation of privacy in data collected from the "airbag control module" in his car after a high-speed crash).

14. Riley v. California, 573 U.S. 373, 393 (2014) ("One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy.").

15. Ronald Leenes, *Of Horses and Other Animals of Cyberspace*, 1 TECH. & REGUL. 1, 1 (2019), https://techreg.org/index.php/techreg/article/view/3/techreg.2019.001. A stark example of a court simply denying that, in the context of arrest-related searches, digital realities differ from physical realities is a South African case, *State v. Miller*. 2015 (4) All SA (WCC) at 27 para. 51 (S. Afr.) ("In any event, given the importance of speedy investigatory steps in the fight against crime it seems counter-productive to require the police to follow a bureaucratic procedure to access digital information, a procedure which would not be required in respect of non-digital evidential material.").

important questions for continuing or extending our historical approach to criminal procedure—questions that extend beyond the law and experience of any single nation.

This is particularly true since the law has often protected underlying privacy interests by protecting concrete proxies (for example, objects or containers, such as houses, bags, or digital devices that enclose or surround aspects of a person's private life)[16] rather than the underlying (and sometimes abstract) privacy interests themselves. This is largely a pragmatic solution, as it provides police officers (and other government agents) with relatively concrete and identifiable rules to work with, rather than forcing them to make complex, *ex ante* determinations about when a search is allowed based on abstract notions of privacy. However, protecting privacy by proxy can also limit flexibility down the line as new technologies or investigatory measures develop that bypass historically identified proxies, and that facilitate the privacy intrusions the earlier proxies were designed to prohibit.

In this Article, our first aim is to analyze how legislators and judges in three countries (the United States, Canada, and the Netherlands) are responding to the increasingly common scenario where police seek to obtain information from people's smartphones incident to an arrest—an investigatory method that challenges traditional legal frameworks within procedural criminal law, especially since the privacy-intrusiveness of smartphone searches extends well beyond what lawmakers anticipated when drafting existing criminal procedure law (including various search-incident-to-arrest exceptions across jurisdictions). Importantly, we exclude consent-based searches from our analysis, examining only those cases where searches are conducted without the consent of the suspect.[17]

Our second aim is to outline various conceptual and normative anchor points that may help legislators and others deal with this issue. In earlier research, we identified new boundary-marking concepts arising in various jurisdictions to protect privacy in the context of criminal procedure.[18] This paper allows us to analyze whether and to what extent these new concepts may help in regulating police smartphone searches. Specifically, we examine whether and how a combination of emerging and pre-existing container-based and content-based approaches to regulating police searches might be used to solve the challenge of finding a framework that is both sufficiently concrete (to be manageable for police officers) and sufficiently technology-neutral (to be sustainable in light of significant and ongoing socio-technical change). This

16. *See* Bert-Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Škorvánek, Tomislav Chokrevski & Maša Galič, *A Typology of Privacy*, 38 U. PA. J. INT'L L. 483, 540–44 (2017) (exemplifying objects used as proxies in privacy law).

17. Consent provides a basic exception to limits on investigatory police searches in all three jurisdictions examined in this study.

18. Bert-Jaap Koops, Bryce Clayton Newell & Ivan Škorvánek, *Location Tracking By Police: The Regulation of 'Tireless and Absolute Surveillance'*, 9 U.C. IRVINE L. REV. 635, 685 (2019); Ivan Škorvánek, Bert-Jaap Koops, Bryce Clayton Newell & Andrew Roberts, "*My Computer Is My Castle": New Privacy Frameworks to Regulate Police Hacking*, 2019 BYU L. REV. 997, 1078 (2019).

analysis can help practitioners and courts further develop rules on smartphone searches, especially since the rules stipulated by the supreme courts we reference here remain rather general and raise questions in post-judgment practice.

In this research, we engage in comparative, doctrinal legal analysis. We conducted doctrinal legal analysis research for three jurisdictions (United States, Canada, and the Netherlands) and compared our findings across jurisdictions. We chose these three jurisdictions based on their relevance to a larger comparative study of privacy and criminal law and procedure and the fact that, of the countries in that larger study, these three have each had a recent supreme court ruling addressing the question of when police may search a suspect's smartphone during or shortly after an arrest.[19]

Some limitations apply. Our analysis only covers searches conducted by the police following and connected (incidental) to a lawful arrest. We do not examine legal rules that govern police searches of smartphones (or cellphones) outside the search-incident-to-arrest context. We also do not examine the regulation of device searches at international borders or points of entry, where different legal rules often apply. Additionally, we assume for the purposes of our analysis that police are technically capable of looking inside a seized smartphone, for instance, because it is not password-protected, or it is seized when unlocked. Questions of compelled disclosure of passwords or biometric disclosure raise different types of questions and fall outside the scope of our analysis.[20]

In Part I, we outline the basic contours of the law regarding police searches incident to arrest in the three chosen countries and then examine how the respective supreme courts have ruled in cases involving searches of cellphones incident to arrest. In Part II, we examine these developments from a more conceptual and theoretical perspective, analyzing how the reasoning in these recent court rulings fits into broader debates about protecting privacy in an era when the "privacies of life"[21] are often held in (or are accessible through) a small device that fits inside a person's pocket. We highlight how the U.S. approach to protecting privacy and limiting law enforcement investigations focuses on protecting proxies, like smartphones themselves, while Canadian and Dutch approaches focus more on the content to be searched or examined. The regulatory choice to either institute a blanket ban on investigatory conduct (like that imposed by *Riley*) or a more nuanced, case-by-case, and context-dependent inquiry (like those promulgated in Canada and the Netherlands) has a significant

19. *See* Koops et al., *supra* note 16, at 504–10 (noting information about the methodology we employed in the broader study); Koops et al., *supra* note 18, at 639–40; Bert-Jaap Koops, Bryce Clayton Newell, Andrew Roberts, Ivan Škorvánek & Maša Galič, *The Reasonableness of Remaining Unobserved: A Comparative Analysis of Visual Surveillance and Voyeurism in Criminal Law*, 43 L. & SOC. INQUIRY 1210, 1212–13 (2018).

20. For recent discussions of compelled decryption, see, for example, Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767, 799 (2019); Laurent Sacharoff, Response, *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, 97 TEX. L. REV. ONLINE 63, 72 (2019).

21. Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018) (quoting Riley v. California, 573 U.S. 373, 403 (2014)).

impact on how privacy is protected. In conclusion, we argue that a balance between these container- and content-based approaches to regulating police searches of smartphones (and similar devices) might provide a better way forward, providing practical, usable guidance for police officers on the ground but not ignoring the fact that not all searches of digital devices are, or need to be, flights to the moon.

I. THE POWER TO SEARCH CELLPHONES INCIDENT TO ARREST

In this Part, we outline the basic contours of the law regarding police searches incident to arrest in our three chosen countries, analyze recent high court decisions that examine how their respective search-incident-to-arrest doctrines apply in the context of cellphone searches, and finally examine how these decisions have been interpreted in subsequent case law. We focus in particular on how the privacy interest in these cases has been conceptualized and translated into legal limits on law enforcement searches of cellphones.

A. UNITED STATES OF AMERICA

1. Overview of the Search-Incident-to-Arrest Doctrine

In the United States, police searches (generally, investigatory measures carried out to collect evidence) are regulated by the Fourth Amendment to the U.S. Constitution.[22] The Fourth Amendment prohibits state agents from conducting "unreasonable searches"—those that would intrude on a person's interests in their property or their reasonable expectations of privacy—without first obtaining a judicial warrant.[23] The Amendment explicitly covers "persons, houses, papers [including correspondence], and effects [property]."[24] Over the years, SCOTUS has crafted a variety of exceptions to this general rule. Although it existed in practice prior to its formal recognition by the courts, SCOTUS first acknowledged the search-incident-to-arrest exception in 1914, in *Weeks v. United States*,[25] even though it was not directly relevant in that case. In *Weeks*, the Court acknowledged, in *dicta*, "the right on the part of the Government, always recognized under English and American law, to search the person of the accused when legally arrested to discover and seize the fruits or evidences of crime."[26] According to the Court in *Riley v. California*, one hundred years later,

> Since that time, it has been well accepted that such a search constitutes an exception to the warrant requirement. Indeed, the label "exception" is something of a misnomer in this context, as warrantless searches incident to arrest occur with far greater frequency than searches conducted pursuant to a warrant.[27]

22. U.S. CONST. amend. IV.
23. *Id.*
24. *Id.*
25. Weeks v. United States, 232 U.S. 383, 392 (1914).
26. *Id.*
27. Riley v. California, 573 U.S. 373, 382 (2014).

In the one hundred years between *Weeks* and *Riley*, the scope of the search-incident-to-arrest exception garnered a "checkered history."[28] When the Court was confronted with questions about the applicability of the exception to smartphone searches in *Riley*, there were three primary cases that governed searches incident to arrest: *Chimel v. California*,[29] *United States v. Robinson*,[30] and *Arizona v. Gant*.[31] In *Chimel* (from 1969), the Court invalidated an exhaustive search of an arrestee's entire house and noted that the purposes served by the exception were to *protect officer safety* and to *preserve evidence*.[32] According to the Court,

> When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction. . . . There is ample justification, therefore, for a search of the arrestee's person and the area "within his immediate control"—construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence.[33]

However, four years later in *Robinson*, the Court interpreted this test rather broadly, holding that an arresting officer may conduct a pat-down of the arrestee's body and clothing and even go so far as to open containers found on the suspect's person, even when the search moves beyond being a search for weapons or evidence related to the crime at hand.[34] Ultimately, the Court held that searches incident to arrest are a legitimate response to "the need to disarm and to discover evidence"[35] (to ensure officer safety, to preserve evidence, and to secure evidence related to the crime for which the suspect had been arrested). As long as the arrest itself was lawful, the Court held,

> a search incident to the arrest requires no additional justification. It is the fact of the lawful arrest which establishes the authority to search, and we hold that in the case of a lawful custodial arrest a full search of the person is not only an exception to the warrant requirement of the Fourth Amendment, but is also a "reasonable" search under that Amendment.[36]

Finally, in *Gant*, the Court applied the language of *Chimel* to limit the ability of police officers to search the passenger compartment of an automobile incident to an arrest, except in circumstances "when the arrestee is unsecured

28. *Id.* (quoting Arizona v. Gant, 556 U.S. 332, 350 (2009)).
29. Chimel v. California, 395 U.S. 752, 768 (1969).
30. United States v. Robinson, 414 U.S. 218, 236 (1973).
31. *Gant*, 556 U.S. at 351.
32. *Chimel*, 395 U.S. at 762–63.
33. *Id.*
34. *Robinson*, 414 U.S. at 236. In this case, a "crumpled package of cigarettes" containing illicit drugs. *Id.*
35. *Id.* at 235.
36. *Id.*

and within reaching distance of the passenger compartment at the time of the search."[37]

2. *Searching Cellphones Incident to Arrest Prior to* Riley

In *Riley*, SCOTUS consolidated two separate underlying cases: *United States v. Wurie*[38] (a federal First Circuit case from Massachusetts) and *People v. Riley*[39] (a California state case). In *Wurie*, a Boston Police Department detective observed Brima Wurie engage in what looked like a drug transaction.[40] After arresting the buyer and confirming that Wurie had sold him crack cocaine, the police followed Wurie and arrested him near his home as he exited his vehicle.[41] The police seized two phones, but did not immediately search them incident to Wurie's arrest.[42] Rather, their limited search of one of the phones came later, while Wurie was waiting to be booked into jail.[43] After noticing that one of the phones was receiving calls from a number marked as "my house," the police accessed the phone, viewed the wallpaper on the screen, accessed the call log, and acquired the number that had been making the incoming calls.[44] The trial court judge noted that although "[i]t seems indisputable that a person has a subjective expectation of privacy in the contents of his or her cell phone . . . the search of Wurie's cell phone incident to his arrest was limited and reasonable."[45] In so holding, the judge cited numerous district court decisions from around the country that had come to similar conclusions.[46]

---

37. *Gant*, 556 U.S. at 343. In *Gant*, the Court also announced a new, automobile-specific exception, allowing officers to search a passenger compartment "when it is 'reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.'" *Id.* (quoting Thornton v. United States, 541 U.S. 615, 632 (2004) (Scalia, J., concurring)).

38. United States v. Wurie, 728 F.3d 1, 14 (1st Cir. 2013), *aff'd sub nom.* Riley v. California, 573 U.S. 373 (2014).

39. People v. Riley, No. D059840, 2013 WL 475242, at *6 (Cal. Ct. App. Feb. 8, 2013), *rev'd and remanded sub nom.* Riley v. California, 573 U.S. 373 (2014).

40. *Wurie*, 728 F.3d at 1.

41. *Id.* at 2.

42. *Id.*

43. *Id.*

44. *Id.*

45. United States v. Wurie, 612 F. Supp. 2d 104, 109–10 (D. Mass. 2009).

46. For example, in *United States v. Finley*, the Fifth Circuit held that a cellphone was analogous to other types of closed containers that might be found on a person, such as a package of cigarettes or a footlocker. 477 F.3d 250, 260 (5th Cir. 2007) (holding that the exception applied to the search of "call records and text messages" on the arrestee's phone); *see also* United States v. Mercado-Nava, 486 F. Supp. 2d 1271, 1277 (D. Kan. 2007) ("Traditional search warrant exceptions apply to the search of cell phones."); United States v. Deans, 549 F. Supp. 2d 1085, 1094 (D. Minn. 2008) ("[I]f a cell phone is lawfully seized, officers may also search any data electronically stored in the device."); United States v. Valdez, No. 06-CCR-336, 2008 WL 360548, at *3–4 (E.D. Wis. Feb. 8, 2008) (searching the defendant's phone contemporaneously with his arrest was reasonable); United States v. Dennis, No. 07-008, 2007 WL 3400500, at *7 (E.D. Ky. Nov. 13, 2007) (finding that the search of a cell phone incident to valid arrest was no different from the search of any other type of evidence seized incident to arrest). In other cases, judges analogized cellphones to pagers, an earlier technology that courts had already decided fit into the container analogy. *See, e.g.*, *Wurie*, 612 F. Supp. 2d at 109; United States v. Reyes, 922 F. Supp. 818, 834 (S.D.N.Y. 1996) (finding that a warrantless search of the stored memory of two pagers was justified by the search-incident-to-arrest exception); United States v. Chan, 830 F. Supp. 531, 535 (N.D. Cal. 1993) (finding that the warrantless search of pager memory was comparable to searching through the contents

However, not all lower courts were convinced that cellphones should be treated as ordinary containers. In *United States v. Wall*,[47] for example, a judge in the Southern District of Florida rejected the cellphone-as-container analogy, stating that "searching through information stored on a cell phone [in the context of an inventory search] is analogous to a search of a sealed letter, which requires a warrant."[48] And in *United States v. Park*,[49] a California court likewise distinguished cellphones from pagers (and other, more traditional, containers). "Any contrary holding," the court stated, "could have far-ranging consequences," because

> modern cellular phones have the capacity for storing immense amounts of private information. Unlike pagers or address books, modern cell phones record incoming and outgoing calls, and can also contain address books, calendars, voice and text messages, email, video and pictures. Individuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations on their cell phones through email and text, voice and instant messages.[50]

In *Wurie*, on appeal, the First Circuit reversed the trial judge's holding that the search of Wurie's phone was reasonable, finding that the search-incident-to-arrest exception, as a general rule, does not authorize the warrantless search of data on a cellphone seized from an arrestee's person during an arrest.[51] The First Circuit noted that courts around the country

> have struggled to apply the Supreme Court's search-incident-to-arrest jurisprudence to the search of data on a cell phone seized from the person. The searches at issue in the cases that have arisen thus far have involved everything from simply obtaining a cell phone's number to looking through an arrestee's call records, text messages, or photographs.[52]

Although most courts to address the issue had upheld warrantless searches of cellphones incident to arrest, the First Circuit rejected this line of argumentation, noting that it "fails to account for the fact that the Supreme Court has determined that there are categories of searches undertaken following an arrest that are inherently unreasonable because they are never justified by one of

---

of a container); United States v. Diaz-Lizaraza, 981 F.2d 1216, 1223 (11th Cir. 1993) (finding that it was reasonable for law enforcement agents to activate the defendant's pager to confirm its number). As other evidence that courts had latched onto the cellphone-as-container idea, some judges also authorized warrantless searches of cellphones pursuant to the automobile exception. In *United States v. James*, one district court judge held that "the automobile exception allows the search of the cell phone just as it allows a search of other closed containers found in vehicles." No. 1:06CR134 CDP, 2008 WL 1925032, at *4 (E.D. Mo. Apr. 29, 2008).

47. United States v. Wall, No. 08-60016-CR, 2008 WL 5381412, at *3 (S.D. Fla. Dec. 22, 2008).

48. *Id.*

49. United States v. Park, No. CR 05-375SI, 2007 WL 1521573, at *8 (N.D. Cal. May 23, 2007).

50. *Id.* (footnote omitted).

51. United States v. Wurie, 728 F.3d 1, 11–12 (1st Cir. 2013), *aff'd sub nom.* Riley v. California, 573 U.S. 373 (2014).

52. *Id.* at 5 (citations omitted).

the *Chimel* rationales: protecting arresting officers or preserving destructible evidence."[53]

Thus, the First Circuit held that, to be lawful, a search of a cellphone incident to arrest must fall within one of these limits imposed by *Chimel* (for example, protecting officers or preserving evidence).[54] The court emphasized their finding that cellphones (as well as tablet or laptop computers) have the capacity to store much more information than something like a pager, purse, or cigarette package (more traditional "containers"), and that this

> information is, by and large, of a highly personal nature: photographs, videos, written and audio messages (text, email, and voicemail), contacts, calendar appointments, web search and browsing history, purchases, and financial and medical records. It is the kind of information one would previously have stored in one's home and that would have been off-limits to officers performing a search incident to arrest.[55]

This difference, the court noted, expanded the "nature and scope of the *search itself*," and was not only limited to a distinction based on the nature of the object seized.[56] Thus, at issue is the fact that, "[a]t the touch of a button a cell phone search becomes a house search, and that is not a search of a 'container' in any normal sense of that word, though a house contains data."[57] Although other courts had decided these questions on a case-by-case basis, the First Circuit went so far as to proclaim a general rule that cellphones could never be authorized by the search-incident-to-arrest exception; the court stated, "[w]e therefore hold that the search-incident-to-arrest exception does not authorize the warrantless search of data on a cell phone seized from an arrestee's person, because the government has not convinced us that such a search is ever necessary to protect arresting officers or preserve destructible evidence."[58]

In the second case consolidated into *Riley v. California* at the Court, *People v. Riley*, the California Court of Appeals upheld a search of David Riley's cellphone.[59] In that case, Riley was arrested after he had become a suspect in a gang-related shooting of a passing vehicle.[60] His phone was seized (along with two firearms), and an officer searched and noticed gang-related content on the phone.[61] Later, another officer searched Riley's phone at the police station, accessing videos, photographs, and other files during his search.[62] In holding

---

53. *Id.* at 7.

54. *Id.*

55. *Id.* at 8 (footnote omitted) (citation omitted).

56. *Id.* at 9.

57. *Id.* at 8–9 (quoting United States v. Flores-Lopez, 670 F.3d 803, 806 (7th Cir. 2012)). The *Flores-Lopez* court found that evidence preservation concerns in that case outweighed any invasion of privacy, upholding the warrantless search of the cell phone, because the search at issue was minimally invasive—only directed at discovering the phone's number. 670 F.3d at 809–10.

58. *Wurie*, 728 F.3d at 13.

59. People v. Riley, No. D059840, 2013 WL 475242, at *3 (Cal. Ct. App. Feb. 8, 2013), *rev'd and remanded sub nom.* Riley v. California, 573 U.S. 373 (2014).

