Location Tracking by Police: The Regulation of 'Tireless and Absolute Surveillance'

Bert-Jaap Koops,* Bryce Clayton Newell,** and Ivan Škorvánek***

Location information reveals people's whereabouts, but can also tell much about their habits, preferences, and, ultimately, much of their private lives. Current surveillance technologies used in criminal investigation include many techniques to track someone's movements; not all are equally intrusive. This raises the following questions: how do jurisdictions draw boundaries between lesser and more serious privacy intrusions? What factors play a role? How are geolocational privacy interests framed? In this Article, we answer these questions through a comparative analysis of location-tracking regulation in eight jurisdictions: Canada, Czechia, Germany, Italy, the Netherlands, Poland, the United Kingdom, and the United States.

We analyze the legal status of location tracking through human observation, GPS tracking, cell-phone tracking, IMSI catchers (Stingrays), silent SMS, automated license-plate recognition, and directional Wi-Fi tracking in these countries. This results in highly context-dependent and case-specific assessments, in which eight factors play a role: use of a technical device, place, intensity, duration, degree of suspicion, object of tracking, covertness, and active generation of data. At a deeper level of analysis, we identify different conceptualizations of privacy underlying these assessments: not only classic privacy frames, such as communications secrecy, protection of home and body, and informational privacy, but also two new privacy frames: freedom of movement in combination with anonymity, and the mosaic theory. Thus, we discern a tentative but unmistakable shift in how lawmakers and

* 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.
** Assistant Professor, School of Information Science, University of Kentucky; Research Associate, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University.
*** PhD Researcher, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University.

courts assess the intrusiveness of location tracking, particularly of people's movements in public space.

Traditional privacy frames tend to downplay the seriousness of the privacy infringement enabled by location tracking, and our analysis demonstrates an increasing discomfort with this tendency, leading to the emergence of novel privacy frames (or theories) to regulate what might easily turn into what the Supreme Court of the United States has called "tireless and absolute surveillance." We conclude that legal privacy frameworks developed in past centuries prove ill-suited for assessing the privacy-intrusiveness of contemporary location-tracking investigation methods, and that emerging, novel frameworks for understanding and protecting privacy may provide lawmakers and courts with the tools needed to address the challenge of preserving (geolocational) privacy in the twenty-first century.

INTRODUCTION

In the cell-phone era, one of the most common questions people ask each other is "Where are you?"[1] In fact, people have always been interested in knowing where someone is or has been, and they have devised various strategies to find out, besides simply asking, "Where are you?" or "Where have you been?" For instance, the Mehinacu in Brazil can track people's movements from telltale traces on the ground: "The paths are also sandy, and people know one another's footprints, so that a person's whereabouts are known even if he or she isn't readily visible."[2] Today's footprints stretch widely beyond the sand: we leave digital footprints everywhere, including locational traces. Moreover, current surveillance technologies include a wide variety of techniques to track someone's movements, including GPS trackers, IMSI catchers (Stingrays), automatic vehicle location (AVL), and automated license/number plate recognition (ALPR/ANPR). Additionally, new or more sophisticated methods continue to be developed, such as stealth SMS, directional Wi-Fi tracking,[3] and wide-area surveillance arrays mounted on flying objects such as planes or helicopters.[4]

---

1. MAURIZIO FERRARIS, WHERE ARE YOU? AN ONTOLOGY OF THE CELL PHONE 2 (Sarah De Sanctis trans., 2005) (arguing that the question "Where are you?" grasps the essence of the transformation induced by cell phones).

2. IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY, CROWDING 12 (1975).

3. *See infra* Sections II(B)–(E).

4. Monte Reel, *Secret Cameras Record Baltimore's Every Move from Above*, BLOOMBERG BUSINESSWEEK (Aug. 23, 2016), https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/[https://web.archive.org/web/20190128162420/https:/www.bloomberg.com/features/2016-baltimore-secret-surveillance/] (by using a wide-area array of surveillance cameras mounted on a plane flying over Baltimore, investigators "could backtrack to see where [a] vehicle had come from, marking all of the addresses it had visited. They also could fast-forward to see where the driver went after [committing a crime]").