60. *Id.* at *1.

61. *Id.* at *3.

62. *Id.*

that the warrantless search of Riley's phone was justified, the California Court of Appeals relied on a prior California Supreme Court decision holding that even "a delayed search of an item immediately associated with the arrestee's person may be justified as incident to a lawful custodial arrest without consideration as to whether an exigency for the search exists."[63] The *People v. Riley* court did not offer any substantive discussion related to privacy, nor about equating cellphones with ordinary containers. Indeed, in *People v. Diaz*, the California Supreme Court had expressly disclaimed any ability to restrict searches of cellphones based on their information-rich nature under existing SCOTUS precedent.[64] According to the court, "[t]he relevant high court decisions do not support the view that whether police must get a warrant before searching an item they have properly seized from an arrestee's person incident to a lawful custodial arrest depends on the item's character, including its capacity for storing personal information."[65]

In contrast to *Wurie* (and, eventually, the subsequent decision by SCOTUS), the California Supreme Court was not persuaded that the storage capacity of a cellphone should be determinative of the issue of whether a search was reasonable.[66] According to the court, "[e]ven 'small spatial container[s]' that hold less information than cell phones may contain highly personal, intimate and *private* information, such as photographs, letters, or diaries."[67]

3. Riley *at the Supreme Court*

In January 2017, SCOTUS granted certiorari to both underlying cases, consolidating them into a single case for the purpose of determining whether the search-incident-to-arrest exception to the Fourth Amendment's warrant requirement should extend to searches of cellphones.[68] A unanimous Court ruled that they should not—and that searches of cellphones, even incident to arrest, should generally require a judicial warrant.[69]

In his primary opinion, Chief Justice Roberts focused attention on the long-standing principle that "the ultimate touchstone of the Fourth Amendment is '*reasonableness*'" and that, in the law enforcement investigative context, "reasonableness generally requires the obtaining of a judicial warrant."[70] Then, after outlining general search-incident-to-arrest doctrine (including *Chimel* and

63. *Id.* at *4 (citing People v. Diaz, 244 P.3d 501, 506 (Cal. 2011)).

64. *Diaz*, 244 P.3d at 506.

65. *Id.*

66. *Id.* at 507.

67. *Id.* at 508 (second alteration in original) (citation omitted). *But see* United States v. Bah, 794 F.3d 617, 632–34 (6th Cir. 2015) (holding that *Riley* was distinguishable because "[t]he storage capacity of the magnetic strip of a credit, debit or gift card pales in comparison to that of a computer hard drive, cell phone, or even audiocassette").

68. Riley v. California, 573 U.S. 373, 378 (2014). The Court framed the question as: "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." *Id.*

69. *Id.* at 403.

70. *Id.* at 381–82 (emphasis added) (first quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006); and then quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)).

Robinson, discussed above), Justice Roberts moved directly to addressing the intrusive nature of cellphone searches. In his words, modern "phones are based on technology nearly inconceivable just a few decades ago, when *Chimel* and *Robinson* were decided."[71] Thus, the "categorical rule" set out in *Robinson* (that searches incident to arrest were reasonable as a consequence of the arrest itself)—while striking "the appropriate balance in the context of physical objects"—should not carry "much force with respect to digital content on cell phones."[72] Indeed, while "the two risks identified in *Chimel*—harm to officers and destruction of evidence—are present in all custodial arrests," the Court found that, "[t]here are no comparable risks when the search is of digital data."[73]

According to the Court, exemptions to the warrant requirement must be assessed by balancing "the degree to which [the search] intrudes upon an individual's privacy [with] the degree to which it is needed for the promotion of legitimate governmental interests."[74] In the case of cellphone searches, the Court opined,

> The United States asserts that a search of all data stored on a cell phone is "materially indistinguishable" from searches of these sorts of physical items. That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse.[75]

The Court subsequently elaborated the many traditional devices a cellphone might incorporate ("[t]hey could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers") and focused, at length, on the storage capacity of the devices.[76] Storage capacity was important to the Court, because it related directly to questions of privacy and the intrusiveness of an investigatory search.[77] In sum, the Court's concerns can be summarized as a direct reaction to "the likelihood that an electronic device will contain 1) many kinds of data, 2) in vast amounts, and 3) corresponding to a long swath of time."[78]

First, the Court drew on concerns related to the mosaic theory,[79] finding that, "a cell phone collects in one place many distinct types of information—an

71. *Id.* at 385.
72. *Id.* at 386.
73. *Id.*
74. *Id.* at 385.
75. *Id.* at 393.
76. *See id.* at 393–97.
77. *Id.*
78. United States v. Lichtenberger, 786 F.3d 478, 488 (6th Cir. 2015) (discussing the considerations the Court in *Riley* relied on in determining the need for a warrant to search a cellphone).
79. For more on the mosaic theory, see, for example, Koops et al., *supra* note 18, at 693–95; Bryce Clayton Newell, *Privacy and Surveillance in the Streets: An Introduction*, *in* SURVEILLANCE, PRIVACY AND PUBLIC SPACE 1, 4–6 (Bryce Clayton Newell, Tjerk Timan & Bert-Jaap Koops eds. 2019); Christopher Slobogin, *Making*

address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record."[80] Relatedly, the Court noted that a

> cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet.[81]

Second, the Court found it persuasive that cellphones documented a person's personal life and communication much more pervasively than older technologies, such as a diary, and that this meant it is more likely that law enforcement would be able to find evidence in any given investigation.[82] As noted by the Court, "[a]llowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case."[83]

Additionally, the Court noted that, since cellphones often contained information that was stored elsewhere (for example, in the cloud), allowing police to search these records incident to arrest might allow the search to "extend well beyond papers and effects in the physical proximity of an arrestee,"[84] an important limitation on the exception. And, in response to concerns raised in the underlying cases about cellphone searches essentially amounting to searches of an arrestee's house, the Court stated,

> In 1926, Learned Hand observed . . . that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.[85]

In *dicta*, the Court also rejected prosecutors' proposals that police ought to be able to search cellphones incident to arrest solely for evidence related to the

---

the Most of United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 12–13 (2012); David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381, 402–11 (2013) (raising a number of criticisms of the impact of the mosaic theory on Fourth Amendment law); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 315 (2012) (asserting "as a normative matter, courts should reject the mosaic theory."). The Court has also raised similar concerns in other recent Fourth Amendment cases. *See, e.g.*, United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring); *id.* at 428–31 (Alito, J., concurring); Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (referring to information that was "detailed, encyclopedic, and effortlessly compiled").

80. *Riley*, 573 U.S. at 394.

81. *Id.*

82. *Id.* at 394–95.

83. *Id.* at 395.

84. *Id.* at 398.

85. *Id.* at 396–97 (citation omitted).

crime leading to the arrest or "where an officer reasonably believes that information relevant to the crime, the arrestee's identity, or officer safety will be discovered."[86] These proposed limitations, in the Court's view, "would prove no practical limit at all" or, at least, "impose few meaningful constraints on officers."[87] The Court also rejected the proposal that officers should be able to "search cell phone data if they could have obtained the same information from a pre-digital counterpart," refusing to force courts and officers from engaging on "a difficult line-drawing expedition to determine which digital files are comparable to physical records" on a case-by-case basis.[88] According to the Court,

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life." The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.[89]

*4. Post-*Riley *Case Law*

In the years since *Riley* was decided, hundreds of state and federal cases have cited the decision, many also involving cellphone searches. These cases have ranged from high school principals searching students' phones for text messages,[90] to searches of government employees' cellphones by their supervisors,[91] to officers viewing call logs or text messages or verifying a phone's number,[92] and officers searching parolees' phones during an investigatory detention.[93] Courts have held that certain populations have

86. *Id.* at 399.

87. *Id.*

88. *Id.* at 400–01.

89. *Id.* at 403 (citation omitted).

90. Jackson v. McCurry, 762 F. App'x 919, 927 (11th Cir. 2019) (distinguishing this case, because *Riley* "did not attempt to spell out how its holding could be transposed to the setting of a public school").

91. United States v. Cochran, 682 F. App'x 828, 839 (11th Cir. 2017) (finding that existing precedent did not give supervisor "fair warning" that search was unlawful).

92. *See, e.g.*, United States v. Gary, 790 F.3d 704, 709 (7th Cir. 2015); United States v. Jenkins, 850 F.3d 912, 916 (7th Cir. 2017); United States v. Lustig, 830 F.3d 1075, 1077 (9th Cir. 2016); United States v. Lewis, 615 F. App'x 332, 337–38 (6th Cir. 2015) (finding that *Riley* applied to officer's accessing text messages on an arrestee's cell phone incident to arrest, but that the violation constituted "harmless error" due to the amount of additional evidence the police had acquired from other means); United States v. Govan, 641 F. App'x 434, 435 (5th Cir. 2016); United States v. Blackman, 625 F. App'x 231, 234 (6th Cir. 2015); United States v. Monestime, 677 F. App'x 76, 79 (3d Cir. 2017) (admission of evidence obtained pursuant to officer's search "for recent calls and contacts," conducted pre-*Riley*, was justified by the good faith and independent source exceptions to the exclusionary rule).

93. *See, e.g.*, United States v. Johnson, 875 F.3d 1265, 1275 (9th Cir. 2017) (holding that that a warrantless search of the defendant's phone was not unconstitutional because parolees have a diminished expectation of privacy); United States v. Collier, 932 F.3d 1067, 1073–74 (8th Cir. 2019) (holding that an offender under supervised release has a diminished expectation of privacy, even after *Riley*); United States v. Hathorn, 920 F.3d 982, 975 (5th Cir. 2019) (finding that a special condition allowing probation officer to access probationer's cell phone did not violate the Fourth Amendment); United States v. Jackson, 866 F.3d 982, 983 (8th Cir. 2017)

diminished privacy interests in their phones—for example, a parolee might lose the ability to contest a warrantless search on this basis,[94] but probationers may not, as their interests are not as significantly reduced.[95] Even in the border search context, where law enforcement usually has greater ability to search devices at international entry points, courts, like the Ninth Circuit, have used the reasoning in *Riley* to limit investigatory powers.[96] The Ninth Circuit has also extended *Riley*'s holding that cellphones should not be analogized to traditional "containers" in the contexts of automobile or probation searches.[97]

Additionally, courts have extended *Riley*'s reasoning to searches of other electronic devices, including laptop computers[98] and digital cameras.[99] For example, in *Schlossberg v. Solesbee* (decided pre-*Riley*, but relying on similar reasoning), one district court judge stated,

> it is impractical to distinguish between electronic devices—between a laptop and a traditional cell phone or a smart phone and a camera, before an officer decides whether to proceed with a search of the electronic device incident to arrest. A rule requiring officers to distinguish between electronic devices is impractical. It would require officers to learn and memorize the capabilities of constantly changing electronic devices. A primary goal in search and seizure law has been to provide law enforcement with clear standards to follow. In sum because an electronic device like a camera has a high expectation of privacy in its contents, an officer may not review the contents as a search incident to arrest.[100]

Citing both *Riley* and *Schlossberg*, a federal judge in New York similarly held that searches of digital cameras were comparable to searches of smartphones, due to their "capacity to store a vast number[] of images."[101] However, other courts have come to (arguably) alternate conclusions, for

---

(holding that warrantless search of Jackson's cell phone did not violate the Fourth Amendment because Jackson was serving a term of supervised release and living in a community correctional facility, and that, in these circumstances, Jackson had "no legitimate expectation of privacy in the cell phone").

94. *See, e.g.*, *Johnson*, 875 F.3d at 1275; *Collier*, 932 F.3d at 1073–74; *Hathorn*, 920 F.3d at 975; *Jackson*, 866 F.3d at 983.

95. United States v. Lara, 815 F.3d 605, 610–12 (9th Cir. 2016). The Ninth Circuit held that "while the privacy interest of a probationer has been 'significantly diminished,'" the defendant still "had a privacy interest in his cell phone and the data it contained. That privacy interest was substantial in light of the broad amount of data contained in, or accessible through, his cell phone." *Id.*

96. United States v. Cano, 934 F.3d 1002, 1019–20 (9th Cir. 2019).

97. *Lara*, 815 F.3d at 610–11 (first citing *Riley*, 573 U.S. at 397; and then citing United States v. Camou, 773 F.3d 932, 942–43 (9th Cir. 2014) (finding that a cellphone should not be considered a "container" as part of a reasonable "search of an automobile" or "for purposes of a probation search")).

98. United States v. Lichtenberger, 786 F.3d 478, 487–91 (6th Cir. 2015).

99. *See* Schlossberg v. Solesbee, 844 F. Supp. 2d 1165, 1170 (D. Or. 2012). *Cf.* Am. News & Info. Servs., Inc. v. Gore, No. 12-CV-2186 BEN KSC, 2014 WL 4681936, at *10 (S.D. Cal. Sept. 18, 2014) ("The Supreme Court's recent decision in *Riley v. California* provides some guidance, but leaves the law with regard to cameras unsettled.").

100. *Schlossberg*, 844 F. Supp. 2d at 1170.

101. United States v. Whiteside, No. 13 CR 576 PAC, 2015 WL 3953477, at *4 (S.D.N.Y. June 29, 2015) ("Here, the digital camera provided officers with much of the same information about Whiteside as that obtained by the officers, and used against the defendant, in *Riley*.").

example, in a case involving the search of an arrestee's video cameras on multiple occasions, in which the judge concluded that the "cameras at issue here appear to fall somewhere between the physical search of a cigarette package found in a pocket during a search incident to arrest allowed under *United States v. Robinson*, and the data search of a cell phone under *Riley* that generally requires a warrant."[102]

Decisions such as this, which are in conflict with the reasoning in *Schlossberg*, demonstrate the existing ambiguity in how, or whether, lower courts will seek to differentiate between types of digital devices (for example, based on the specific storage capacity or technical capabilities of different devices).

Several cases (both pre- and post-*Riley*) have held that the police calling a suspect's phone (to verify the number associated with the seized phone and its connection to the suspect) or simply viewing information available on a phone's lock screen did not constitute searches under the Fourth Amendment.[103] These decisions have rested on a distinction between police officers: (1) interacting with the phone at an external level (for example, merely viewing a message on the lock screen or calling the phone's number); and (2) affirmatively opening, manipulating, accessing, or retrieving "any information from *within* the phone."[104]

For example, in *United States v. Brixen*, an undercover detective posing as a fourteen-year-old girl in online conversations with the defendant sent the defendant a Snapchat message just after his arrest to "illustrate that the officers knew why he was there and that he had been interacting with an undercover detective."[105] The Seventh Circuit found that, once a suspect had been arrested, he lost his right to keep his phone in his pocket (out of sight of the officers), and that "just as an individual who fails to conceal a phone's ring from those in earshot does not have a reasonable expectation of privacy, an individual who allows notifications to appear to those in plain sight does not have a reasonable expectation of privacy."[106]

Importantly, the Seventh Circuit read "*Riley* and its progeny" as maintaining "a common thread—they involve law enforcement officers *affirmatively accessing the content within cell phones* to gather evidence against arrestees."[107] Thus, the court held that no Fourth Amendment search had

102. *Am. News & Info. Servs.*, 2014 WL 4681936, at *10 (citation omitted).

103. *See, e.g.*, United States v. Brixen, 908 F.3d 276, 282 (7th Cir. 2018) (sending a Snapchat message to the arrestee's phone and viewing a contemporaneous receipt notification on the lock screen did not constitute a search); United States v. Lawing, 703 F.3d 229, 238 (4th Cir. 2012) (calling a suspect's number twice and hearing the suspect's phone ring both times did not constitute a search).

104. *Brixen*, 908 F.3d at 281 (emphasis added) ("[The officer's] actions simply do not amount to a search of Brixen's cell phone. He did not open or otherwise manipulate Brixen's phone. Nor did he gain access to any of the phone's content or attempt to retrieve any information from within the phone."); *Lawing*, 703 F.3d at 238 ("The police did not attempt to retrieve any information from within the phone.").

105. *Brixen*, 908 F.3d at 279.

106. *Id.* at 282.

107. *Id.* at 281 (emphasis added).

occurred because the detective merely "watched the phone . . . as a Snapchat notification appeared on the screen" and "did not access any content within Brixen's phone, nor did he manipulate the phone in any way before he obtained a search warrant."[108] In sum, "since the phone's content was not affirmatively accessed by law enforcement officers, no search occurred."[109]

In comparison to these cases, in which *officers* have sent signals to an arrestee's phone, the Canadian cases discussed in Part I.B.4 generally address situations where officers view incriminating information—sent by a *third party*—on the lock screen of a phone. As in these Canadian cases, the plain-view exception is relevant in the United States. Indeed, although it did not conduct an explicit plain-view analysis, the *Brixen* court rested its holding on the fact that the investigating officer in that case "only witnessed what was in plain view."[110] Under U.S. law, the "plain-view" doctrine holds that

> if police are lawfully in a position from which they view an object, if its incriminating character is immediately apparent, and if the officers have a lawful right of access to the object, they may seize it without a warrant. If, however, the police lack probable cause to believe that an object in plain view is contraband without conducting some further search of the object—i.e., if "its incriminating character [is not] 'immediately apparent'"—the plain-view doctrine cannot justify its seizure.[111]

Thus, if the police observe information—such as a text message—on the lock screen of an arrestee's phone, for example, they would be justified in seizing the phone on the basis of the plain-view doctrine only if the "incriminating character" of the observed information "is immediately apparent."[112] A subsequent search of the device, however, would generally require a warrant. In such cases, according to the Supreme Court, "the seizure of an object in plain view does not involve an intrusion on privacy."[113] Some courts have interpreted this rule cautiously in the context of police searches of digital data, especially given the privacy-friendly language in cases like *Riley*.[114]

Unsurprisingly, post-*Riley* search-incident-to-arrest cases cover a broad range of factual and legal contexts, as lower courts have had to apply the broad reasoning of *Riley* to a variety of factual scenarios. Across circuits, decisions have not always been consistent and new decisions are being published very frequently, making it impossible to make up-to-date, generalizable statements about the current state of the law. Notably, however, these lower courts have both expanded *Riley*'s privacy-related protections beyond smartphones (for

108. *Id.* at 279.

109. *Id.* at 282.

110. *Id.*

111. Minnesota v. Dickerson, 508 U.S. 366, 375 (1993) (alteration in original) (citations omitted) (quoting Horton v. California, 496 U.S. 128, 136 (1990)).

112. *Id.*

113. *Horton*, 496 U.S. at 141.

114. For example, the Colorado Supreme Court has held that "the plain view exception to the warrant requirement must be applied cautiously in situations involving digital data." People v. Davis, 438 P.3d 266, 271 (Colo. 2019) (interpreting its prior holding in People v. Herrera, 357 P.3d 1227, 1233–34 (Colo. 2015)).

example, applying SCOTUS's reasoning to cases involving laptop computers and digital cameras) and enumerated exceptions or limitations to *Riley*'s holding (for example, based on diminished expectations of privacy). Decisions limiting *Riley*'s applicability have focused on the legal status of the device owner (for example, a probationer), the visibility of the information on the phone's lock screen (something akin to the plain-view exception), and the level of active manipulation of the phone by the police.

B. CANADA

1. Overview of the Search-Incident-to-Arrest Doctrine

In Canada, police searches are largely regulated by Section 8 of the Canadian Charter of Rights and Freedoms (although statutory law also provides the police power to search).[115] The intent of Section 8 is to "protect individuals from unjustified state intrusions upon their privacy."[116] In doing so, Section 8 also protects "the underlying values of dignity, integrity and autonomy."[117]

The Supreme Court of Canada has differentiated between three types of privacy protected by Section 8: personal, territorial, and informational. According to the Court, the Charter protects informational privacy by seeking "to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[118]

In determining whether any search is reasonable, the Supreme Court of Canada analyzes whether the contested "police activity invades a reasonable expectation of privacy."[119] Examining the totality of the circumstances, this involves a two-step test for determining whether subjective expectations of privacy are objectively reasonable, fashioned after the test proposed by Justice Harlan of the United States Supreme Court in *Katz v. United States*.[120] All warrantless searches are prima facie unreasonable.[121] As in the United States, warrantless searches incident to arrest have become the "majority of searches actually conducted by the police" in Canada, even though intended to be an "exception rather than the rule."[122]

---

115. STEPHEN COUGHLAN, CRIMINAL PROCEDURE 93 (2008).

116. *Id.* at 62.

117. R. v. Plant, [1993] 3 S.C.R. 281, 293 (Can.).

118. *Id.* (emphasis added).

119. R. v. Wise, [1992] 1 S.C.R. 527, 533 (Can.).

120. R. v. Edwards, [1996] 1 S.C.R. 128, para. 45 (Can.); *see also* R. v. Tessling, [2004] 3 S.C.R. 432, para. 19 (Can.).

121. COUGHLAN, *supra* note 115, at 81.

122. *Id.* at 97; *see also* Riley v. California, 573 U.S. 373, 382 (2014) ("'[E]xception' is something of a misnomer in this context, as warrantless searches incident to arrest occur with far greater frequency than searches conducted pursuant to a warrant.").

Much like the Fourth Amendment in the United States, Section 8 prohibits agents of the state from conducting unreasonable searches or seizures.[123] In exception to this general rule, Canadian "police have a common law power to search incident to a lawful arrest,"[124] a power developed to promote efficiency in criminal investigations[125] and justified by the state's interest in protecting the safety of officers and others.[126]

At its core, a search incident to arrest is legitimate when the underlying arrest is lawful, the search is truly incidental to the underlying arrest, and the search was conducted in a reasonable manner.[127] According to the Supreme Court of Canada, "[t]his means, simply put, that the search is only justifiable if the purpose of the search is related to the purpose of the arrest."[128] Additionally, and in contrast to the U.S. position in *Robinson* that the search is justified by the fact of the arrest itself, in Canada "the police officer's motives and purposes for the search" are central to the question of whether the search is lawful.[129] "That is, not only must a valid purpose objectively exist, but subjectively the officer must have made an individualized decision to conduct the search for that purpose," otherwise the search is not truly incidental to the arrest.[130] Like in *Robinson*, a valid arrest gives the officer the power to search (without any additional showing of suspicion or cause); however, in Canada, the officer must also be able to explain the purpose of the search and how it related to the arrest.[131] There are three valid purposes: ensuring the safety of police officers or others, preventing the destruction of evidence, and discovering evidence (although, "[t]here remains some ambiguity in the case law over whether this third purpose relates to *any* evidence or is restricted to evidence that may go out of existence if the search was delayed").[132]

The search-incident-to-arrest exception can refer to either items (for example, a cigarette pack) or places (for example, automobiles) to be searched (including the area surrounding the arrestee). "The central guiding principle is that the search must be, as the case law puts it, truly incidental to the arrest."[133] However, some particularly invasive searches, such as taking bodily samples,

123. Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, *being* Schedule B to the Canada Act, 1982, c 11 (U.K.), § 8 ("Everyone has the right to be secure against unreasonable search or seizure.").

124. R. v. Fearon, [2014] 3 S.C.R. 621, para. 1 (Can.).

125. *Id.* at para. 16 ("The cases teach us that the power to search incident to arrest is a focussed power given to the police so that they can pursue their investigations promptly upon making an arrest."); R. v. Beare, [1988] 2 S.C.R. 387, 404 (Can.) (The exception exists "to arm the police with adequate and reasonable powers for the investigation of crime" and because "[p]romptitude and facility in the identification and the discovery of indicia of guilt or innocence are of great importance in criminal investigations").

126. COUGHLAN, *supra* note 115, at 85 (citing R. v. Caslake, [1998] 1 S.C.R. 51, para. 17 (Can.)).

127. *Id.* at 98.

128. *Caslake*, 1 S.C.R. at para. 17.

129. COUGHLAN, *supra* note 115, at 99.

130. *Id.*

131. *Id.* at 102 (citing *Caslake*, 1 S.C.R. at para. 25).

132. *Id.* at 100.

133. R. v. Fearon, [2014] 3 S.C.R. 621, para. 16 (Can.).

are not allowed incident to arrest, as they would constitute a "an 'affront to human dignity.'"[134] Although the power to search incident to arrest does, in some cases, allow officers to search a room, building, or vehicle in the immediate vicinity of the arrestee, the Court of Appeal for Ontario (the highest court in the province) has held that such a power only extends to an arrestee's *home* in exceptional circumstances, due to the arrestee's heightened privacy interest in their home.[135]

In *R. v. Fearon*, the Supreme Court of Canada stated that the permissibility of a search conducted incident to arrest was dependent on "the nature of items seized, the place of search and the time of search in relation to the time of arrest."[136] Thus, "the permissible scope of searches incident to arrest will be affected by the particular circumstances of the particular arrest."[137] In *Cloutier v. Langlois*, the Supreme Court of Canada noted the purposes for which a search incident to arrest was lawful under the Charter, reaffirming the rule that "the police have a power to search a lawfully arrested person and to seize anything in his or her possession or immediate surroundings to guarantee the safety of the police and the accused, prevent the prisoner's escape or provide evidence against him."[138]

2. *Searching Cellphones Incident to Arrest Prior to* Fearon

A number of Supreme Court of Canada cases have dealt with the search and seizure of computers or cellphones in a variety of search contexts. In *R. v. Vu*, for example, the court held that a search warrant for a home cannot extend to searching computers inside the home (if not specified in the warrant) on the traditional theory that receptacles (for example, cupboards and drawers) could be searched, because personal computers should be "treated . . . as a separate place" to be searched, and should require a separate warrant.[139]

Prior to the SCC's 2014 decision in *R. v. Fearon*, Canadian courts had not uniformly applied the search-incident-to-arrest doctrine to cellphone searches. In fact, in *Fearon*, the Supreme Court of Canada identified four different approaches taken by the lower courts. First, some lower courts had allowed cellphone searches incident to arrest—but only "provided that the search is truly incidental to the arrest."[140] Second, at least one decision allowed only "cursory"

134. *Caslake*, 1 S.C.R. at para. 15 (citing R. v. Stillman, [1997] 1 S.C.R. 607, para. 42 (Can.)).

135. R. v. Golub, [1997] 34 O.R. (3d) 743, para. 41 (Can. Ont. C.A.) ("[S]earches of a home as an incident of an arrest, like entries of a home to effect an arrest, are now generally prohibited subject to exceptional circumstances where the law enforcement interest is so compelling that it overrides the individual's right to privacy within the home."); *see also* COUGHLAN, *supra* note 115, at 98.

136. *Fearon*, 3 S.C.R. at para. 13 (citing *Caslake*, 1 S.C.R. at paras. 15–16).

137. *Id.*

138. *Id.* at para. 18 (quoting Cloutier v. Langlois, [1990] 1 S.C.R. 158, 180–81 (Can.)).

139. R. v. Vu, [2013] 3 S.C.R. 657, paras. 48–52 (Can.).

140. *Fearon*, 3 S.C.R. at para. 2 (citing R. v. Giles, 2007 BCSC 1147, paras. 54–55, 62 (Can.); R. v. Otchere-Badu, 2010 ONSC 1059, paras. 81, 83 (Can.); Young v. Canada, 2010 CarswellNfld 388, para. 45 (Can. Nfld. L. Prov. Ct.) (WL); R. v. Howell, 2011 NSSC 284, para. 33 (Can.); R. v. Franko, 2012 ABQB 282, para. 157 (Can.); R. v. Cater, 2014 NSCA 74, para. 161 (Can.); R. v. D'Annunzio, (2010) 224 C.R.R. (2d) 221, paras. 23–24 (Can. Ont. Sup. Ct. J.)).

searches of cellphones.[141] Third, at least two cases held that "thorough 'data-dump' searches are *not* permitted incident to arrest."[142] Fourth, at least one case held that cellphone searches were not permitted at all, "except in exigent circumstances, in which a 'cursory' search is permissible."[143]

In these cases, courts were frequently confronted with arguments that expanding the search-incident-to-arrest doctrine to cellphones (and similar computing devices) would infringe arrestees' "high informational privacy interests"[144] in such devices. According to the defense counsel in one of these cases, "the capacity of electronic storage media to store vast quantities of information creates the potential for large-scale invasions of privacy."[145] However, judges were not always convinced. In a decision among the first set of cases, one trial judge held that a search through emails on the arrestee's phone for the limited purpose of securing evidence related to the underlying crime did not raise reasonable privacy expectations that were "different in nature from what might be disclosed by searching a notebook, a briefcase or a purse found in the same circumstances."[146] Another also found that the search of an unlocked and unencrypted phone raises lesser privacy concerns than a search of an encrypted and password-protected phone.[147]

In the other three sets of cases, courts restricted the ability of police to search incident to arrest to varying degrees. In these cases (and other cases dealing with searches of cellphones outside the search-incident-to-arrest context), judges often focused on the informational privacy interests at stake.[148] In *R. v. Polius*, for example, the judge ruled that a person maintains a "reasonable expectation of privacy in the contents of his/her cell phone" because "[t]he information in a cell phone, computer or other electronic device may relate to aspects of life that are deeply personal."[149] The court held that "the power to seize a cell phone during a [search incident to arrest] where there is reason to believe it may afford evidence of the crime does not include a power to examine

141. *Id.* (citing R. v. Polius, (2009) 196 C.R.R. (2d) 288, para. 41 (Can. Ont. Sup. Ct. J.)).

142. *Id.* (first citing R. v. Hiscoe, 2013 NSCA 48, paras. 68–69 (Can.); and then citing R. v. Mann, 2014 BCCA 231, paras. 118–19 (Can.)).

143. *Id.* (citing R. v. Liew, 2012 ONSC 1826, paras. 124, 144 (Can.)).

144. R. v. Giles, 2007 BCSC 1147, para. 52 (Can.).

145. *Id.* at para. 49.

146. *Id.* at para. 6; *see also* R. v. Otchere-Badu, 2010 ONSC 1059, paras. 84–87 (Can.) (holding that even if a search of a cell phone incident to arrest violated the Charter, the breach was "minimal" and not one that would undermine the reliability or admissibility of the evidence obtained).

147. Young v. Canada, 2010 CarswellNfld 388, para. 40 (Can. Nfld. L. Prov. Ct.) (WL).

148. *See, e.g.*, R. v. Mann, 2014 BCCA 231, para. 118 (Can.) ("It seems to me that downloading the entire contents of a cell phone or smartphone, like the BlackBerrys in this case, seized on the arrest of the accused, after some delay, without a search warrant, can no longer be considered valid under s. 8 of the Charter as a reasonable warrantless search. The highly invasive nature of these searches exceeds the permissible scope for a warrantless search authorized under the common law as a search incident to arrest."); R. v. Polius, (2009) 196 C.R.R. (2d) 288, para. 52 (Can. Ont. Sup. Ct. J.); R. v. T.O., 2010 ONCJ 334, paras. 32–46 (Can.) (WL) ("[T]he Applicant maintained a subjective and objective reasonable expectation of privacy in the photos" found on his cell phone.); R. v. Little, 2009 CarswellOnt 8024, para.147 (Can. Ont. Sup. Ct. J.) (WL) (finding that cell phones raise the same privacy interests as typical computers for search purposes).

149. *Polius*, 196 C.R.R. (2d) at para. 52.

the contents of the cell phone without a prior judicial authorization, absent exigent circumstances."[150]

The judge also analogized a cellphone to a "locked briefcase," stating that "[a] cell phone is the functional equivalent of a locked briefcase in today's technologically sophisticated world."[151] Other cases equated cellphones with traditional computers.[152] This is meaningful, because the Supreme Court of Canada has held that "[i]t is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer."[153] This line of cases led the high court of British Columbia to find (just a few months prior to the Supreme Court's judgment in *Fearon*) that "the law as it stands today no longer permits police to conduct warrantless searches of the entire contents of an individual's cell phone."[154]

In *Fearon*, police arrested Fearon and an associate on suspicion of committing robbery. At the time of his arrest, officers conducted a pat-down search of his person, found a cellphone in his pocket, and conducted a cursory search of the phone.[155] Police also searched his phone again within the next couple of hours. During these searches, police discovered two relevant photos and "a draft text message referring to jewellery and opening with the words 'We did it.'"[156] Fearon argued at trial and on appeal to the Ontario Court of Appeal that the search of his phone violated his rights under Section 8 of the Charter. Both the trial judge and the Ontario Court of Appeals disagreed.

The trial judge found that the arresting officer "was justified in his belief that the cell phone may contain evidence relevant to the armed robbery for which Mr. Fearon was being arrested" and that "there was a reasonable prospect of securing evidence of the offence for which the accused was being arrested in searching the contents of the cell phone."[157] The judge distinguished this initial

150. *Id.* at para. 34.

151. *Id.* at para. 47.

152. R. v. Hiscoe, 2013 NSCA 48, para. 40 (Can.) ("[T]he cell phone in this case was described as akin to a mini-computer capable of storing many gigabytes not unlike personal or home computers . . . .").

153. R. v. Morelli, [2010] 1 S.C.R. 253, paras. 2, 105 (Can.) ("Computers often contain our most intimate correspondence. They contain the details of our financial, medical, and personal situations. They even reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet."); *see also* R. v. Cole, [2012] 3 S.C.R. 34, para. 47 (Can.) ("Computers that are used for personal purposes, regardless of where they are found or to whom they belong, 'contain the details of our financial, medical, and personal situations.' This is particularly the case where, as here, the computer is used to browse the Web. Internet-connected devices 'reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet.'" (citation omitted) (quoting *Morelli*, 1 S.C.R. at para. 105)).

154. R. v. Mann, 2014 BCCA 231, para. 123 (Can.). However, the court did not rule as to the legitimacy of so-called "cursory" searches incident to arrest. *Id.*

155. R. v. Fearon, 2010 ONCJ 645, paras. 19–22 (Can.). Upon finishing the pat down, the arresting officer "'had a look through the cell phone, saw some things in that cell phone, and seized it at that point in time as evidence in relation to the investigation'. He could not recall specifics, but believed that he found some photos in the cell phone at the time, including photos of males and a photo of a gun. . . . He explained that he manipulated the keypad to the extent that he entered into different modes to access text messages and photographs on the phone." *Id.* at para. 21–22.

156. R. v. Fearon, [2014] 3 S.C.R. 621, para. 8 (Can.).

157. *Fearon*, 2010 ONCJ at paras. 43–44.

search of Fearon's phone from the search conducted in *Polius* on the grounds that the officer in the earlier case "did not have a reasonable basis to believe that the cell phone may have been evidence of the alleged murder when he arrested the accused."[158] The judge dismissed the defendant's arguments that phones should be excluded from the search incident to arrest power due to their capacity to store large amounts of personal information, stating

> While there is no doubt that cell phones can contain significant amounts of personal information, the evidence in this case does not lead to the conclusion that Mr. Fearon had an extraordinarily high expectation of privacy in this phone. . . . There is no evidence that the phone was password protected or subject to any security barriers. Nor is there any evidence that it had "mini-computer" capabilities like [phones in earlier cases].[159]

The judge found it particularly persuasive that "[t]he cell phone in this case . . . was not 'locked' and had no password protection or other security walls on it."[160] Concluding, the trial judge stated that

> In my view, an ordinary cell phone objectively commands a measure of privacy in its contents. However, the expectation of privacy in the information contained in the cell phone is more akin to what might be disclosed by searching a purse, a wallet, a notebook or briefcase found in the same circumstances. The evidence in this case is that the LG cell phone appears to have had the functions of cell phone operation, text messaging, photographs and contact lists. While certainly private, the information stored is not so connected to the dignity of the person that this court should create an exception to the police ability to search for evidence when truly incidental to arrest and carried out in a reasonable manner.[161]

On appeal, the Ontario Court of Appeal upheld the trial judge's findings, affirming the reasonableness of the search and the officers' conclusion that evidence of the robbery might be found on the phone.[162] The court noted that they would have found the subsequent searches of the phone at the police station to be attenuated from the arrest, but that they would not overrule the trial judge's findings that those searches were still incidental to the arrest.[163] At a more general level, the court was also unwilling to announce a new rule carving cellphones out of the search-incident-to-arrest power, despite "the highly personal and sensitive nature of the contents of a cell phone and the high

158. *Id.* at para. 45.

159. *Id.* at para. 49.

160. *Id.* at para. 50.

161. *Id.* at para. 51.

162. R. v. Fearon, 2013 ONCA 106, para. 47 (Can.) ("The police had information that the appellant had acted with a second person and that a third person was involved in the stashing of the stolen jewellery. There was therefore a potential for communication among the three suspected participants. In addition, the police had a legitimate concern about the location of the gun and the stolen jewellery. Any communication among the three suspects could lead to the discovery of one or both. In respect of the photographs found in the cell phone, the police knew from experience that robbers will sometimes take photos of the stolen property and even of themselves with the loot.").

163. *Id.* at para. 58.

expectation of privacy that they may attract."[164] In particular, the court reiterated findings from the trial court, stating that "it is significant that the cell phone was apparently not password protected or otherwise 'locked' to users other than the appellant when it was seized"[165]—if it had been, the court noted, police would then need to acquire a warrant prior to conducting a search.[166]

3. Fearon *at the Supreme Court*

On appeal, the Supreme Court of Canada held that warrantless searches of cellphones incident to lawful arrests comply with Section 8 of the Charter only when: (1) the arrest is lawful; (2) the search is truly incidental to the arrest and is conducted for the purpose of protecting the police, the accused, or the public, or to preserve or discover evidence; (3) the nature and the extent of the search are tailored to the purpose of the search; and (4) the police take detailed notes of what they have examined on the device and how it was searched.[167] In doing so, the Court held that the searches conducted in the case were consistent with the existing common law power to search incident to arrest but that the law needed to be modified to ensure it stayed consistent with the Charter.[168]

In its analysis, the Court found that "cell phone searches incidental to arrest may serve important law enforcement objectives," including interests that surpass those of other types of searches in their importance to the state.[169] However, privacy interests were also heightened; indeed, "the search of cell phones, like the search of computers, implicates important privacy interests which are different in both nature and extent from the search of other 'places.'"[170] The court also rejected analogizing cellphones to other types of containers searchable upon arrest (including briefcases or documents):

> It is unrealistic to equate a cell phone with a briefcase or document found in someone's possession at the time of arrest. . . . [C]omputers—and I would add cell phones—may have immense storage capacity, may generate information about intimate details of the user's interests, habits and identity without the knowledge or intent of the user, may retain information even after the user thinks that it has been destroyed, and may provide access to information that is in no meaningful sense "at" the location of the search.[171]

164. *Id.* at para. 72.

165. *Id.* at para. 73.

166. *Id.* at para. 75.

167. R. v. Fearon, [2014] 3 S.C.R. 621, para. 83 (Can.). Subsequently, lower courts have referred to these four requirements as the "Fearon criteria." *See infra* note 186 and accompanying text.

168. *Id.* at paras. 43, 58 ("[M]y view is that the general common law framework for searches incident to arrest needs to be modified in the case of cell phone searches incident to arrest. In particular, the law needs to provide the suspect with further protection against the risk of wholesale invasion of privacy which may occur if the search of a cell phone is constrained only by the requirements that the arrest be lawful and that the search be truly incidental to arrest and reasonably conducted.").

169. *Id.* at para. 49.

170. *Id.* at para. 51 (quoting R. v. Vu, [2013] 3 S.C.R. 657, paras. 38, 40–45 (Can.)).