Obviously, such methods are highly relevant to criminal investigations. Indeed, location tracking by the police (or the acquisition and use of historical location data) has become a central question in a number of high-profile cases in recent years.[5] In these cases, the question is reframed by investigators as something like, "Where were you at the time the crime was committed?" As suggested by that version of the question, location information can be vital for pinning down a suspect to a crime scene or providing them with an alibi. Indeed, real-time and historical geolocation data has become a common piece of evidence collected in criminal investigations. As one indication of the importance of locational records to police investigations, the United States Supreme Court has addressed geolocational tracking in a growing number of Fourth Amendment cases stretching back to the 1980s. For example, in *United States v. Knotts*[6] and *United States v. Karo*,[7] the Supreme Court had to decide whether the warrantless use of 1980s tracking technologies ("beepers") to track the movements of suspects' automobiles amounted to unreasonable searches (the Court held they did not, in both cases, but for different reasons). In 2012, the Court decided that the warrantless installation of a GPS tracking device did violate a suspect's Fourth Amendment rights, on the theory that the physical installation of the device amounted to an unlawful interference with the suspect's property interests in the vehicle.[8] Most recently, in *Carpenter v. United States,* the Court held that the police generally need a warrant to acquire a subscriber's historical location records from a wireless carrier, as cell-phone users maintain a reasonable expectation of privacy in the records of their movements generated by the use of their cellular phones.[9]

Location tracking by police not only encompasses various technologies, it also features different forms and methods. For instance, police can track particular suspects, but also trace possible witnesses of a crime; they can follow the movements of persons, but also of objects, such as cell-phones or containers; and they can collect data about movements in the past, or track movements in real time. Some of these forms of tracking are highly intrusive. The creation of an ALPR database has been associated with the move towards a surveillance society and called "straight out of the Big Brother handbook,"[10] while the use of tracking devices to dominate and control the location of others has been called a form of

5. *See e.g.*, Carpenter v. United States, 138 S. Ct. 2206 (2018); United States v. Jones, 565 U.S. 400 (2012). For earlier cases, see also, e.g., United States v. Knotts, 460 U.S. 276 (1983); United States v. Karo, 468 U.S. 705 (1984).

6. *Knotts*, 460 U.S. at 276.

7. *Karo*, 468 U.S. at 705.

8. *Jones*, 565 U.S. at 400.

9. *Carpenter*, 138 S. Ct. at 2206.

10. Roger Clarke, *The Covert Implementation of Mass Vehicle Surveillance in Australia*, *in* THE SOCIAL IMPLICATIONS OF COVERT POLICING: THE FOURTH WORKSHOP ON THE SOCIAL IMPLICATIONS OF NATIONAL SECURITY 47, 57–58 (Simon Bronitt, Clive Harfield & Katina Michael eds., 2010).

"geoslavery."[11] The cell-phone metadata released by German politician Malte Spitz enabled the creation of not only a precise map of his movements over the prior six months, but also a clear picture of his habits and preferences: "it reveals an entire life."[12]

Yet not all forms and applications of location tracking are equally intrusive: putting a transponder on a package or container to determine where it will be delivered is less privacy-intrusive than tailing someone for a month; collecting cell-site location information of peoples' cell-phone movements is more privacy-invasive than GPS tracking of their cars (since phones are usually used more often than cars and kept closer to the person). These differences raise questions about how intrusive location tracking is, or rather, on what basis we can and should assess the intrusiveness of the many forms of location tracking by police. This question is relevant not only because new forms of location tracking challenge lawmakers and courts, but also since they may not neatly fit into current legal frameworks. It is also relevant because a shift seems to be taking place with how the intrusiveness of location tracking is assessed, particularly where it concerns tracking people's movements in public spaces. Traditionally, this is seen as only somewhat intrusive, since people voluntarily expose their movements in such places to third parties.[13] Increasingly, however, scholars (and, to some extent, lawmakers and courts), are recognizing that surveillance in public places can be highly intrusive as well. Thus, new normative frameworks, such as the mosaic theory, are being developed to assess location tracking's intrusiveness without resorting to the age-old private space/public space distinction.[14]