171. *Id.* (citing *Vu*, 3 S.C.R. at paras. 41–44).

The Court also held that the individual capabilities of a cellphone, whether basic or advanced, should not be a determining factor and that the same test should be applied to both unsophisticated cellphones and smartphones (as well as "other devices that are the equivalent of computers").[172] The Court also largely rejected findings from the lower courts that the use of passwords was tied to the level of privacy interests an accused might have in the phone. "An individual's decision not to password protect his or her cell phone does not indicate any sort of abandonment of the significant privacy interests one generally will have in the contents of the phone. Cell phones—locked or unlocked—engage significant privacy interests."[173]

However, the Court found that cellphone searches did not engage the same level of privacy intrusion as extracting bodily samples or conducting a strip search. While those sorts of searches "are *invariably* and *inherently* very great invasions of privacy and are, in addition, a significant affront to human dignity," cell phone searches are not.[174] According to the Court,

> while cell phone searches—especially searches of "smart phones", which are the functional equivalent of computers—may constitute very significant intrusions of privacy, not every search is inevitably a significant intrusion. Suppose, for example, that in the course of the search in this case, the police had looked only at the unsent text message and the photo of the handgun. The invasion of privacy in those circumstances would, in my view, be minimal. So we must keep in mind that the real issue is the potentially broad invasion of privacy that may, *but not inevitably will*, result from law enforcement searches of cell phones.[175]

The Court rejected a categorical prohibition on warrantless cell phone searches incident to arrest of the kind announced in *Riley*, finding that it was possible to "impose meaningful limits on the purposes, threshold and manner of such searches."[176] In the case at hand, the Court found that the initial search of Fearon's phone violated the Charter, due to the fact that the prosecution could not provide "detailed evidence about precisely what was searched, how and why"[177]—evidence needed to meet the modified test announced by the Court (discussed at the beginning of this Subpart). However, the Court still ruled that the evidence obtained from the search should be admissible.[178]

---

172. *Id.* at para. 52 ("We should not differentiate among different cellular devices based on their particular capacities when setting the general framework for the search power. So, for example, the same general framework for determining the legality of the search incident to arrest should apply to the relatively unsophisticated cellular telephone in issue in this case as it would to other devices that are the equivalent of computers.").

173. *Id.* at para. 53 (citation omitted).

174. *Id.* at para. 55.

175. *Id.* at para. 54.

176. *Id.* at para. 63.

177. *Id.* at para. 87.

178. *Id.* at para. 98. It did so on the grounds that the search was conducted reasonably and in good faith, the evidence obtained was "cogent and reliable," and that Fearon's privacy interests were diminished somewhat on the facts of this specific case. *Id.* at paras. 95–97.

In determining whether a search of a cell phone is incidental to an arrest, the Court stated that,

> [b]oth the nature and the extent of the search performed on the cell phone must be truly incidental to the particular arrest for the particular offence. In practice, this will mean that, generally, even when a cell phone search is permitted because it is truly incidental to the arrest, only recently sent or drafted emails, texts, photos and the call log may be examined as in most cases only those sorts of items will have the necessary link to the purposes for which prompt examination of the device is permitted.[179]

In dissent, Justice Karakatsanis (joined by Justices LeBel and Abella) emphasized the significant privacy interests that individuals have in relation to their computers and smartphones, the search of which can allow the police to see through the "windows to our inner private lives."[180] Indeed, the dissenting Justices noted, "[o]ur digital footprint is often enough to reconstruct the events of our lives, our relationships with others, our likes and dislikes, our fears, hopes, opinions, beliefs and ideas."[181] Therefore, "as technology changes, our law must also evolve so that modern mobile devices do not become the telescreens of George Orwell's *1984*."[182] In contrast to the majority opinion, Justice Karakatsanis argued that cell phone searches were akin to searches of homes or taking bodily samples: "In my view, searches of personal digital devices risk similarly serious encroachments on privacy."[183]

In conclusion, Justice Karakatsanis argued that the evidence should have been excluded. He wrote,

> the high privacy interest individuals have in their electronic devices tips the balance in favour of exclusion. Judicial pre-authorization is an essential bulwark against unjustified infringements of individual privacy. Unwarranted searches undermine the public's confidence that personal communications, ideas and beliefs will be protected on their digital devices. This is particularly important given the increasing use and ubiquity of such technology. It is difficult to conceive of a sphere of privacy more intensely personal—or indeed more pervasive—than that found in an individual's personal digital device or computer. To admit evidence obtained in breach of this particularly strong privacy interest, one of concern to an ever-increasing majority of Canadians, would tend to bring the administration of justice into disrepute.[184]

*4. Post-*Fearon *Case Law*

Since 2014, lower courts have applied the *Fearon* test in a variety of contexts and involving cursory and more detailed searches of arrestees' cell

179. *Id.* at para. 76.
180. *Id.* at para. 101 (Karakatsanis, J., dissenting).
181. *Id.* (Karakatsanis, J., dissenting).
182. *Id.* at para. 102 (Karakatsanis, J., dissenting).
183. *Id.* at para. 104 (Karakatsanis, J., dissenting).
184. *Id.* at para. 197 (Karakatsanis, J., dissenting).

phones.[185] Courts have referred to the four primary requirements laid out in Fearon as the "*Fearon* criteria."[186] Courts have applied these criteria in cases involving cellphones and smartphones of various sorts, as well as computers, tablets,[187] USB flash drives,[188] and GoPro cameras.[189] One general takeaway from *Fearon* that pervades many subsequent cases is the notion that,

> [f]rom *Fearon* we also learn that police are not entitled to navigate through unsettled areas of the law by following the least burdensome route. As a general rule, faced with genuine uncertainty, police should err on the side of caution by settling on a course of action that is more, rather than less respectful of the accused's privacy rights.[190]

As in the United States, some Canadian courts have also made distinctions between searches that involve merely viewing a phone's screen and those that involve manipulation of the phone to view additional contents. In the words of one trial court judge in British Columbia, "[i]t is, in my view, one thing to pick up such a device and to see on an open and visible screen a text conversation. It is quite another to do an in-depth analysis of all of the content."[191] While "picking up the phone and seeing an open screen and visible conversation" might be "no different than picking up a document like a driver's licence or a letter or a note of some sort," manipulating the phone to search through its contents is much more invasive.[192] Another trial court judge found that activating a phone's screen to see if it was locked or to prevent the phone from reverting to a locked state was minimally invasive, while searching through the phone's contents was more "problematic."[193] In another, the fact that incriminating messages were plainly visible on the unlocked screen of the arrestee's phone supported the

185. *See, e.g.*, R. v. Kossick, 2017 SKPC 67, para. 97 (Can.), *aff'd on appeal*, R. v. Kossick, 2018 SKCA 55 (Can.); R. v. Wasilewski, 2016 SKCA 112, paras. 25, 28 (Can.) (holding that the breach of Charter rights was not serious, as law was unsettled at the time and the officer acted in good faith); R. v. Adeshina, 2015 SKCA 29, paras. 27, 29 (Can.) (determining the same); R. v. Emery, 2019 BCSC 702, paras. 91–97 (Can.) (finding that a search was in compliance with *Fearon*, and photographs of search were sufficient under the note-taking requirement); R. v. Byrnes, 2019 ONSC 1287, para. 68 (Can.) ("[P]rivacy protections prohibit investigating cell phones after a routine traffic stop absent extraordinary circumstances.").

186. *See, e.g.*, R. v. Ly, 2016 ABCA 229, para. 18 (Can.); *Kossick*, 2018 SKCA at para. 37.

187. R. v. Harder, 2017 ONCJ 280, para. 56–57 (Can.).

188. *See, e.g.*, R. v. Villaroman, 2018 ABCA 220, para. 17 (Can.) ("*Fearon* . . . elevated the requirement to take notes to a constitutional requirement in cases where a police officer searches an electronic device incident to arrest.") (citing *Fearon*, 3 S.C.R. at para. 82); R. v. Balendra, 2016 ONSC 5143, para. 49 (Can.) ("[T]he search of a USB drive engages many of the same privacy considerations that apply to searches of personal computers.") (citing R. v. Tuduce, 2014 ONCA 547, para. 70 (Can.)), *on appeal at* R. v. Balendra, 2019 ONCA 68, paras. 39–52 (Can.) (applying the *Fearon* criteria to the search of a USB drive incident to arrest, but noting that the note-taking requirement was not as important in this context); R. v. Mahamud, 2019 SKQB 115, para. 40 (Can.) (finding that the officer had not taken notes as required by *Fearon*); R. v. Armstrong and Courchene, 2016 MBQB 134, paras. 36, 45 (Can.) (finding the officers violated the note-taking requirement and that the scope of their search was too broad).

189. R. v. Roy, 2016 ABPC 135, para. 22, 26 (Can.) (finding that a seizure incident to arrest and subsequent, warranted search of camera was lawful).

190. R. v. Tsekouras, 2017 ONCA 290, para. 94 (Can.) (citing *Fearon*, 3 S.C.R. at para. 94).

191. R. v. Khosravi, 2018 BCSC 1791, para. 47 (Can.).

192. *Id.*

193. R. v. Roberto, 2018 ONSC 847, para. 13 (Can.).

officers' claim that the subsequent search of the phone was truly incidental to arrest and was directed at preserving and discovering evidence of the crime underlying the arrest.[194]

However, based on the assertion in *Fearon* that "both locked and unlocked cell phones engage significant privacy interests," one trial judge concluded that, "*Fearon* does not appear to distinguish between a cursory viewing of cell phone messages and those requiring some positive act on the part of the officer."[195] Thus, according to the judge, merely viewing full or partial messages on the lock screen as they arrived could implicate Charter rights under Section 8.[196] Additionally, the judge found that accessing the phone and searching through recent instant messages was subject to the requirements for searches incident to arrest under *Fearon*, regardless of whether the phone was password-protected.[197] Indeed, according to the appellate court, when reviewing the trial court's judgment, applying the "plain view" exception to searches of cellphones is fraught with difficulty, as "simply seeing the cellphone receive a number of messages and reading the names of the persons who had sent them" on the lock screen is often not enough to generate probable cause to seize the device, let alone conduct a more exhaustive search without a warrant.[198] Yet, in other cases, courts have concluded that searches that involved short, focused examinations of an arrestee's smartphone for specific evidence were permissible,[199] while more exhaustive forensic analysis was not.[200]

In *R. v. Marakah*, the SCC was asked to determine when a claimant might have a reasonable expectation of privacy in a text message, even after it was sent to a recipient (although this was not a search-incident-to-arrest case). The SCC held that a suspect could challenge the warrantless search of the recipient's cell phone for messages sent by the suspect. This is so because the suspect can maintain a reasonable expectation of privacy in those messages.[201] Interestingly,

194. R. v. Solano-Santana, 2018 ONSC 2609, para. 62–63 (Can.).

195. R. v. Kossick, 2017 SKPC 67, para. 86 (Can.) (citing *Fearon*, 3 S.C.R. at para. 53).

196. *Id.* ("The search by Cst. Parker in the patrol car, shortly after arrest, involved viewing complete or partial messages as they were being received. The Crown argues those messages were in plain view and that the officer's conduct did not amount to a search subject to the criteria set out in *Fearon*. However, *Fearon* does not appear to distinguish between a cursory viewing of cell phone messages and those requiring some positive act on the part of the officer. For example, both locked and unlocked cell phones engage significant privacy interests." (citing *Fearon*, 3 S.C.R. at para. 53)).

197. *Id.*

198. R. v. Kossick, 2018 SKCA 55, para. 46 (Can.).

199. *See, e.g.*, R. v. Bourdon, 2016 ONSC 2113, para. 383 (Can.) ("What they did not do is telling. They did not answer the incoming call. They did not search to see what, if any, Internet sites had been accessed. They did not read the texts. They did not look at the contacts. They investigated for camera capacity and Internet access, and concluded that search within 3 minutes. Their search was similar to the example set out in para. 54 of *Fearon*. It is in accordance with para. 57 in that there was no routine browsing of the cell phone in an unfocused way."); R. v. Jones, 2015 SKPC 29, para. 62 (Can.) ("The officer performed only a cursory search [limited to recent text messages] and did not stray into other areas or applications on the phone that would not have yielded further evidence of an offence.").

200. *Jones*, 2015 SKPC at para. 71 (finding that downloading and analyzing all content on a phone without a warrant violated *Fearon*'s third criterion).

201. R. v. Marakah, [2017] 2 S.C.R. 608, para. 4 (Can.).

the majority decision in *Marakah* defined the subject matter of the search at issue not as the text message recipient's smartphone, but rather the "electronic conversation" of which the text messages were a part.[202] The majority noted that the "[Section] 8 analysis must be robust" to the reality that where messaging "data are physically or electronically located varies from phone to phone, from service provider to service provider, or, with text messaging more broadly, from technology to technology."[203] Rather than simply looking at the search of a smartphone itself, the Court examined a number of factors that speak to whether the claimant held a reasonable expectation of privacy in the particular search at issue in the case, including "the place where the search occurred . . . the private nature of the subject matter" and whether the claimant maintained some "control over the subject matter."[204] Refusing to limit the place of the search to its origins as a physical, "territorial privacy interest," the majority explained that,

> an electronic conversation does not occupy a particular physical place. All or part of it may be on the sender's phone or the recipient's, or in radio waves or a service provider's database, or on a remote server to which both the sender and the recipient (or the recipients) have access, or some combination of these. This interconnected web of devices and servers creates an electronic world of digital communication that, in the 21st century, is every bit as real as physical space. . . . Although electronic, these rooms are the place of the search.[205]

However, multiple courts have held that the privacy interest a suspect has in their electronic device (and thus, the seriousness of the intrusion by police during a search) is based on the type of information actually contained on the device and accessible to the police, regardless of whether the device itself "clearly ha[s] the potential to contain a great deal of personal information" due to its technological capabilities (for example, storage capacity).[206] As summarized by one Ontario trial court, it is the "informational contents of a cell phone" that give rise to the "important privacy interests" in these cases.[207]

---

202. *Id.* at para. 17 ("To describe text messages as part of an electronic conversation is to take a holistic view of the subject matter of the search. This properly avoids a mechanical approach that defines the subject matter in terms of physical acts, spaces, or modalities of transmission. It also reflects the technological reality of text messaging." (citation omitted)).

203. *Id.* at para. 19.

204. *Id.* at para. 24.

205. *Id.* at para. 28. This is also similar in some regards to language in the *Fearon* decision, that "[i]t is well settled that the search of cell phones, like the search of computers, implicates important privacy interests which are different in both nature and extent from the search of other 'places.'" R. v. Fearon, [2014] 3 S.C.R. 621, para. 51 (Can.) (quoting R. v. Vu, [2013] 3 S.C.R. 657, paras. 38, 40–45 (Can.)).

206. R. v. Balendra, 2019 ONCA 68, para. 72 (Can.); R. v. Ranglin, 2016 ONSC 3972, para. 99 (Can.) ("The only items found on the Blackberry were photographs and five audio recordings. While this information is nevertheless confidential personal information, this limited information obtained by the police, was a limited invasion of privacy which is a factor putting this breach at the middle or lower end of the spectrum.").

207. R. v. Bourdon, 2016 ONSC 2113, para. 358 (Can.).

C. NETHERLANDS[208]

1. Overview of the Search-Incident-to-Arrest Doctrine

In the Netherlands, the power of the police to conduct searches incident to arrest is tied inherently to the powers of the police to seize objects, which are spread across different statutory provisions regulating searches. As the following overview shows, in comparison to the common law systems in the United States and Canada, the Dutch civil law system is characterized by a detailed set of statutory rules that regulate a variety of search-related conduct (including but also expanding well beyond searches incident to arrest). Dutch law regulates different types of frisks,[209] but for the purposes of this Article, the main forms of clothes and body searches are most relevant.

The investigation of clothes has various forms. The least intrusive is frisking for identification purposes (*identificatiefouillering*): investigating officers who stop or arrest a suspect have the power to search the suspect's clothes as well as the objects he or she is carrying at the time, at least insofar as necessary to establish the suspect's identity.[210] If necessary for identifying the suspect, police may also search handbags, suitcases, backpacks, or the personal items in a car—including searching the car's glovebox.[211]

More intrusive is the frisking for investigation purposes (*opsporingsfouillering*), which is regulated in the same provision as the investigation on the body.[212] The prosecutor or assistant prosecutor can order an investigation of the clothes or on the body in the interest of the investigation; this is only allowed in cases of "serious objections" (*ernstige bezwaren*), a term indicating a higher level of suspicion than a "reasonable suspicion" (*redelijke verdenking*, a standard that is similar to probable cause): there must be a high likelihood that the suspect has committed the offense for which he was detained.[213] Also, investigators can examine an arrested suspect's clothes in cases of serious objections, but they are not allowed to search on the body.[214] The most intrusive is a search *in* the body, which we leave aside here since smartphones are (at least now or in the near future) not to be found inside bodies.

For the purposes of this Article, the most relevant question is whether and to what extent law enforcement officers can search (the contents of) objects they

208. This Part is partly based on Bert-Jaap Koops, *Criminal Investigation and Privacy in Dutch Law* (TILT L. & Tech., Working Paper No. 21, 2016), http://ssrn.com/abstract=2837483.

209. *See* Politiewet 2012 [Police Act 2012] (wet van 12 juli 2012, Stb. 2012, 315), art. 7, paras. 3, 5 (regulating safety or security frisks (*veiligheidsfouillering*) and searches on the body of detainees); *id.* at art. 9, paras. 4–5 (regulating frisks of persons to be detained (*insluitingsfouillering*)); Gemeentewet [Municipality Act] (wet van 14 februari 1992, Stb. 1992, 96), art. 151b and 174b (regulating frisking in so-called "safety risk areas").

210. Art. 55b, para. 1 Sv (Neth.).

211. HR 31 mei 2011, ECLI:NL:HR:2011:BP6043 (Neth.).

212. Art. 56, para. 1. Sv; Instellingsbesluit Commissie modernisering opsporingsonderzoek in het digitale tijdperk [Decree Establishing the Committee on Modernizing Criminal Investigations in the Digital Age], 12 juli 2017, Stcrt. 2017, No. 39081, https://wetten.overheid.nl/BWBR0039770/2018-01-01 (Neth.).

213. G.J.M. CORSTENS & M.J. BORGERS, HET NEDERLANDS STRAFPROCESRECHT [THE DUTCH CRIMINAL PROCEDURE LAW] 578 (8th ed. 2014).

214. Art. 56, para. 4, Sv (Neth.).

have seized in the context of a clothes or body search. This question is particularly relevant to smartphones that are seized by investigation officers in circumstances that do not require authorization from a prosecutor or judge. The traditional doctrinal answer to this question is simple: it is inherent to the seizure power—and implicitly embedded in the provisions on seizable items and seizure of goods incident to arrest[215]—that seized objects can be investigated in order to bring to light the truth.[216] Traces on the object (for example, fingerprints) may be secured, and their contents may be investigated. Absent a specific rule that indicates otherwise, this general rule would also apply to smartphones, laptops, and other computer devices.

2. Searching Cell Phones Incident to Arrest Prior to the "Smartphone Judgment"

Until relatively recently, Dutch law followed the doctrine that computers simply were part of the traditional doctrine that the rules on seizure implicitly allow searching contents of seized objects.[217] However, as smartphones grew in functionalities and data-processing capacities, questions arose whether it was acceptable to legitimate the privacy interference of computer searches incident to arrest implicitly on the basis of general rules without particular safeguards. The under-regulation of these searches (in particular, searches of smartphones) led to a split in lower courts' case law. While courts had been following the traditional rule, in 2015, the Court of Appeal Arnhem-Leeuwarden passed a forcefully formulated verdict breaking with this line.[218] They determined that a police investigation of a seized smartphone violates article 8 of the European Convention on Human Rights (ECHR):[219]

> The seizure, investigation of the smartphone and the copying of data from the smartphone by the police on the basis of art. 94 CCP infringe the right to protection of privacy established in article 8 ECHR. The police competence to infringe this right must written down in the law in a sufficiently knowable and foreseeable manner.
>
> The technological developments current in 2015 imply that a smartphone does not only provide access to traffic data, but also to the contents of communications and private information of the smartphone's user. And this without any form of prior assessment of the subsidiarity and/or proportionality of the competence. This leads the court of appeal to determine that this is such an intrusive competence that, also taking into account art. 1 CCP [the legality principle], the general description of the competence of article 94 CCP can

215. Art. 94 Sv (Neth.) (defining which items can be seized in the context of criminal procedure); Art. 95 Sv (Neth.) (regulating seizure of goods incident to arrest).

216. CORSTENS & BORGERS, *supra* note 213, at 541.

217. HR 29 maart 1994, ECLI:NL:HR:1994:AD2076 (Neth.); HR 20 februari 2007, ECLI:NL:HR:2007:AZ3564 (Neth.).

218. Hof Arnhem-Leeuwarden 22 april 2015, ECLI:NL:GHARL:2015:2954 (Neth.).

219. COUNCIL OF EUR., EUROPEAN CONVENTION ON HUMAN RIGHTS art. 8 (establishing the right to protection of private and family life, home and correspondence, and requiring interferences with this right to be foreseeable by law and necessary in a democratic society).

> nowadays no longer be deemed to be a legislative precept that can be deemed sufficiently knowable and foreseeable when exercising the competence. Therefore, it cannot (any longer) pass the test of article 8 ECHR. The court therefore agrees with the defence that the investigation by the police of the smartphone's contents violates his right to privacy.[220]

This judgment was quoted and followed by the District Court Noord-Holland.[221] However, a mere three weeks later, and without much argument, a different section of the same court stuck to the old doctrine, considering a police search of a smartphone incident to arrest to be lawful under the existing seizure provisions.[222] The District Courts of Oost-Brabant and Limburg also upheld the existing doctrine that article 94 CCP provides a sufficient basis for warrantless investigations of a seized smartphone.[223] The divergence in case law caused considerable legal uncertainty for law enforcement authorities, so that—in the absence of legislative reform, which would be the normal route in the Dutch civil law system to change the doctrine but would likely take years—a judgment by the Supreme Court was eagerly awaited.

3. The "Smartphone Judgment" at the Supreme Court

On April 4, 2017, the Dutch Supreme Court passed three judgments on smartphone searches incident to arrest, which contained the same—extensive—general reasoning, only differing in minor details based on the application to the facts of each case.[224] Collectively, these judgments have become known as "the smartphone judgment" (*het smartphonearrest*).[225]

Basically, the Supreme Court followed the Arnhem-Leeuwarden court in breaking with the doctrinal interpretation that smartphone searches were implicitly allowed under the traditional rules of search and seizure;[226] it did not, however, go as far as to require warrants for all smartphone searches. Based on Art. 8 ECHR, which requires privacy interferences to be "foreseeable by law," the court held that the general provisions on seizure (articles 94–95 CCP) only

220. Hof Arnhem-Leeuwarden 22 april 2015, ECLI:NL:GHARL:2015:2954 (Neth.).

221. Rb. Noord-Holland 4 juni 2015, ECLI:NL:RBNHO:2015:4660 (Neth.) (finding a police search of a burglary arrestee's phone, discovering three photos in the WhatsApp image folder of weapons—not directly connected to the burglary—unlawful).

222. Rb. Noord-Holland 26 juni 2015, ECLI:NL:RBNHO:2015:5447 (Neth.).

223. Rb. Oost-Brabant 5 juni 2015, ECLI:NL:RBOBR:2015:3228 (Neth.); Rb. Limburg 28 oktober 2015, ECLI:NL:RBLIM:2015:9128 (Neth.).

224. HR 4 april 2017, ECLI:NL:HR:2017:584 (Neth.); HR 4 april 2017, ECLI:NL:HR:2017:588 (Neth.); HR 4 april 2017, ECLI:NL:HR:2017:592 (Neth.). Nos 584 and 588 concerned an appeal of judgements by the Court of Appeal Amsterdam that had upheld the traditional doctrine; No. 592 was the appeal of the Arnhem-Leeuwarden Court of Appeal's judgement that rejected the old doctrine. In the following, we refer to the latter judgement as illustrative of all three.

225. COMMISSIE MODERNISERING OPSPORINGSONDERZOEK IN HET DIGITALE TIJDPERK [COMMITTEE ON MODERNIZING CRIMINAL INVESTIGATIONS IN THE DIGITAL AGE], REGULERING VAN OPSPORINGSBEVOEGDHEDEN IN EEN DIGITALE OMGEVING [REGULATION OF INVESTIGATIVE POWERS IN A DIGITAL ENVIRONMENT], RIJKSOVERHEID [GOV'T OF THE NETH.] (June 2018), 6 (Neth.), https://www.rijksoverheid.nl/documenten/rapporten/2018/06/26/rapport-commissie-koops---regulering-van-opsporingsbevoegdheden-in-een-digitale-omgeving [hereinafter COMMITTEE ON MODERNIZING].

226. HR 4 april 2017, ECLI:NL:HR:2017:592, para. 4.4–4.5 (Neth.).

allowed smartphone searches by police officers if the search can be considered to constitute a limited privacy intrusion:

> To establish the truth, seized objects may be searched in order to obtain data for the criminal investigation. Data stored in or available to computers are no exception to this (…). This also applies to data stored in or available to other seized electronic data carriers and computers, such as smartphones. The legal basis for this investigation by investigative officers lies in the combination of the provisions on which the power to seize is based.
>
> For an investigative officer to investigate seized electronic data carriers and computers in order to obtain data stored therein or available thereto, the law does not require prior assessment by a judge or intervention by a public prosecutor. If the privacy infringement of the investigation can be considered limited, the general power of investigative officers, stipulated in art. 94, in combination with art. 95 and 96 CCP, offers sufficient legitimation for this. This can be the case if the investigation only consists in consulting a small number of specific data stored on or available to the electronic data carrier or computer.[227]

The inclusion of "or available to" suggests that smartphone searches may also consist in investigations of remotely stored data accessible through the phone, for example, in the cloud (provided that territory-based investigative jurisdiction is respected, of course).

However, the Court went on to say, for more serious privacy intrusions, the general seizure provisions are insufficient for smartphone searches without further authorization:

> If the investigation goes as far as to result in a more or less complete image being obtained of certain aspects of the data carrier or computer user's private life, the investigation might be unlawful vis-à-vis him. This can especially be the case if it concerns investigating with use of technical tools all data stored in or available to the electronic data carrier or computer.
>
> Given this, the view that Article 94 CCP always as such provides an adequate legal basis for an investigation officer's investigation of a seized smartphone, is incorrect.[228]

In expressing when an investigative action may constitute a more than limited privacy intrusion, the court used a criterion used elsewhere in statutory law on investigation powers, namely "systematicness" (*stelselmatigheid*).[229] This criterion entails that a more than limited privacy intrusion occurs when an investigation power is applied in a way that is "systematic," which is the case if it results in "a more or less complete image being obtained of certain aspects of someone's [private] life."[230] The use of this criterion was surprising (because it had been limited only to visual observation and intelligence-gathering powers),

227. *Id.* at para. 3.4.
228. *Id*. at para. 3.4–3.5.
229. Article 126g, para. 1, SV (Neth.); Article 126j, para. 1, SV (Neth.).
230. COMMITTEE ON MODERNIZING, *supra* note 225, at 132–33.

but might be considered appropriate because it was one of the prevalent conceptualizations of privacy in Dutch law. The criterion resonates with the mosaic theory, the "more or less complete image" functioning similarly as the "mosaic picture" in the mosaic theory.[231] Thus, the judgment also resonates with the U.S. Supreme Court's reasoning in *Riley*.[232] Similarly, the Canadian focus on protecting a "biographical core of personal information" is also aimed at limiting police investigations that tend to "reveal intimate details of the lifestyle and personal choices of the individual."[233]

An important difference with *Riley*, however, is that "systematicness" functions to distinguish between limited and more than limited searches, and not to identify when a warrant (or similar forms of judicial authorization under Dutch law) is required. The Dutch Supreme Court spent far fewer words on how privacy-invasive a smartphone search can be, and left it rather open when a judicial authority should authorize a smartphone search incident to arrest. A more than limited privacy intrusion requires some form of prior authorization, but this can be an order from a prosecutor or authorization from an investigatory judge. Both powers of public prosecutors and powers of investigatory judges are deemed sufficient to legitimate searches that yield a more or less complete image of certain aspects of the phone user's private life.[234] Whether a police officer desiring to investigate the contents of a seized smartphone should seek permission from a prosecutor or (through the prosecutor) from an investigatory judge, was largely left to practice. The only guidance that the Supreme Court gave was the statement that "in light of art. 8 ECHR, an investigation by the investigative judge can especially be thought of in cases where it is foreseeable in advance that the privacy infringement will be very serious."[235]

The Court did not elucidate which types of investigations constitute "very serious" privacy interferences. Neither, for that matter, did they articulate when exactly a search yields a more or less complete image of aspects of the user's private life. The only guideline is the observation that if the court (that would re-judge the quashed case) were to find that in the case, all data on the smartphone and/or the SIM card had been retrieved using hardware and/or software (and possibly manually looked at as well) so that "[complete] insight has been obtained in contacts, call history, messages, and photos, this will give rise to the presumption that a more than limited privacy interference has occurred."[236] Although one could easily imagine that such comprehensive insight should definitely be considered a "very serious" privacy interference, the court refrained from making such a statement.

231. *Cf.* Bert-Jaap Koops, *The Mosaic Spheres Theory of Privacy Protection* (forthcoming) (discussing the Dutch "systematicness" criterion as an (implicit) example of the mosaic theory).

232. *Riley*, 573 U.S. at 403.

233. R. v. Plant, [1993] 3 S.C.R. 281, 293 (Can.).

234. HR 4 april 2017, ECLI:NL:HR:2017:592 (Neth.).

235. *Id.*

236. HR 4 april 2017, ECLI:NL:HR:2017:584 (Neth.); HR 4 april 2017, ECLI:NL:HR:2017:588 (Neth.).

Altogether, the Supreme Court left a very considerable grey area between "consulting a small number of specific data"[237] (as a limited privacy interference) and "investigating with use of technical tools all data"[238] (as a presumably more than limited privacy interference), and between more than limited and "very serious"[239] privacy interferences.

4. Post-"Smartphone Judgment" Case Law

Several dozens of Dutch judgments have been published that refer to and apply the "smartphone judgment."[240] The general impression arising from these post-smartphone judgment cases is that, so far, courts tend to downplay the privacy interest and seldom find a smartphone search conducted by police to constitute a very serious privacy interference, as the following examples show.

In many cases, courts hold that a smartphone search only concerned a limited privacy intrusion, particularly because, apparently or presumably, only few files had been investigated.[241] For example, searching for a contact in the WhatsApp contact list and making a screenshot of the associated profile picture is a limited search,[242] as is searching a suspect's phone for confirmation of information found on a victim's phone and finding some WhatsApp messages and conversations between suspect and victim as well as a photograph of the victim.[243] Manually searching (scrolling) and looking at several videos was also held a limited privacy intrusion (even though two of these had been filmed inside a home),[244] as was targeted looking at pictures in the photo gallery.[245] One court even held that a large data set did not yield a more or less complete image of certain aspects of the suspect's private life (and thus, was a limited privacy intrusion), arguing that most of the contacts found concerned first names or nicknames (further investigation into these persons largely having proved fruitless), that the suspect's Facebook, WhatsApp, email, text messages, Internet history, and photos had a "very fragmented character," and that "no

237. HR 4 april 2017, ECLI:NL:HR:2017:592 (Neth.).

238. COMMITTEE ON MODERNIZING, *supra* note 225, at 6.

239. *See supra* note 228 and accompanying text.

240. COMMITTEE ON MODERNIZING, *supra* note 225, at 6.

241. *See, e.g.*, HR 14 november 2017, ECLI:NL:HR:2017:2869 (Neth.) in combination with Parket HR 26 september 2017, ECLI:NL:PHR:2017:1245 (Neth.) (finding that apparently only few files had been consulted, given that the police officer manually investigating the smartphone had only seen that the suspect had various missed calls, messages, and WhatsApp messages (and accidentally seeing a new message coming in a day after the arrest, which triggered a search of the suspect's home)).

242. Hof Den Haag 11 juli 2018, ECLI:NL:GHDHA:2018:2167 (Neth.).

243. HR 26 juni 2018, ECLI:NL:HR:2018:1013 (Neth.) in combination with Parket HR 15 mei 2018, ECLI:NL:PHR:2018:683 (Neth.).

244. HR 23 januari 2018, ECLI:NL:HR:2018:71 (Neth.) in combination with Parket HR 28 november 2017, ECLI:NL:PHR:2017:1470 (Neth.).

245. HR 10 juli 2018, ECLI:NL:HR:2018:1121 (Neth.) and Parket HR 15 mei 2018, ECLI:NL:PHR:2018:764 (the Advocate-General, in his advisory opinion in this case, observing that the privacy intrusion of targeted looking at pictures may be more than minor if it concerns "very many photographs," but that—absent evidence that the police officer looked at very many pictures—there was no indication that the case involved a more than limited privacy intrusion).

communications of a personal character" were found.[246] Other factors favoring a conclusion of limited privacy interference include that the particular type of phone has limited functionality[247] or that messages have a business rather than personal character.[248]

While many cases thus concern minor privacy intrusions, we found only two cases involving a "very serious" privacy intrusion. Following the smartphone judgment, a public prosecutor requested that an investigative judge authorize a smartphone search in the so-called "sex bailiff" case (featuring a bailiff who compelled debtors to pay "in kind" rather than in cash).[249] The investigative judge agreed with the prosecutor's assessment that the investigation of the bailiff's smartphone could uncover "certain photos, images, and other files" that could constitute a very serious interference with the suspect's privacy, and authorized the search because of the serious character of the suspected sexual and official crimes.[250] The other case also involved investigation of a sexual offense, namely uploading to public porn sites a covertly recorded video of (consensual) sex between the suspect and the victim.[251] Since the suspect was an attorney, the public prosecutor expected that not only sexual images but also privileged information might be encountered in the search, and therefore requested permission from the investigatory judge.[252] The District Court of Noord-Holland stipulated that such permission should be granted, provided that the search remain limited to several precise, offense-specific search terms (additional search terms requiring separate permission) and that it be conducted by a technical expert who was not part of the investigation team.[253]

Given the Dutch Supreme Court's mention that a privacy intrusion can be more than limited especially "if it concerns investigating with use of technical tools all data,"[254] courts frequently mention the use of automated search tools as a possibly relevant factor—often to argue *a contrario* that a search was manual and hence not very intrusive.[255] Even if all data are automatically copied from a smartphone, courts still consider that the privacy interference is limited, as the

246. Hof Amsterdam 13 oktober 2017, ECLI:NL:GHAMS:2017:4153 (Neth.).

247. Hof Amsterdam 14 december 2018, ECLI:NL:GHAMS:2018:4610 (Neth.) (holding that a so-called "PGP phone" (a Blackberry using the Pretty Good Privacy encryption application) only served to make notes or send messages, but did not allow calling or making photographs, so that many aspects of private life could not be pictured by the phone).

248. *Id.* (observing that, as apparent from message contents, communication was read with business relations, constituting very limited interference with private life); *see also* Hof Amsterdam 13 oktober 2017, ECLI:NL:GHAMS:2017:4153 (Neth.) (emphasizing that, as far as call or message contents could be distilled, these concerned business correspondence).

249. Rb. Limburg 8 mei 2017, ECLI:NL:RBLIM:2017:4484 (Neth.).

250. *Id.*

251. Rb. Noord-Holland 29 juli 2019, ECLI:NL:RBNHO:2019:6764 (Neth.).

252. *Id.* at 3.

253. *Id.* at 3–4.

254. Hof Arnhem-Leeuwarden 22 april 2015, ECLI:NL:GHARL:2015:2954 (Neth.).

255. HR 14 november 2017, ECLI:NL:HR:2017:2869 (Neth.) in combination with Parket HR 26 september 2017, ECLI:NL:PHR:2017:1245 (Neth.).

following examples make clear. One court argued that making a mirror copy of the smartphone data and then using automated tools to investigate the data does not necessarily constitute "systematicness":[256] technical tools "can also, or perhaps rather, enable a limited search. Specifically, one can think of a search into a limited period or particular groups of files."[257] Another court simply, and in our view erroneously, argued that a search using forensic software tools of all textual data copied from an iPhone constituted only a minor privacy interference because the police officers "only investigated those data that they considered relevant to the investigation. It has not been substantiated that the phone was investigated for other purposes than finding evidence of the case for which the suspect was arrested."[258] This would suggest that any search of smartphone data could be conducted by police officers without higher authorization, as long as the search is targeted to the case at hand; that would effectively do away with privacy protection in criminal procedure.

One important aspect of the Dutch post-smartphone judgment case law is that courts only seem to consider the privacy infringement of smartphone files that were eventually used in the case. They seldom consider how narrow or broad a search actually was, perhaps for lack of insight into what police officers actually did when searching the phone. This outcome-oriented rather than process-oriented perspective features in many cases, perhaps most visibly in the Amsterdam Court of Appeal's judgment that the large data set that the police had found turned out not to tell too much about the suspect's personal life, because of the "fragmented" and business character of the contents.[259] However, one could easily imagine that the Blackberry's contact list could have contained not only first names and nicknames, but many full names, that more pictures might have been found than "a few pictures of the suspect with other women" (that is, other than his wife), which in itself might, in certain cases, already be considered a more than minor privacy infringement), and particularly that the suspect's Facebook, WhatsApp, email (with attachments), text messages, Internet history, and photos on the suspect's smartphone (a Samsung S4) might have revealed more than "fragmented" information about his private life.[260] It is highly questionable to argue that some search activity constituted only a minor privacy intrusion if the information the search yields does not show a more or less complete image of certain aspects of someone's private life; rather, the intrusiveness of the search ought to be based on an *ex ante* assessment of what the search is, in the circumstances, reasonably likely to yield in terms of information about private life.

256. COMMITTEE ON MODERNIZING, *supra* note 225, at 81 (discussing systematicness).

257. Gemeenschappelijk Hof van Justitie van Aruba, Curaçao, Sint Maarten en van Bonaire, Sint Eustatius en Saba 5 oktober 2017, ECLI:NL:OGHACMB:2017:197 (Neth.). Relevant in this case was the fact that the suspect, when asked what private information the smartphone contained, could only remember a couple of pictures, so that automatically targeted searches might perhaps still be "systematic" if the phone evidently contains much private information. *Id.*

258. Hof's-Hertogenbosch 7 juli 2017, ECLI:NL:GHSHE:2017:3151 (Neth.).

259. Hof Amsterdam 13 oktober 2017, ECLI:NL:GHAMS:2017:4153 (Neth.).

260. *Id.*

Another striking, related aspect in Dutch case law is the focus on the privacy intrusion of the items that end up in the criminal file: courts do not seem to consider whether or not police officers have looked at, and taken knowledge of, many other smartphone items that they considered uninteresting or irrelevant to the case. It is plausible to argue that searching in the contact list for a particular contact, and finding a photo of the victim of a sexual offense on the suspect's phone, are limited privacy intrusions; but if it is unknown what the police looked at in order to find these particular items, and what else they may have looked at, can one plausibly argue that the search, as such, was a minor privacy intrusion? From one administrative case, we can surmise that police investigations of seized smartphones may well involve a far broader range of items than the incriminating one(s) ending up in the criminal file.[261] In this case, the plaintiff requested deletion of data from police records, arguing that the investigation of her seized smartphone had constituted a more than minor privacy interference and was therefore unlawful, given that the criminal file in the case against her contained one WhatsApp conversation with her son (featuring thirteen messages), parenthetically mentioning that "the entire printout of the file [of WhatsApp and text messages found on the seized phone] consists of 343 pages and was not included" in the file.[262] The request was denied, both for procedural reasons and because the smartphone had been seized with authorization from the investigative judge (which surely covered the privacy intrusion of the investigation).[263] However, the case is interesting because it shows that, even if only one WhatsApp conversation or text message is included in the file, the investigation may well have involved looking through all the conversations and messages on the phone—which to us definitely seems a more than limited privacy intrusion.