In this Article, we aim to identify how eight different jurisdictions assess and establish the privacy-invasiveness of location tracking and how they are drawing boundaries between lesser and more serious privacy intrusions. We analyze the factors that play a role in these assessments and how privacy interests in location information are being framed. To answer these questions, we conducted doctrinal legal analysis[15] of the relevant law in eight jurisdictions (Canada, Czechia, Germany, Italy, the Netherlands, Poland, the United Kingdom, and the United States) and

---

11. William A. Herbert, *No Direction Home: Will the Law Keep Pace with Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?*, 2 I/S: J.L. POL'Y 409, 429 (2006) (arguing that imposing restrictions, control, and monitoring over another's location constitutes a vestige and incident of slavery).

12. Kai Biermann, *Betrayed by Our Own Data*, DIE ZEIT, (Mar. 10, 2011), http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz [https://perma.cc/TAC4-8KZB].

13. *See, e.g.*, United States v. Knotts, 460 U.S. 276 (1983).

14. *See, e.g.*, PRIVACY IN PUBLIC SPACE: CONCEPTUAL AND REGULATORY CHALLENGES (Tjerk Timan, Bryce Clayton Newell & Bert-Jaap Koops eds., 2017) (featuring contributions that explore contemporary challenges to achieving privacy and anonymity in physical public space where legal protection remains limited compared to private spaces); *see also infra* Sections II(B)(2) and III(B)(3).

15. Legal doctrinal analysis involves study of statutes and case law to analyze how and why an issue is regulated in a legal system. *See* Terry Hutchinson, *Doctrinal Research*, *in* RESEARCH METHODS IN LAW 7 (Dawn Watkins & Mandy Burton eds., 2013).

compared our findings across jurisdictions.[16] We selected these countries because while they have somewhat different cultures and histories and reflect both common-law and civil-law traditions, they are sufficiently similar in terms of their legal systems and technological development to enable comparisons; thus, the selection offers a useful mix of differences and similarities. These similarities and differences offer interesting insights into how various legal traditions shape their privacy assessments in the context of criminal procedure.[17]

The Article is structured as follows. We start in Section I with a broad overview of the relevant laws, broadly summarizing the legal status of location tracking across each of the eight jurisdictions. This may also serve as a quick reference section for the reader. In Section II, we discuss the legal status of location tracking in more detail, distinguishing between human observation, GPS tracking, cell-phone tracking, ALPR, and other forms of tracking. In Section III, we follow this description with an analysis and discussion of our primary findings. First, we analyze which factors lawmakers and courts in the studied jurisdictions use to assess the intrusiveness of location tracking; eight such factors turn out to be relevant: use of a technical device, place, intensity, duration, degree of suspicion, object of tracking, covertness, and active generation of data. Second, we analyze how privacy is framed—that is, which conceptualizations of privacy are applied in the context of location tracking? We identify not only classic privacy frames, such as communications secrecy, protection of the home, bodily integrity, and informational privacy, but also two new privacy frames being applied to address new criminal investigation methods, namely freedom of movement in combination with anonymity, and the mosaic theory. Finally, we conclude that legal privacy frameworks developed in past centuries prove ill-suited for assessing the privacy-intrusiveness of contemporary location-tracking investigation methods, and that emerging, novel frameworks for understanding and protecting privacy may provide lawmakers and courts with the tools needed to address the challenge of preserving geolocational privacy in the twenty-first century.

16. Throughout the text, we refer to these countries' Code of Criminal Procedure as [country name's] CPC, and to the Criminal Code as [country name's] CC. For brevity's sake, we use the term "warrant" as shorthand for the requisite authorization by a judge or court, although the exact type and term for court authorization may differ per country. All translations are ours (unless otherwise indicated).