One reason for this narrow perspective on privacy intrusiveness is the fact that courts generally argue that the privacy harm of a smartphone search consists of a police officer having been able to take knowledge of contents, but that the defense has not demonstrated that "taking knowledge of the suspect's private data by the police officers has led, other than in the framework of the investigated criminal case, to any further dissemination of private data or any other concrete prejudice."[264] This is not to say that there is no privacy intrusion when police officers get to see private information, but the fact that data have only been seen by investigating officers and have not further spread is a reason for courts to consider the privacy violation to be excusable. This is all the more so since almost all cases concern investigations that happened prior to the smartphone judgment, so that police officers acted in good faith under then-

261. Raad van State 6 juni 2018, ECLI:NL:RVS:2018:1807 (Neth.).

262. *Id.* at 9.

263. *Id.*

264. Hof Den Haag 22 juni 2017, ECLI:NL:GHDHA:2017:2325 (Neth.), *confirmed by* HR 10 juli 2018, ECLI:NL:HR:2018:1119 (Neth.). Similar reasoning and language is used in, for example, Hof's-Hertogenbosch 17 oktober 2017, ECLI:NL:GHSHE:2017:4433 and Hof Arnhem-Leeuwarden 22 maart 2019, ECLI:NL:GHARL:2019:2508 (Neth.).

applicable law. Also, courts point to a (somewhat gratuitous, in our opinion) statement by a public prosecutor that she would certainly have given authorization for the smartphone search, had she been asked at the time.[265] As a result of these factors, even if courts consider that the authorization-lacking smartphone search constituted a more than minor privacy intrusion,[266] they do not attach legal consequences to the privacy violation, other than noting that it happened.[267] This is in line with the general finding that Dutch criminal procedure, with its limited sanctioning of unlawfully obtained evidence, tends to be pragmatic, placing more importance on fighting crime than protecting privacy.[268]

5. Statutory Reform: Modernizing the Dutch Code of Criminal Procedure

In 2014, the Dutch government started a large-scale process to modernize the Code of Criminal Procedure, which dates from 1926 and, partly because the many amendments and changes since 1926 make it hard to see the forest for the trees, there is a need to update it in integral fashion.[269] Another reason for modernization is the increasing role and special characteristics of digital investigations, and the fact that current law is not well-aligned to the realities of digital investigation practice. Computer searches incident to arrest are illustrative of this, as the Minister of Justice recognizes in the so-called Contour Memorandum:

> It is hard to justify that the investigation of a computer and securing data stored thereon during a search is covered by specific safeguards, while if that same computer would have been seized during the search, the investigation of that seized computer and the securing of the data stored thereon is not surrounded by similar safeguards. Moreover, on the basis of the separate seizure powers for investigation officers, for example with stopping and arrest, current law does not foresee in authorization from a higher authority for investigating for instance a seized smartphone and taking knowledge of the data stored thereon. . . . In this light, I consider it necessary to further regulate the investigation of seized electronic data carriers and the securing of the data stored thereon for investigation purposes. I am thinking of the requirement

265. *See, e.g.*, Rb. Limburg 2 juni 2017, ECLI:NL:RBLIM:2017:5133; Hof Arnhem-Leeuwarden 22 maart 2019, ECLI:NL:GHARL:2019:2508 (Neth.).

266. *See, e.g.*, Hof's-Hertogenbosch 17 oktober 2017, ECLI:NL:GHSHE:2017:4433 (Neth.) (finding that the copying of all data from a Blackberry phone and a notebook and the analysis of the images, video files, chats, emails, Internet history, and Skype data could yield a more or less complete image of certain aspects of the suspect's private life).

267. *See* HR 10 juli 2018, ECLI:NL:HR:2018:1121 (Neth.); Parket HR 15 mei 2018, ECLI:NL:PHR:2018:764 (Neth.); Hof Amsterdam 13 oktober 2017, ECLI:NL:GHAMS:2017:4153 (Neth.).

268. Parket HR 26 September 2017, ECLI:NL:PHR:2017:1245 (Neth.).

269. *See Toespraak van minister Opstelten 1e Congres Modernisering Wetboek van Strafvordering [Speech by Minister Opstelten at the 1st Congress on Modernizing the Code of Criminal Procedure]*, RIJKSOVERHEID [GOV'T OF THE NETH.] (June 19, 2014) (Neth.), https://www.rijksoverheid.nl/documenten/toespraken/2014/06/19/toespraak-van-minister-opstelten-bij-het-congres-modernisering-wetboek-van-strafvordering

> that a higher authority decides on investigating the seized electronic data carrier and the securing of the data stored thereon. . . .[270]

A discussion memorandum on search and seizure explained just how intrusive computer investigations are:

> Taking knowledge of and securing the email correspondence, photos and videos, personal notes and Internet search history stored on a data carrier can, separately or combined, seriously interfere with the subject's privacy. Compare the seizure of all photo albums, all video tapes, all personal letters, all personal notes (diaries) of a person suspected of for example drug trafficking. Such a seizure would easily be deemed disproportional.[271]

Here, the argumentation compares investigating a seized smartphone or other type of computer with a very extensive use of seizure of objects normally stored in the home, and thus implicitly compares computer searches with dwelling searches (echoing the U.S. Supreme Court's argumentation in *Riley*). It is therefore surprising that the memorandum and the subsequent draft Bill proposed that the Public Prosecutor would be the main authority with power to authorize smartphone searches incident to arrest rather than the investigatory judge—who is the regular authority to decide on dwelling searches.[272] The draft Bill triggered considerable criticism from practitioners in the consultation stage on its regulation of digital investigation powers, including on the designation of the Public Prosecutor as the default authority for all investigations of digital devices (which would seem to offer too much protection for very simple devices, such as a bike chip with only an identification number, and possibly too little for extensive smartphone searches).[273] In the meantime, the Supreme Court also passed the "smartphone judgment,"[274] suggesting that "very serious" privacy interferences require authorization from the investigatory judge, also raising questions on the proposed draft Bill's provisions. As a result, the government decided to install a committee to examine and advise them on the regulation of digital investigation powers in the modernized Code.[275]

---

270. KAMERSTUKKEN II 2015–16, 29 279, no. 278, 63–64 (Neth.).

271. *Discussiestuk: Onderzoek ter plaatse, inbeslagneming en doorzoeking en onderzoek van gegevensdragers en in geautomatiseerde werken (Boek 2) [Discussion Paper: On-Site Investigation, Seizure, Search and Investigation of Data Carriers and in Computers (Book 2)]*, 37 DOCPLAYER (June 4, 2014) (Neth.), https://docplayer.nl/6697301-Discussiestuk-onderzoek-ter-plaatse-inbeslagneming-en-doorzoeking-en-onderzoek-van-gegevensdragers-en-in-geautomatiseerde-werken-boek-2.html.

272. *See id.* at 52; *see also Concept Wetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek [Draft Bill Establishing Book 2 of the New Code of Criminal Procedure: Criminal Investigation]*, RIJKSOVERHEID [GOV'T OF THE NETH.], 13 (Feb. 2017) (Neth.), https://www.rijksoverheid.nl/documenten/kamerstukken/2017/02/07/wetsvoorstel-tot-vaststelling-van-boek-2-van-het-nieuwe-wetboek-van-strafvordering [hereinafter *Bill Establishing Book 2*].

273. COMMITTEE ON MODERNIZING, *supra* note 225, at 6, 81.

274. *Id.* at 7.

275. *Instellingsbesluit Commissie modernisering opsporingsonderzoek in het digitale tijdperk [Decree Establishing the Committee on Modernizing Criminal Investigations in the Digital Age],* OVERHEID [GOV'T] (July 12, 2017), Stcrt. 2017 No. 39081 1 (Neth.), https://wetten.overheid.nl/BWBR0039770/2018-01-01.

This Committee on modernizing criminal investigation in the digital age[276] recommended applying a general criterion for assessing the intrusiveness of digital investigations, to searches of smartphones and laptops incident to arrest, as well as to computer investigations during searches of dwellings and other premises, and to various special investigation powers such as data production orders and open-source intelligence.[277] Their proposed general criterion followed the existing criterion of "systematicness"[278] and elaborated this into a threefold distinction of (profound) systematicness:

- non-systematicness: a minor privacy intrusion;
- systematicness: when (reasonably foreseeably) a more or less complete picture arises of certain aspects of someone's private life;
- profound systematicness: when (reasonably foreseeably) a more or less complete picture arises of a) an essential [*wezenlijk*] part of someone's private life ("deep") or b) a substantial part of someone's private life ("broad").[279]

The committee tied these three degrees of intrusiveness to different authorization levels, requiring approval from the police, public prosecutor, and investigatory judge, respectively.[280] Other conditions may apply to approval as well, such as differentiated levels of suspicion, types of offenses, and subsidiarity requirements.[281]

The committee's advice was taken up in the revised draft Bill of October 2018, which adopted the threefold criterion of (profound) systematicness in the proposed regulation of, *inter alia*, computers seized incident to arrest.[282] According to the draft Explanatory Memorandum, the use of this criterion follows the committee's advice, the Dutch Supreme Court's smartphone judgment, and current practice following the latter judgment.[283] The explanation of profound systematicness largely reiterated the committee's explanation.[284]

The draft Explanatory Memorandum provided examples to help interpret the abstract criterion. Non-systematic (a minor privacy intrusion), for example, are investigations of data carriers that intrinsically contain only few data, such as "bike chips" (only containing identification numbers for theft prevention), and manual investigations of a limited number of files on smartphones, for instance the most recent photos or videos on a smartphone seized from bystanders of nightlife violence, or looking up the username in certain apps.[285] Automated searches for evidence will normally constitute systematic

276. The committee is also called the Koops Committee, after its chairperson—the same as the second author of this paper.

277. COMMITTEE ON MODERNIZING, *supra* note 225, at 36–41.

278. *Id.*

279. *Id.* at 37–40.

280. *Id.* at 41.

281. *Id.* at 48–50.

282. *Id.* at 41.

283. *Bill Establishing Book* 2, *supra* note 272, at 17.

284. *Id.* at 24–25.

285. COMMITTEE ON MODERNIZING, *supra* note 225, at 45.

investigations, but if searches are highly targeted and offense-specific, for instance, images resembling a suspect's graffiti tag, in which presumably only relevant (graffiti) pictures will show up, this is still non-systematic.[286] In contrast, investigation officers manually scrolling through the entire collection of the past year's pictures to look for graffiti pictures are conducting a systematic search (a more than minor privacy intrusion), since they can broadly take note of the suspect's private life.[287] Thus, even without copying search results, looking at all or many photos on a smartphone will be systematic.[288] More generally, the Memorandum mentions various factors to take into account to determine whether investigation activities are (profoundly) systematic: number and type of data, whether data can be automatically investigated, type of data carrier, mode of storage, and automation of the investigation.[289] How these factors can be applied will be explained in more detail for open-source investigations in the future Explanatory Memorandum of the final Bill that is to be submitted to parliament sometime in 2020.[290]

II. DISCUSSION

In Part I, we extensively described how courts (and, in the Netherlands, legislators) assess the intrusiveness of smartphone searches incident to arrest. In this Part, we will analyze and compare these findings, starting with explaining the framework of our analysis.

A. THEORETICAL LENS: CONTENT AND CONTAINER APPROACHES TO PROTECTING PRIVACY

In previous research, we analyzed how legislators and courts assess the intrusiveness of new (manifestations of) police investigation methods by examining which privacy frameworks they resort to in response to privacy-intrusive conduct by police.[291] We are interested in this question because privacy protection in the law is often not achieved using an abstract concept of privacy, but through more concrete proxies that capture relevant elements of privacy. Legal frameworks protect, for instance, privacy of the home, letters, writings, communications, bodies, thoughts, property, family, social relations, and identity.[292] These proxies help make privacy concrete, which enhances legal certainty, both for citizens (to know how their privacy may legitimately be infringed by the police under criminal procedure rules) and police (to know under which conditions they may infringe privacy when conducting investigative activities). Although such proxies are intrinsically imperfect (they can never fully capture privacy, given privacy's complex, multi-faceted, and

286. *Id.* at 45–46.
287. *Id.* at 46.
288. *Id.*
289. *Id.* at 37.
290. *Id.*
291. *See generally* Koops et al., *supra* note 18; Škorvánek et al., *supra* note 18.
292. Koops et al., *supra* note 16, at 541 fig.1.

context-dependent character); but, generally, they work well enough to protect privacy, striking an apposite balance between abstractness and concreteness of the law. However, over time, proxies can become less suitable for protecting privacy due to socio-technical change.[293] In the current data-pervasive and ubiquitously connected world, older proxies such as privacy of the home and secrecy of communications content have become less powerful at capturing what privacy means in today's age.[294] Our broader research over the past years has therefore analyzed whether new privacy proxies could better capture what privacy means in the twenty-first century.

A major insight derived from this research is that there are (at least) two different general types of privacy protection in the law: container-based approaches and content-based approaches.[295] Container-based approaches, for instance, protect the home, communications channels, and "boxes, bags . . . wrapped packages, glove compartments, and locked trunks"[296] as *per se* protection-worthy spaces, independent from their actual contents.[297] A dwelling, for instance, is protected from a search even if nothing privacy-relevant is actually stored there; a communication channel is protected against wiretapping even if it transmits only non-personal or non-private communications. In contrast, content-based approaches focus on content as *per se* protection-worthy, independent from the specific container that holds it. For instance, data protection law protects personal data or personally identifiable information as such, regardless of whether the information is stored in a private or public space, stored in a closed container, or openly visible.

In our research, we found that "there is increasing discomfort with the answers . . . yielded by the traditional privacy frames" to assess the intrusiveness of location tracking by police,[298] and that the

> adequacy of [the classic privacy] frames in assessing the intrusiveness of police hacking is limited . . . . Across the jurisdictions, we observe the contours of two such new frames emerging: a container-based approach focusing on the computer as protection-worthy in itself and a content-based approach focusing on the data.[299]

We concluded that the two new frames "complement each other in their capacity to serve as a yardstick to assess the intrusiveness of police hacking (and,

293. *See* Bert-Jaap Koops, *On Legal Boundaries, Technologies, and Collapsing Dimensions of Privacy*, 3 POLITICA E SOCIETÀ 247 (2014).

294. *Id.*

295. Škorvánek et al., *supra* note 18, at 1078–81.

296. United States v. Camou, 773 F.3d 932, 943 (9th Cir. 2014).

297. Note that, in articulating this container approach, we use "container" in a broad sense, denoting anything that encloses a certain space, for example, envelopes, changing rooms, dwellings, and computers; many such containers can function as "privacy spaces." *See* Bert-Jaap Koops, *Privacy Spaces*, 121 W. VA. L. REV. 611, 614 (2018) (defining privacy space as a "space in which you can be yourselves"). This is similar to the U.S. Supreme Court's definition of a container, for Fourth Amendment purposes, as "any object capable of holding another object." New York v. Belton, 453 U.S. 454, 460 n.4 (1981).

298. Koops et al., *supra* note 18, at 696.

299. Škorvánek et al., *supra* note 18, at 1069–70.

perhaps, of criminal investigation powers in digital contexts more generally)" and hypothesized "that a combination of both is likely to be the most suitable new framework for evaluating the intrusiveness of police hacking."[300]

Now, we want to test whether, to what extent, and how a combination of container- and content-based approaches could be a suitable framework for assessing the intrusiveness of police investigations. The context of smartphone searches incident to arrest is particularly suitable for this, with many and varied cases in the three jurisdictions outlined in Part I, above. Through the lens of the framework of container- versus content-based approaches, we analyze, first, how container and/or content approaches feature in search-incident-to-arrest cases in the jurisdictions we studied, and second, how preferences for container or content approaches, or combinations thereof, play out in this context.

B. CONTAINER AND CONTENT ARGUMENTS

In all three jurisdictions, we see similar argumentation for why the search-incident-to-arrest doctrine should apply differently to smartphones (and other types of computers) than to traditional objects. The difference between a ride on horseback and a flight to the moon is simply too substantial. All jurisdictions recognize that, generally, smartphones are devices that potentially contain a vast amount of diverse and privacy-sensitive information. Combined with smartphones' large storage capacity as a significant factor,[301] the mosaic theory[302] functions, albeit implicitly, as an important privacy framework here. As the *Riley* court observed, "a cell phone collects in one place *many distinct types* of information . . . that reveal much more *in combination* than any isolated record. . . . The *sum* of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions."[303] Similarly, the dissent in *Fearon* argued that smartphone searches allow the police to see through the "*windows* to our inner private lives."[304] The Dutch criteria of systematicness ("a more or less *complete image* being obtained of certain aspects of [the user's] private life")[305] and of profound systematicness (that is, when "a more or less *complete picture* arises of a) an essential . . . or b) a substantial part of someone's private life")[306] likewise use mosaic metaphors (pictures resulting from a data set) to highlight privacy intrusiveness.

An additional factor plays a role here: the ease of obtaining mosaic pictures because of the prevalence of modern-day smartphones. Traditional objects that can reveal significant parts of private life, such as (printed) photographs or diaries, may also occasionally be found on arrestees, but these are exceptional cases; in contrast, smartphones are likely found in most cases. Thus, the default

300. *Id.* at 1080–81.
301. Riley v. California, 573 U.S. 373, 393–97 (2014); R. v. Fearon, [2014] 3 S.C.R. 621, para. 51 (Can.).
302. *See supra* note 79 and accompanying text.
303. *See Riley*, 573 U.S. at 394 (emphasis added).
304. *Fearon*, 3 S.C.R. at para. 101 (emphasis added).
305. HR 4 april 2017, ECLI:NL:HR:2017:592, para. 3.4 (Neth.) (emphasis added).
306. COMMITTEE ON MODERNIZING, *supra* note 225, at 37–40.

situation flips from an incidental finding to an almost routine investigation of private life if objects found on or near an arrestee are seized and searched.[307] The ubiquity of smartphones significantly reduces the effort police have to make to gather data and, thus, the cost of investigation. This factor, as Matthew Tokson has recently argued, is a major factor in Fourth Amendment privacy assessments.[308]

Essentially, we observe courts combining container-based and content-based arguments: smartphones (as devices or containers) are special because they generally contain content that, in combination, reveals a mosaic picture of private life; and smartphone contents (information, data, or links between data) are special because, crucially, smartphones combine different functions, are ubiquitous, and have large storage capacity. These are mutually reinforcing rationales: smartphones are particularly protection-worthy because of key characteristics of their contents, and smartphone contents are particularly protection-worthy because of key characteristics of their container.

What emerges most strikingly from our comparative overview, is that while the underlying reasoning of smartphone searches of potentially high intrusiveness is similar (namely that a smartphone search can easily result in an intrusive mosaic picture of someone's private life), the conclusions drawn from this reasoning differ significantly. The *Riley* court (similarly to the *Fearon* dissent) concluded that because smartphones "as a category" often contain so much private information, they should be protected *categorically* from warrantless searches.[309] Thus, U.S. doctrine applies a container approach to privacy protection, defining smartphones[310] as *per se* protection-worthy privacy spaces—regardless of what the specific smartphone in an individual case actually contains. In contrast, the majority in the *Fearon* case and the Dutch Supreme Court concluded that because smartphones often contain so much private information, *their contents* should be protected from warrantless searches. Rather than give categorical protection to smartphones, these courts held that the intrusiveness of a search depends on what is actually investigated. Thus, Canadian and Dutch doctrines apply a content approach to privacy protection, protecting smartphones (and other computers) against intrusive searches depending on which data are (likely to be) investigated, and thus also depending on what the specific smartphone in a particular case actually contains.

We conclude that the United States legal framework has adopted a container approach, while the Canadian and Dutch frameworks have adopted a content approach. Given our finding from earlier research that both approaches have limitations, and our hypothesis that a combination works best,[311] it is

307. *See supra* notes 75–76, 177–178 and accompanying text.

308. Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 25 (2020) (arguing that the cost of investigation, besides the intimacy of the place or thing targeted and the amount of information sought, is a consistent principle in Fourth Amendment privacy assessments).

309. Riley v. California, 573 U.S. 373, 393 (2014).

310. Defining smartphones here possibly includes similar devices. *See infra* Part II.C.1.

311. *See supra* notes 276–279 and accompanying text.

interesting to further analyze the advantages and drawbacks of the different frameworks adopted by the three jurisdictions, and how these jurisdictions attempt to mitigate the drawbacks of their adopted approaches.

C. CONTAINER PROTECTION

1. Advantages and Drawbacks

Under the container approach, the smartphone is considered an object worthy of protection in and of itself, and thus functions as a new proxy for privacy protection. The protection resembles home protection, where the dwelling functions as a classical proxy for privacy protection: both are spaces enclosing a large part of private life. The Dutch discussion memorandum compared looking through all the information on a seized smartphone to "the seizure of all photo albums, all video tapes, all personal letters, all personal notes (diaries) of a person,"[312] similar to the First Circuit court's argument in *Wurie* that "[a]t the touch of a button a cell phone search becomes a house search."[313] SCOTUS in *Riley* even considered that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house," making smartphones an even more important privacy space than the home (at least in terms of government interference).[314] It does not really matter whether a protection-worthy space is physical or virtual—in the words of the Canadian Supreme Court, the "electronic world of digital communication . . . is every bit as real as physical space" and can serve as "the place of the search."[315] This recognition of smartphones as the new "home" locus of private life resonates with the concept of the "digital home" that emerges in some jurisdictions as an important new privacy framework.[316]

The container approach can serve as a powerful and practical analytic tool for guiding police work on the ground. Indeed, the primary benefit of the container approach is that it can provide clear-cut, bright-line rules governing police investigations and the issuance of warrants. In Canada and the Netherlands, police officers must decide whether their intended investigation of a smartphone is sufficiently limited to not require a warrant—not an easy decision, given that the answer depends on many factors.[317] For U.S. police

312. RB Noord-Holland, 29 juli 2019, ECLI:NL:RBNHO:2019:6764 (Neth.).

313. United States v. Wurie, 728 F.3d 1, 8–9 (1st Cir. 2013) (quoting United States v. Flores-Lopez, 670 F.3d 803, 806 (7th Cir. 2012)). Although the *Flores-Lopez* court found that *evidence* preservation concerns in that case outweighed any invasion of privacy, the court upheld the warrantless search of the cell phone, because the search at issue was minimally invasive—only directed at discovering the phone's number. *Flores-Lopez*, 670 F.3d at 810.

314. *Riley*, 573 U.S. at 396.

315. R. v. Marakah, [2017] 2 S.C.R. 608, para. 28 (Can.).

316. *See* Škorvánek et al., *supra* note 18, at 1056–58 (discussing the emergence of "informatic home" as a new privacy frame).

317. *See infra* Part II.D.2.b.

officers wanting to investigate a seized smartphone incident to arrest, the answer is very simple: "get a warrant."[318]

A corollary of this is that the Canadian and Dutch jurisdictions grant some discretionary power of the police to conduct (simple or minimal) smartphone searches, which may be stretched, abused, or hidden from oversight, and which, therefore, require some measure to keep this discretionary power in check.[319] The United States has no need for such measures, since even simple or minimal smartphone searches are not allowed.

The simplicity of the container approach is, however, not only an advantage but also a drawback. It is a crude, black-and-white approach that treats all devices alike: smartphone searches categorically require a warrant, regardless of specifics.[320] This has three major consequences. First, in this approach, the only limitation of police smartphone searches lies in the access point: to get in, police need a warrant. But once a warrant is granted and police can enter, the container protection is lost, no longer offering any guidance as to what can be investigated within the container (unless the warrant itself includes restrictions established by the issuing judge). This contrasts with the content-based protection's more nuanced approach, which focuses directly on regulating the search of the phone's contents.[321]

A second consequence is that much hinges on the qualification of a certain device as pertaining to the category that has container protection. When exactly is a computing device functionally equivalent to "[m]odern cell phones . . . [w]ith all they contain and all they may reveal"[322] that merit *Riley*'s container protection? This question should be answered for many types of devices that resemble, in some sense but not in all senses, modern cellphones, including laptops, tablets, smart watches, USB drives, digital cameras, and in-car computers. So far, the question seems to have been addressed (not necessarily authoritatively) to a limited range of information carriers, such as laptops[323] and digital cameras.[324] However, practitioners and courts may have to grapple for a considerable period with classifying other devices under SCOTUS's reasoning and holding in *Riley*. Additionally, there exists some ambiguity in whether, or how, the law should apply differently to searches of "subcontainers" (for example, separate files, folders, apps, or directories that exist inside a broader digital "container" such as a cellphone).[325] Moreover, this question will need to be continuously answered for future devices that currently are not sufficiently cellphone-like to be covered by *Riley* but that may become

318. *Riley*, 573 U.S. at 403.

319. *See infra* Part II.D.2.

320. *Cf.* Škorvánek et al., *supra* note 18, at 1079 (articulating the crudeness of the container approach).

321. *See infra* Part II.D.1.

322. *Riley*, 573 U.S. at 403.

323. United States v. Lichtenberger, 786 F.3d 478, 487–91 (6th Cir. 2015).

324. United States v. Whiteside, No. 13 CR 576 PAC, WL 3953477, at *3 (S.D.N.Y. June 29, 2015).

325. *See* Michael Mestitz, Note, *Unpacking Digital Containers: Extending* Riley*'s Reasoning to Digital Files and Subfolders*, 69 STAN. L. REV. 321, 323 (2017).

equivalent when new functions are added. In that sense, the container approach is technology-specific and may not be very sustainable over time.

A third consequence of the black-and-white container approach is that even simple or minimal investigations require a warrant. For instance, accessing the call log on a phone to acquire the number of incoming calls that were visible on the screen as "my house"[326] is no longer possible without a warrant under *Riley*, although such activity is very far removed from assembling a mosaic-like picture or a typical (let alone an exhaustive) house search. Allowing, as Canada and the Netherlands do, such simple, targeted search activities by police officers without higher authorization seems reasonable. In adopting categorical container protection for smartphones, SCOTUS has rightly differentiated smartphone searches from investigations of traditional objects such as bags or cigarette packages (which are comparatively "rides on horseback"[327]); but it has also effectively treated *all* smartphone searches as comparable to flights to the moon. Yet there are many ways of getting from A to B, and depending on your goal, you might choose between many different modes of travel: walking, cycling, driving a car, taking a high-speed train or transatlantic flight, or engaging in space travel. Smartphone searches can have different goals, and do not always—indeed, often do not—take the form of the high end of the spectrum; several types of simple searches the police might want to conduct quickly following arrest are more comparable to rides on horseback than to spaceflight. In this sense, the sole reliance on the container approach to protecting privacy in the search-incident-to-arrest context will likely overprotect privacy at the expense of police investigations.

2. Mitigating the Drawbacks

The first drawback of the black-and-white container approach—only regulating access to the device but not the scope of the search of the device's contents—is relatively easily mitigated by the Fourth Amendment's particularity requirement.[328] Warrants must circumscribe what may and may not be investigated in the seized phone.[329] Thus, the intrusiveness of smartphone searches is primarily regulated by another normative framework in U.S. legal doctrine—regulating the issuance of, and compliance with, warrants—than by the container protection of smartphones. This is not in itself an issue, but it does limit the thrust of using smartphones as a new proxy for privacy protection in terms of finding new frameworks for making privacy assessments; the container

326. *See* United States v. Wurie, 728 F.3d 1, 2 (1st Cir. 2013).

327. *Riley*, 573 U.S. at 393.

328. *See, e.g.*, Marron v. United States, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.").

329. *See, e.g.*, United States v. Russian, 848 F.3d 1239, 1244–46 (10th Cir. 2017) (finding that "a 'recognizable line' [exists for] considering how much particularity is required for computer searches" and holding that a warrant to search a cell phone was invalid since it failed to "specify what material (e.g., text messages, photos, or call logs) law enforcement was authorized to seize").

approach, in this sense, may not easily be usable in other legal systems that lack something like the United States' strict particularity requirement for limiting searches.

In a similar vein, the second drawback—having to determine whether each different type of device belongs to the class of protected containers—seems a feature of the U.S. common law system itself, in which the facts of each case have to be analyzed on the basis of their resemblance to precedent. Courts are used to dealing with questions concerning the similarities and differences between a present case and existing doctrine; it is perhaps less a drawback than a systemic feature that courts must determine whether each digital device falls within *Riley*'s conception of modern cellphones. This does not, however, diminish the legal uncertainty that practitioners may experience when police want to investigate a digital device that is not a cellphone but that also stores potentially much and/or varied information. Legal certainty can only be acquired over time, when cases involving different devices reach higher courts and receive authoritative judgments.

The third drawback—the overprotective prohibition of any warrantless smartphone search, however minimal—is more challenging to mitigate. The main workaround we have observed in post-*Riley* cases is the application of the plain-view doctrine, exempting searches of the smartphone's screen from *Riley*'s warrant requirement, because there is no reasonable expectation of privacy in something in plain view.[330] This fits well in the container approach, since container protection typically protects the inside of containers, not what is visible on their outside. It is plausible to consider what is visible on the screen (without manipulating the device, because hitting any key or touchscreen might show something of the device's contents that was not visible before) as falling under the plain-view exception. However, there is arguably a relevant difference between smartphone screens and the outsides of traditional containers. While the latter are usually static, the former can be dynamic: if a smartphone is seized, the screen may still show (notifications of) incoming messages, without any intervention by police or the smartphone user. Although such (notifications of) incoming messages are plainly visible for the police, they were not visible at the time of seizure. Whether this difference matters (or should matter), in practice, for the plain-view doctrine remains an open question—although, given the general analysis offered by the Supreme Court in *Riley*, there may be room for adapting the plain-view doctrine in this context as well.

A second mitigation strategy is that certain contexts are exempted from *Riley*'s standards, because the context implies a lower reasonable expectation of privacy, for example, if the smartphone belongs to a parolee.[331] These exceptions limit the container approach's overprotection of privacy somewhat, but of course do not cover the bulk of typical search-incident-to-arrest cases.

330. *See supra* notes 96–99, 105–109 and accompanying text.

331. *See supra* notes 87–93 and accompanying text.

Other than plain-view situations of what is visible on smartphone screens and some context-specific special situations, we have not found major strategies to mitigate the overprotective reach of *Riley*'s categorical protection of smartphones by lower U.S. courts. We think that two additional mitigation strategies may be envisioned. First, law enforcement could argue that certain cursory investigations, such as those allowed under Canadian and Dutch doctrines without a warrant, do not constitute a Fourth Amendment "search" or, even if they do, that they are objectively reasonable in situations where the suspect or arrestee does not maintain any reasonable expectation of privacy.[332] Second, law enforcement could argue that the device at issue is not, in effect, a *Riley* type of protected device. Although *Riley* covers not only smartphones but also simpler types of cellphones (such as a "flip phone" exhibiting "a smaller range of features than a smart phone"),[333] its reasoning rests on the particular affordances of smartphones, including their large storage capacity and their multifunctionality and prevalence (allowing multiple data types to be recorded in widely varying contexts). In concrete cases involving a cellphone with only a few functions, so that the cellphone in question is incapable of actually revealing a mosaic-like picture of (part of) someone's private life, let alone of the "privacies of life," it might, perhaps, be plausibly argued that this device falls outside the *Riley* category of protected devices.

Whether such strategies could work sufficiently to mitigate the drawbacks of the bright-line, black-and-white approach of container protection is something we cannot presume to answer here. Case law is still developing dynamically post-*Riley*; time will tell how practice and jurisprudence manage to address the challenges we discussed here.

D. CONTENT PROTECTION

1. Advantages and Drawbacks

Under the content approach, the contents of smartphones are considered protection-worthy, rather than the device itself. This is because "searches of 'smart phones' . . . may constitute very significant intrusions of privacy, [but] not every search is inevitably a significant intrusion."[334] Instead of regulating access to the device as the key activity, content-based protection "impose[s] meaningful limits on the *purposes*, threshold *and manner* of such searches."[335] Thus, content protection focuses, in particular, on the totality of data that are

332. This might look something like an extension of the analyses offered by U.S. judges in *United States v. Brixen*, 908 F.3d 276, 281 (7th Cir. 2018) ("[The officer's] actions simply do not amount to a search of Brixen's cell phone. He did not open or otherwise manipulate Brixen's phone. Nor did he gain access to any of the phone's content or attempt to retrieve any information from within the phone.") and *United States v. Lawing*, 703 F.3d 229, 238 (4th Cir. 2012) ("The police did not attempt to retrieve any information from within the phone."), although both of these cases rested somewhat on the plain-view doctrine in coming to their respective conclusions.

333. Riley v. California, 573 U.S. 373, 380 (2014).

334. R. v. Fearon, [2014] 3 S.C.R. 621, para. 54 (Can.).

335. *Id.* at para. 63 (emphasis added).

investigated and that may, in their combination, create a revealing picture of (parts of) someone's private life. The protection resembles, or may even be seen as being based on, the framework of the mosaic theory, which is emerging in several jurisdictions around the world as an important new privacy framework.[336]

The benefits and drawbacks of the content approach largely mirror the drawbacks and benefits of the container approach outlined in the previous Part, so we shall not elaborate on those here. Briefly put, the main benefit of the content approach is its flexibility (as opposed to the crudeness of the black-and-white container approach), allowing, for instance, warrantless cursory searches and focusing on data actually (envisioned to be) investigated rather than on the question of whether the device belongs to the category of protected devices.

Its main drawback is the complexity that comes along with its flexibility (as opposed to the simple, bright-line character of the container approach). The content protection depends on the estimated level of intrusiveness of a search: limited, shallow intrusions trigger limited protection; broader or deeper intrusions trigger stronger protection. Whether an intrusion is (likely to be) limited (shallow) or broad (deep) depends on many factors, related to both the search activity and the device in question. Since investigating officers only have to apply for higher authorization if the privacy intrusion is more than limited, the officers face the challenge of assessing, on the ground and in the moment, whether their envisioned investigation remains below or goes beyond the threshold of intrusiveness—a threshold that is not particularly well-defined. Not only does this bring along legal uncertainty, the discretionary power for making the initial assessment also raises questions of control and oversight of police investigations. How do Canada and the Netherlands deal with these challenges to the content approach?

2. Mitigating the Drawbacks

To off-set the problem of overly complex intrusiveness assessments, both jurisdictions offer sets of criteria or factors that should be taken into account when determining whether an envisioned investigation meets the threshold of intrusiveness: Canada has the *Fearon* criteria,[337] the Netherlands has the threefold criterion of (profound) systematicness and an associated list of factors influencing the level of intrusiveness.[338] We can distinguish two mitigation strategies here, aiming to make the complex intrusiveness assessment simpler and more manageable for practitioners, and one strategy to ensure oversight of warrantless searches.

---

336. *See supra* Part II.B; *see also* Škorvánek et al., *supra* note 18, at 1073–78 (discussing the "informatic privacy" and the mosaic theory as an emerging new privacy frame); Koops et al., *supra* note 18, at 693–95 (showing the emergence of the mosaic theory in the U.S. and in other jurisdictions as a new privacy frame).

337. *See supra* note 167 and accompanying text.

338. *See supra* notes 276–281, 289 and accompanying text.

a. Guiding Examples of Levels of Intrusiveness

First, both jurisdictions have developed relatively abstract criteria,[339] which are sufficiently general to allow covering many situations and to be sustainable over time. Abstract criteria or general principles do not offer much concrete guidance, but that is offset by courts applying the criteria or principles to concrete cases over time, building up a collection of illustrative, and therewith perhaps authoritative, examples of investigations that do or do not cross the relevant threshold. The case law following the supreme court cases in both jurisdictions already gives interesting indications, generating the following picture of different levels of intrusiveness distinguished by courts. Note that this list is indicative; it can serve as a first inventory of examples but, given that they often derive from lower-court case law, they cannot (yet) be considered authoritative.

Level 1: low intrusiveness (implying police can conduct such searches without higher authorization).

- Activating a phone's screen to see if it is locked or to prevent the phone from reverting to a locked state.[340]
- Observing (copying) what is in plain view, for example, a conversation on the screen of a seized phone, or notifications appearing there.[341]
- A targeted, offense-related search for a relatively small number of specific data,[342] for example, missed calls or messages,[343] a contact in the WhatsApp contact list and the associated profile picture,[344] some videos,[345] pictures in the photo gallery (if there is no indication that the photo gallery has very many pictures that might be seen in passing),[346] the most recently made photos or videos[347] or recent text messages,[348] looking up the user name in certain apps,[349] or checking for camera capacity and Internet access.[350] Note that several U.S. cases involve activities of this kind, such as retrieving the phone number of an incoming message from the call log, viewing call logs or text messages, or verifying a phone's number; while considered intrusive in the United States

339. *See supra* Parts I.B.3, I.C.3.

340. R. v. Roberto, 2018 ONSC 847, para. 13 (Can.).

341. R. v. Khosravi, 2018 BCSC 1791, para. 47 (Can.); United States v. Brixen, 908 F.3d 276, 282 (7th Cir. 2018). *But see* R. v. Kossick, 2017 SKPC 67, para. 86 (Can.).

342. HR 4 april 2017, ECLI:NL:HR:2017:592, para. 3.4 (Neth.).

343. Parket HR 26 september 2017, ECLI:NL:PHR:2017:1245, para. 3.12 (Neth.).

344. Hof Den Haag 11 juli 2018, ECLI:NL:GHDHA:2019:2524 (Neth.).

345. Parket HR 28 november 2017, ECLI:NL:PHR:2017:1470, para. 25–26 (Neth.).

346. Parket HR 15 mei 2018, ECLI:NL:PHR:2018:764, para. 10 (Neth.).

347. *Bill Establishing Book* 2, *supra* note 272, at 21–22.

348. R. v. Jones, 2015 SKPC 29, para. 62 (Can.).

349. *Bill Establishing Book* 2, *supra* note 272, at 21–22.