17. *See* Gerhard Danneman, *Comparative Law: Study of Similarities or Differences?*, *in* THE OXFORD HANDBOOK OF COMPARATIVE LAW 384, 389–98, 403–04, 408 (Mathias Reimann & Reinhard Zimmermann eds., 2006) (discussing the importance of comparing jurisdictions which share both similarities and differences); *see also* 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, 505–06 (2017) (further explaining the reasons for choosing these countries for comparative purposes).

I. BROAD OVERVIEW OF LAWS ON POLICE LOCATION TRACKING

Since many of the particular technologies discussed below are covered by the same provisions in criminal procedure law, we first give a high-level overview of the most relevant legal provisions and cases in the jurisdictions studied (except where they specifically relate to a particular technology—those are discussed in Section II, *infra*).

In **Canada**, warrantless location tracking by the police is governed by judicial interpretations of section 8 of the Canadian Charter of Rights and Freedoms[18] and generally requires a special tracking warrant. There are very few cases examining the application of section 8 to location tracking by the police; in these, defendants were unsuccessful in arguing that the standards for obtaining tracking warrants are unconstitutional.[19] Location tracking can be authorized, however, by tracking-specific warrants outlined in section 492.1 of the Canadian Criminal Code, which stipulates conditions for obtaining a warrant for tracking devices targeted at transactions, things, or individuals.[20] For purposes of a section 492.1 warrant, a *tracking device* is defined as "a device, including a computer program . . . that may be used to obtain or record tracking data or to transmit it by a means of telecommunication."[21] When such a warrant is granted, it allows a police officer "to install, activate, use, maintain, monitor and remove the tracking device, including covertly,"[22] subject to any conditions imposed by the judge,[23] but only for a maximum of 60 days from the date the warrant was issued.[24]

In **Czechia**, police tracking is governed by Article 158d of the Czech Code of Criminal Procedure on observing persons and objects. Visual recordings of someone's movements in public space[25] or digital maps of the person's movement created by, for instance, GPS tracking[26] can only be created with a public prosecutor's written approval. These approvals can be granted if there is concrete suspicion of criminal activity; sufficient justification of the necessity to create visual, audio, or other records; and a description of the persons or object to be observed.[27] The permit is issued for no longer than six months (but can be extended indefinitely every six months).[28]

---

18. Canadian Charter of Rights and Freedoms § 8, Part I of the Constitution Act, 1982, *being* Schedule B to the Canada Act, 1982, c 11 (U.K.). ("Everyone has the right to be secure against unreasonable search and seizure").
19. *See, e.g.*, R. v. Grandison, 2016 BCSC 1712 (Can.); R. v. Edwards, 2014 ONSC 6323 (Can.).
20. For some discussion, see e.g., R. v. Grandison, 2016 BCSC 1712 (Can.).
21. Criminal Code, R.S.C. 1985, ch. C-46, § 492.1(8) (Can.).
22. *Id.* § 492.1(3).
23. *Id.* § 492.1(4).
24. *Id.* § 492.1(5).
25. TRESTNÍ ŘÁD I, II, III, KOMENTÁŘ 1993 (P. Šámal ed., 2013).
26. *Id.*
27. *Id.* at 2008.
28. Trestní řád, Zákon č. 141/1961 Sb. § 158d(4) (Czech).

In **Germany**, various provisions regulate tracking, depending on the modalities. In limited form—less than 24 hours, using only simple perception-enhancing technology such as binoculars, and only outside of the home—tracking can be based on sections 161 and 163 of the German Code of Criminal Procedure, which regulate the general power of the public prosecutor and police to investigate crime without a warrant. For longer or more intrusive tracking, section 163f on "Long-Term Observation" can be used if the investigation concerns a crime of "substantial significance" and if other means of establishing the perpetrator's location would offer much less prospect of success or would be much more difficult.[29] This requires a warrant (*Richtervorbehalt*).[30] Not only accused persons can be tracked: others can also be subjected to location tracking if a link between the perpetrator and the other person can be established and "the measure will lead to . . . determination of the perpetrator's whereabouts" and "using other means would offer much less prospect of success or be much more difficult."[31]