350. R. v. Bourdon, 2016 ONSC 2113, para. 383 (Can.).

in meeting the *Riley* standard, these would not likely be considered (very) intrusive in Canada and the Netherlands.[351]

- Investigating a data carrier that intrinsically contains only few data, such as chips with an identification number.[352]

Levels 2 and 3: intermediate and high intrusiveness (implying police need a warrant (Canada) or permission from the prosecutor or investigative judge (Netherlands) for such searches).[353]

- Manipulating the phone to search through its contents.[354] (Whether the search meets the threshold of level 2 may, however, depend on the extent and how targeted the search is; minimal manipulation for targeted cursory searches might fall under level 1.)
- Downloading the entire contents of a cell phone or smartphone.[355]
- A more exhaustive forensic analysis (such as downloading and analyzing all content)[356]—in other words, investigating with use of technical tools all data stored in or available to the device,[357] such as acquiring (complete) insight in contacts, call history, messages, and photos,[358] or analyzing the images, video files, chats, emails, internet history, and Skype data.[359]
- Searching for evidence of a sexual offense, in which "certain photos, images, and other files" of an intimate character (potentially also including victims) could well be revealed; this can be considered highly intrusive (level 3).[360]

b. Factors Influencing Intrusiveness

Because guiding examples are case-specific, usually a combination of different facts of the case plays a role in assessing a search as exhibiting low, intermediate, or high intrusiveness. Examples cannot easily be transposed to new cases, which often involve slightly different circumstances. A complementary important mitigation strategy is, therefore, to offer a set of factors that practitioners and courts can or should consider in assessing the

351. *See supra* Part I.A.2 (discussing United States v. Wurie, 728 F.3d 1 (1st Cir. 2013)); *see supra* note 92 and accompanying text.

352. *Bill Establishing Book* 2, *supra* note 272, at 21–22.

353. Canadian case law only distinguishes two levels (searches that do not or do require a warrant). Dutch case law, although applying three levels of authorization (*see supra* Parts I.C.3–5), so far provides little guidance to distinguish between intermediate and serious intrusions (*see supra* Parts I.C.3–4). Therefore, we cannot yet sufficiently distinguish between examples for levels 2 and 3.

354. R. v. Khosravi, 2018 BCSC 1791, para. 47 (Can.); R. v. Roberto, 2018 ONSC 847, para. 13 (Can.). The search of Riley's phone to access videos, photographs, and other files would also be an example of this. *See* Riley v. California, 573 U.S. 373, 373 (2014).

355. R. v. Mann, 2014 BCCA 231, para. 118 (Can.); *see also* R v. Fearon, [2014] 3 S.C.R. 621, para. 32 (Can.).

356. R. v. Jones, 2015 SKPC 29, paras. 62–66 (Can.).

357. HR 4 april 2017, ECLI:NL:HR:2017:592, para. 3.4 (Neth.).

358. HR 4 april 2017, ECLI:NL:HR:2017:584, para. 2.7.2 (Neth.).

359. Hof's-Hertogenbosch 17 oktober 2017, ECLI:NL:GHSHE:2017:4433 (Neth.).

360. Rb. Limburg 8 mei 2017, ECLI:NL:RBLIM:2017:4484 (Neth.).

intrusiveness of smartphone searches. Combining indicators that Canadian and Dutch courts—and the Dutch legislators—have developed, we can identify various relevant factors. We have clustered them in three groups of major factors, each encompassing various indicators or sub-factors.

1. Scope and precision (how focused and targeted is the search itself?).
    a. Relationship to the offense for which the suspect was arrested.
    b. Specificity of the search action.
    c. Use of automated tools.
2. Nature and amount of information to be examined (accessed).
    a. Nature of the offense.
    b. Nature of the storage device.
3. Mode of storage of the data.
    a. Location of the data (local versus cloud; within a shared or private folder or app).
    b. Suitability of the data for automated searches.
    c. Presence of security measures.

The first factor, the **scope and precision** of the search, is perhaps the most important one. It encompasses two of the four *Fearon* criteria: the search is truly incidental to the arrest, and the nature and the extent of the search are tailored to the purpose of the search.[361] Thus, the search itself must bear a close relationship to the offense for which the suspect was arrested and should be precisely targeted to obtain only relevant information or files. The more narrowly the search is focused on finding evidence of the specific offense for which the suspect was arrested, the less intrusive it is likely to be. Typically, this will involve quick manual searches for a specific information object. Automated searches are a double-edged sword: they can be more intrusive, because more data will be investigated, and possibly come into view, than an officer could manually look at;[362] but they can also be less intrusive, because they can help locate the sought information without the officer observing any non-relevant information in passing. If used properly, automated tools can assist in making a search more targeted, and hence less intrusive.[363]

Scope and precision imply that the investigating officers should know (more or less) exactly what they are looking for, so that they can use offense-related search terms that are as specific as possible, or look only in an app or directory that contains the type of information sought. This also implies, as the *Fearon* court has said, that in warrantless arrest-related searches, as a rule, "only recently sent or drafted emails, texts, photos and the call log may be examined

361. R v. Fearon, [2014] 3 S.C.R. 621, 661 (Can.); *see also Bill Establishing Book* 2, *supra* note 272, at 22, 24 (Dutch Draft bill) (automated searching for images resembling a suspect's graffiti tag is highly targeted and therefore low-intrusive; manually scrolling through a smartphone's pictures of the past year to look for graffiti pictures is less targeted and therefore more intrusive).

362. HR 4 april 2017, ECLI:NL:HR:2017:592, para. 3.4–3.5 (Neth.).

363. *See supra* notes 255–256 and accompanying text.

as in most cases only those sorts of items will have the necessary link to the purposes for which prompt examination of the device is permitted."[364] If officers know what they are looking for, but have little clue where the information may be stored or cannot find it easily with highly specific search terms, then the search is likely to become less targeted, which is an important indicator that they should seek authorization from higher up before proceeding.

From the perspective of our interest in new privacy frames emerging in the regulation of digital investigations, it is relevant to note that scope and precision—as a requirement for a search to be offense-related and as specific as possible—is a manifestation of contextual integrity. Contextual integrity is respect for informational norms,[365] that is, norms "that govern activities and practices within and across contexts" and are "specifically concerned with the flow of personal information . . . from one party to another, or others."[366] As long as police carefully target their search for crime-related information, in the context of a search incident to arrest, they are less likely to violate contextual integrity than if they search more broadly: the flow of crime-related information to police can be expected, even if often unintended and undesired, by an arrestee, while police officers looking at non-crime-related information should not be expected. The framework of contextual integrity can thus support the approach of content protection in privacy assessments.

Equally important is the second factor, the **nature and amount of information to be examined**. The *amount* of information accessed obviously matters—looking at one photograph is less intrusive than leafing through an entire photo gallery, for example. More importantly, combinations of data or information can create a larger, more complete picture—a mosaic—than loose data can.[367] The *nature* of the data may be even more significant. Consulting photos may be more privacy-intrusive than consulting text files, since investigating officers can often leave aside text files as irrelevant without (entirely) taking note of their contents, but they will have seen the photos they discard as non-relevant. The subject matter also matters: some content (for example, nudity) is more privacy-sensitive than other content (for example, shopping lists);[368] and some content, such as business-related information, is considered less privacy-relevant.[369] The sensitivity of certain types of information is, however, context-dependent: pictures revealing homosexual orientation will, for instance, be highly sensitive for a closeted religious boy, but

364. *Fearon*, 3 S.C.R. at para. 76. *Cf. Bill Establishing Book* 2, *supra* note 272, at 21–22 (looking at the most recent photos or videos made on a smartphone seized from a bystander of nightlife violence is minimally intrusive).

365. HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 140 (2010) ("[C]ontextual integrity is defined in terms of informational norms: it is preserved when informational norms are respected and violated when information norms are breached.").

366. *Id.*

367. *See supra* Part II.B.

368. *Cf.* Koops et al., *supra* note 19, at 1222–24 (discussing subject matter as an important factor in privacy intrusiveness).

369. Hof's-Amsterdam 14 december 2018, ECLI:NL:GHAMS:2018:4610 (Neth.).

far less so for an openly gay teacher. And information generally considered non-sensitive, such as one's music preferences, may in some cases be highly sensitive.[370] Thus, data classified as "sensitive" under data protection law (relating, *inter alia*, to health, race, sexual life, and religion) are an important indicator of privacy-intrusiveness, but not a decisive factor.[371]

A considerable challenge in applying this factor is that often, police will not know very clearly how much and which information they are going to investigate and retrieve; that will depend on many factors, including how the sought information (if present) is stored relative to other data. Some factors can, however, help in estimating the likelihood of the nature and amount of information being found during a search. One is the nature of the offense: the likelihood of finding pictures showing nudity is larger if someone is arrested for sextortion than for embezzlement.[372] Another is the nature of the storage device. While this is the overarching criterion in the container approach (the nature of smartphones making them protection-worthy as such), it is a supportive criterion in the content approach: the storage capacity and, particularly, the mono-, multi, or hyper-functionality of the device give some indication of what (type of) information can be expected to be stored on (or accessible through) the device. The larger the storage space and the more functions enabled on the phone, the more likely many, diverse, or sensitive data can be found there and, hence, the more intrusive the search will potentially be, especially if it is not targeted and limited in scope, and vice versa.[373]

The third factor is also relevant, but somewhat equivocal and perhaps less weighty than the first two. The **mode of storage** is mentioned by the Dutch legislators as a relevant factor,[374] although with little explanation. We think this factor is a useful umbrella factor for several aspects of the way the data are stored. An interesting aspect is the location of the data. The location may be an indicator of the nature of the data (one expects the Photo Gallery to contain photos, and the internet history to contain information about visited websites). But in relation to the storage mode, location is particularly relevant in terms of whether data are stored on-device or externally, in the cloud. A smartphone search incident to arrest may involve not only data physically stored on the phone, but also data accessible to the phone; although not very explicitly, the *Fearon* decision seems to also encompass data accessible to the phone rather

370. *See* COMMITTEE ON MODERNIZING, *supra* note 225, at 44 (giving the example of a boy in a street gang who carefully keeps his preference for romantic music secret).

371. *Id.*; *see also Bill Establishing Book* 2, *supra* note 272, at 24 (holding that "sensitive data" are an important indicator for assuming a search to be profoundly systematic, but that "not every investigation of such data is immediately profoundly systematic. After all, sensitive personal data often do not yield a profound image of someone's private life").

372. *Cf.* HR 4 april 2017, ECLI:NL:HR:2017:592, para. 2.3 (Neth.).

373. *See supra* notes 273 (bike chip), 247 (PGP phone with disabled functions) and accompanying text. An airbag control module likely also qualifies as a device associated with low intrusiveness, given its monofunctionality. *Cf.* Mobley v. State, 816 S.E.2d 769, 792 (Ga. App. 2018).

374. *See Bill Establishing Book* 2, *supra* note 272, at 23.

than just data physically stored on it.[375] This was also an important argument in *Riley*: since the police can search cloud-stored data from the seized phone, they reach far beyond "the physical proximity of an arrestee."[376] The Dutch smartphone judgment also suggests that smartphone searches might encompass cloud-stored data.[377] Investigating such externally stored data is technically possible and possibly relevant, but makes the smartphone search rather different in character from traditional searches incident to arrest, which only involve objects in close vicinity to the arrestee. This, we think, is therefore an indicator of heightened intrusiveness.

Another aspect of storage mode is the suitability of the data for automated searches, which the Dutch legislators list as a relevant factor.[378] Smartphones by definition contain digital or digitized data, which makes them generally suitable for automatic searches; however, text can also be stored in non-searchable formats, such as non-searchable PDF documents or photos of texts. The presence of such non-searchable data formats lowers the intrusiveness of a search, since they require more effort to make them readable. The same applies to encrypted files, which are, of course, also non-searchable. This connects to a third aspect of storage mode: the presence of security measures. The lower and appeals courts in *Fearon* had considered the absence of security measures—"[t]he cell phone . . . was not 'locked' and had no password protection or other security walls"—a relevant factor, indicating a lower (or at least not a higher) reasonable expectation of privacy.[379] In contrast, the SCC considered this immaterial: someone's "decision not to password protect his or her cell phone does not indicate any sort of abandonment of the significant privacy interests one generally will have in the contents of the phone."[380]

c. Logging and Other Procedural Mechanisms

The notetaking (or logging) requirement announced by the Canadian Supreme Court in *Fearon*, requiring investigating officers to take detailed notes about how and what they examine during a search of a device[381] constitutes a significant procedural control mechanism. This requirement, and others like it, could provide a strong safeguard against overly broad, dragnet searches of arrestees' digital devices. This requirement is conspicuously absent in the Dutch system (and is somewhat irrelevant to the U.S. context, where these searches are banned outright), causing some of the problems we noted in Part I.C.4, above. We suggest that something like this logging requirement could serve as a crucial

375. *See supra* notes 171 and accompanying text (discussing how the SCC observes that a smartphone search "may provide access to information that is in no meaningful sense 'at' the location of the search").

376. *See supra* notes 83–84 and accompanying text.

377. HR 4 april 2017, ECLI:NL:HR:2017:592, para. 3.3 (Neth.). The Dutch draft Bill also allows investigating (lawful) network connections from the seized phone. *See Bill Establishing Book* 2, *supra* note 272, at 26–27.

378. *See Bill Establishing Book* 2, *supra* note 272, at 23.

379. R. v. Fearon, 2010 ONCJ 645, paras. 19–22 (Can.); R. v. Fearon, 2013 ONCA 106, para. 57 (Can.).

380. R v. Fearon, [2014] 3 S.C.R. 621, para. 53 (Can.).

381. *Id.* at para. 82.

regulatory mechanism for controlling and limiting the scope of police smartphone searches in jurisdictions favoring content-based approaches.

Other rules that would control what types of data the police can search, or the range of law enforcement agents who might have access to the data, prior to additional authorization, could also serve a similar limiting purpose. For example, in the rules that regulate police hacking powers (that is, the ability to access digital systems remotely and covertly), each of these three countries discussed in this paper have, to a varying extent, limited police powers to search devices (remotely) based on the functionality of the search (for example, based on the officers' goals, the type of data likely to be discovered, and the nature of a particular investigatory method).[382] This is related to the Canadian requirement that the nature and extent of smartphone searches must be tailored to the purpose of the search, although the Canadian requirement is more vague and context-dependent than, for example, the Dutch rules that segment hacking powers by specific functionalities, which distinguish, for example, between looking for identifying information, communications, and searching through all data.[383]

Moreover, in the Dutch hacking legislation, the legislators have promulgated rules that separate the technical from the tactical officers involved in the investigation as a privacy-protective measure.[384] In one smartphone investigation case, this was also stipulated as a condition for the search.[385] The reasoning behind this is that limiting the circle of people who look at smartphone data can be privacy-enhancing, especially in the context of "thorough 'data-dump' searches"[386] that involve copying all data on the device and then analyzing them with technical tools. Because officers investigating a case have an interest in finding evidence, there is some risk they overstep the boundary of what they can look at. Thus, function separation is a good way to prevent dragnet searches and decrease the privacy-related harm when non-relevant data may be seen, because technical officers (rather than the primary investigating officers) who analyze the data would normally not know the suspects or engage with them.

The Dutch view might seem a narrow perspective on privacy intrusiveness. However, Dutch courts generally argue that the privacy harm that accrues during a smartphone search is based on the consequences of a police officer's taking knowledge of personal information about the individual: as long as an officer's "taking knowledge of the suspect's private data" has not led "to any further dissemination of private data or any other concrete prejudice" beyond the confines of the relevant investigation, Dutch courts have found the privacy violation to be only minimally invasive.[387] Possibly, the line of reasoning in Dutch case law may be shifting in the future: recently, Advocate-General

382. *See* Škorvánek et al., *supra* note 18, at 1012–26, 1079.
383. *Id.* at 1034.
384. *Id.* at 1019.
385. RB Noord-Holland, 29 juli 2019, ECLI:NL:RBNHO:2019:6764 (Neth.).
386. *Fearon*, 3 S.C.R. at para. 2.
387. Hof's-Den Haag 22 juni 2017, ECLI:NL:GHDHA:2017:2325 (Neth.).

Spronken has advised the Supreme Court to rule that courts should investigate by themselves the actual harm that a smartphone search caused to a suspect, because the burden of proving the exact harm cannot be put on the defense.[388] If the Dutch Supreme Court follows this advice, law enforcement officers might be stimulated to document their search activities better in order to convince courts that they did not overstep thresholds of intrusiveness.

Another interesting strategy in this context might be Orin Kerr's proposal (within the Fourth Amendment context) to narrow, or even abolish, the plain view doctrine for computer searches, for example, to disallow use of information about another crime that came "into plain view" when searching for information related to the case at hand.[389] This might, according to Kerr, be a plausible way to prevent dragnet investigations in the future.[390]

CONCLUSION

Tensions between law enforcement interests in conducting criminal investigations and individual privacy are brought to the fore by the regulatory choice to either institute a blanket ban on investigatory conduct (like that imposed by *Riley*) or a more nuanced, case-by-case, and context-dependent inquiry (like those promulgated in Canada and the Netherlands). Both approaches, and recent supreme court attention in all three countries, were motivated by similar concerns about the informational privacy risks attendant in allowing warrantless searches of digital communication devices with massive storage capacity. However, the outcomes reached in each country differ in important ways, especially in terms of how law enforcement officers must modify their daily practice to comply. In comparison to the container-based approach in the United States (restricting almost all searches of cellphones without a warrant), we find that the content-based approaches in Dutch and Canadian law are more granular and would allow more focused, fine-tuned searches for crime-related evidence as long as the search is not too comprehensive, open-ended, or fully automated.

Both approaches have drawbacks. On one hand, the container approach is limited, despite its practical benefits in terms of drawing bright lines that officers on the ground can follow more easily. It works only in combination with many other doctrines in criminal law (some of which, like the particularity and warrant requirements in U.S. law, cannot be easily exported to other jurisdictions). Because not all searches of smartphones are flights to the moon, sole reliance on the container approach to protecting privacy in the search-incident-to-arrest context is likely to overprotect privacy at the expense of police investigations. Indeed, the container approach is *inherently* limited because its blanketing ban on smartphone searches incident to arrest does not always correspond to the

388. Parket HR 5 november 2019, ECLI:NL:PHR:2019:1121, para. 4.11 (Neth).

389. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 566 (2005) ("Narrowing or even eliminating the plain view exception may eventually be needed to ensure that warrants to search computers do not become the functional equivalent of general warrants.").

390. *Id.* at 567–68.

specific concerns that motivated the U.S. Supreme Court to adopt it (that is, the outcome of the ruling does not reflect all the nuance visible in the Court's reasoning to come to its conclusion).

On the other hand, the content approach is also limited. Focusing only on content, and determining the legality of each smartphone search by the level of intrusiveness (or "(profound) systematicness") evident in each case, erases many of the bright lines visible to police officers on the ground, making it much more difficult for them to know, in advance, what they are allowed to do. The unpredictability of the legality of their searches may be reflected in the lack of information provided to judges in Dutch cases on how searches were conducted. As a result, these cases tend to focus on the investigation's outcomes (for example, one incriminating photograph found) rather than its process (for example, looking through all photographs). This concern might be ameliorated by something like the note-taking requirement established by *Fearon*. More generally, the content approach is more likely to work if the three mitigation strategies described above[391] are followed in order to make the approach easier to operationalize in practice. Thus, while the content approach does have limits, these limitations could substantially be addressed in practice by applying mitigation strategies that not only limit broad dragnet searches but also provide some practical guidance to police officers on the ground.

In the end, we conclude that combining both approaches may achieve the best results. We suggest that blending elements from the content- and container-based approaches might provide a fruitful alternative path forward, as they could function as complementary normative frameworks.[392] Indeed, a combination of emerging and preexisting container-based and content-based approaches to regulating police searches might be used to solve the challenge of finding a framework that is both sufficiently concrete (to be manageable for police officers) and sufficiently technology-neutral (to be sustainable in light of significant and ongoing socio-technical change). Thus, balancing the benefits of both approaches, while attending to the drawbacks and mitigation strategies noted above, may provide a better way forward, providing practical, usable guidance for police officers on the ground while at the same time recognizing that not all searches of digital devices are, or need to be, flights to the moon.

391. *See supra* Part II.D.2.

392. We make a similar argument in the context of police hacking powers. *See* Škorvánek et al., *supra* note 18, at 1080–81.

***