Location tracking can also be conducted using existing police checks to search for the accused under section 163e of the German Code of Criminal Procedure.[32] To create a full movement pattern, this measure is aimed at establishing the accused's travel pattern or route, means of transportation, carried goods, and companions.[33] The measure is admissible against people who are not themselves suspects, but only if strong suspicion exists that the measure can lead to relevant findings related to the suspect and other measures would offer much less prospect of success.[34] License plates can be included in the observation of cars registered to or in use with the accused.[35] This type of tracking also requires a warrant and can be conducted for up to one year.[36] Some other forms of tracking can be based on section 100h of the German Code of Criminal Procedure, which regulates "other measures outside of dwellings," using technical devices for observation purposes other than visual or aural recording devices, such as RFID tracking,[37] "stealth ping,"[38] night-vision devices,[39] or drones.[40] To utilize these methods, there must be

29. STRAFPROZESSORDNUNG [STPO] [CODE OF CRIMINAL PROCEDURE] § 163f(1) (Ger.).
30. *Id.* § 163f(3).
31. *Id.* § 163f(1).
32. *Id.* § 163e.
33. URS KINDHÄUSER, STRAFPROZESSRECHT § 163e, Rn. 18–19 (4th ed. 2016).
34. STPO § 163e(1).
35. *Id.* § 163e(2).
36. *Id.* § 163e(4).
37. BJÖRN GERCKE ET AL., HEIDELBERGER KOMMENTAR ZUR STPO § 100h, Rn 4 (5th ed. 2012).
38. SIGRID HEGMANN, BECK'SCHER ONLINE-KOMMENTAR STPO § 100h, Rn. 6 (27th ed. 2017).
39. RALF GÜNTHER, MÜNCHENER KOMMENTAR ZUR STPO § 100h, Rn. 6. (1st. ed. 2014).
40. Tobias Singelnstein, *Bildaufnahmen, Orten, Abhören – Entwicklungen und Streitfragen beim Einsatz technischer Mittel zur Strafverfolgung*, NSTZ 2014 at 305, 308.

reasonable suspicion of a criminal offence of substantial significance,[41] but no warrant is required.

In **Italy**, there are no specific statutory provisions on location tracking, and the case law on tracking is largely limited to GPS tracking. In a consistent stream of case law, spearheaded by a judgment in 2002, the Italian Supreme Court found that GPS tracking can—just as human tailing albeit in this case technologically facilitated at a distance—be considered an ordinary activity of examination and ascertainment required from the police on the basis of Articles 55, 347, and 370 of the Italian Criminal Procedure Code.[42] These Articles allow the police to conduct activities that do not substantially infringe fundamental rights or liberties, without further specific statutory rules or safeguards. Tailing and GPS tracking are considered activities that constitute at most a minor privacy interference (not infringing the constitutional right to secrecy of communications[43]), so that no judicial authorisation is required, not even—in contrast to a production order of traffic data—a motivated order from the public prosecutor.[44]

In **the Netherlands**, location tracking currently generally falls under the power of "systematic observation" (*stelselmatige observatie*), which covers visual surveillance and other forms of sensory perception with or without technical devices, as long as no communications are recorded.[45] Systematic observation is described as "systematically follow[ing] a person or systematically observ[ing] [a person's] movements or behavior."[46] The police can observe suspects but also non-suspected persons, such as witnesses.[47] Systematic observation requires an order from the public prosecutor but no warrant and can be conducted for any felony, so it is a low-threshold investigative power.[48] The order can be given for a maximum period of three months but can be prolonged repeatedly

41. STPO § 100h(1).

42. Cass., sez. V, 27 febbraio 2002, n. 16130 (It.). *See also, e.g.*, Cass., sez, I, 10 febbraio 2012, n. 14529 (It.), quoted in Teresa Bene, *Il pedinamento elettronico: truismi e problemi spinosi*, *in* LE INDAGINI ATIPICHE 347, 348 (Adolfo Scalfati ed., 2014).

43. Art. 15 Costituzione [Cost.] (It.).

44. Cass., sez. V, 27 febbraio 2002, n. 16130 (It.); *see also, e.g.*, Cass., sez, I, 10 febbraio 2012, n. 14529 (It.), quoted in Bene, *supra* note 42 at 348.

45. Art. 126g(1) CPC (Neth.).

46. *Id.*

47. G.J.M. CORSTENS & M.J. BORGERS, HET NEDERLANDS STRAFPROCESRECHT 509 (8th ed. 2014).

48. Art. 126g(1) CPC (Neth.); *cf.* Ybo Buruma, *Stelselmatig, een sleutelbegrip in de Wet bijzondere opsporingsbevoegdheden*, 25 NJCM-BULLETIN 649, 651 (2000) (wondering why systematic observation is considered a less intrusive power than, e.g., entering a shed in a meadow or covertly recording a conversation in a market-place). Note that in the proposed modernization of the Code of Criminal Procedure, systematic observation will be allowed only for offenses carrying a maximum prison sentence of one year or more. For more information on this, see proposed art. 2.8.2.1.1 of the *Concept Wetsvoorstel tot vaststelling van Boek 2 van het nieuwe Wetboek van Strafvordering: Het opsporingsonderzoek* [draft Bill for book 2 of the new Criminal Procedure Code: Criminal Investigation, hereinafter *Concept Wetsvoorstel Boek 2*], February 2017, https://www.rijksoverheid.nl/documenten/kamerstukken/2017/02/07/wetsvoorstel-tot-vaststelling-van-boek-2-van-het-nieuwe-wetboek-van-strafvordering [https://perma.cc/A8X3-FEY7] (Neth.).

with three-month periods.[49] To ensure reliability of the evidence, technical devices (e.g., binoculars, photo and video cameras, infrared cameras, thermal imagers, movement detection equipment, and tracking devices[50]) must comply with conditions of the Technical Devices Decree.[51]

The proposed modernization of the Code of Criminal Procedure, with a draft bill published for consultation,[52] includes a specific power for "systematic determination of location." This would be an auxiliary power to enable executing one of the covert investigation powers, such as observation, infiltration, or oral interception; the conditions for systematic determination of location are therefore not *sui generis* but tied to those of another investigation power. The only limitation is that orders for systematic location-determination can be given for at most a month, which can be prolonged repeatedly with additional one-month periods.[53]

In **Poland**, the Code of Criminal Procedure does not regulate covert surveillance powers, except for telecommunication interception. Observations are regulated instead by the Police Act in the context of operational-exploratory activities, which are extra-procedural police powers.[54] Except for observations in non-public places, which are regulated more strictly,[55] the powers of the police to observe and record anything that occurs in public places are almost unlimited under the Police Act. Article 15 allows the police to observe directly (with physical presence of the police officers) and at a distance (via technical means) any event occurring in public spaces,[56] both openly and covertly.[57] This is not limited to particular criminal offences and can be used in any operational matter, does not require approval of a prosecutor or court, and no time limits apply. The only limitation is that the surveillance must be conducted in a manner that minimizes the interference with the personal goods of the persons against whom it is undertaken.[58]

In **the United Kingdom**, location tracking is covered by Part II of the Regulation of Investigatory Powers Act (RIPA), which extends to "monitoring, observing or listening to persons, their movements, conversations or other activities

49. Art. 126g(4) CPC (Neth.).

50. *Kamerstukken II* 1996/97, 25 403, no. 3, p. 71 (Neth.).

51. Art. 126ee CPC (Neth.). *See* Decree on Technical Devices in Criminal Procedure (*Besluit technische hulpmiddelen strafvordering*) (Neth.).

52. *Concept Wetsvoorstel Boek 2* (Neth.), *supra* note 48.

53. *Id.*, proposed art. 2.8.2.10.1.

54. Act of 6 April 1990 on the Police (Pol.).

55. Art. 19 Police Act (Pol.) (regulating operational surveillance in non-public places).

56. Art. 15(5a) Police Act (Pol.) (stipulating that police officers are allowed in the exercise of their service to "observe and, using technical means, register the image of events in public places, and in cases of operational-exploratory and administrative-order activities performed on statutory basis, also the sound associated with those events").

57. BARTOLOMIEJ OPALINSKI, MACIEJ ROGALSKI & PRZEMYSLAW SZUSTAKIEWICZ, USTAWA O POLICJI, KOMENTARZ 75–76 (2015).

58. Art. 15(6) Police Act (Pol.).

and communications."[59] To engage in location tracking or other forms of surveillance, the police must obtain an "authorisation" whenever the intended surveillance is "directed" or "intrusive," as defined by section 26 RIPA.[60] Authorisations, which typically last for three months, do not generally need to be judicially approved, as a designated official of a public body (e.g., an appointee within the police services) may execute authorisations; for most police forces, this will be the superintendent.[61] The Code of Practice stipulates particular proportionality and subsidiarity requirements for granting authorisations.[62] An authorisation for "directed surveillance" or "intrusive surveillance" under RIPA (Part II) provides a public authority with "a lawful basis . . . to carry out covert surveillance activity that is likely to result in the obtaining of private information about a person,"[63] which includes various forms of location tracking.

Finally, in **the United States**, location tracking is largely regulated through Fourth Amendment case law.[64] Prior to *Jones* and *Carpenter*, the use of GPS devices was generally considered permissible without a warrant, as was tracking the location of certain objects through technical devices.[65] In the landmark case of *Jones*, however, the Supreme Court determined that physically installing a GPS tracking unit on a suspect's vehicle requires a warrant, as it constitutes an interference with the defendant's property interest[66] (and, according to the concurring opinions, because it violated the defendant's reasonable expectation of privacy through the cumulative effect of prolonged instances of short-term surveillance).[67] Furthermore, in *Carpenter*, the Supreme Court held that the warrantless acquisition of 127 days' worth of cell site location information (CSLI) violated a person's protected privacy interests under the Fourth Amendment and that a person maintains a legitimate expectation of privacy in such records regardless of

59. HOME OFFICE, COVERT SURVEILLANCE AND PROPERTY INTERFERENCE: REVISED CODE OF PRACTICE 7 (Aug. 2018) (UK).

60. Regulation of Investigatory Powers Act 2000 c. 23 § 26(1)(a)–(b) (UK).

61. The prescribed authorizing officer depends on the particular police force. *See* The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, Schedule 1 (UK).

62. HOME OFFICE, *supra* note 59, at 27.

63. *Id.* at 26. Private information is defined as "any information" that relates to the "private or family life" of any person. *See* Regulation of Investigatory Powers Act 2010 § 26(10) (UK).

64. U.S. CONST. amend. IV.

65. *See, e.g.,* United States v. Karo, 468 U.S. 705 (1984) ("beeper" installed inside a can); United States v. Knotts, 460 U.S. 276 (1983) (using a "beeper" in a chloroform container).

66. United States v. Jones, 565 U.S. 400 (2012). Note that in many later cases where the GPS tracking had occurred prior to *Jones*, courts have applied the "good faith exception" to the exclusionary rule, admitting evidence since the officers had reasonably relied on existing legal precedent at the time they installed the tracking devices. *See, e.g.,* United States v. Cabrera, 651 Fed. Appx. 118 (3rd Cir. 2016) (pre-*Jones* GPS tracking of vehicle fell within exclusionary rule's good faith exception); United States v. Taylor, 776 F.3d 513 (7th Cir. 2015) (warrantless GPS tracking of vehicle was reasonable pre-*Jones*).

67. *Jones*, 565 U.S. at 417–18 (Sotomayor, J., concurring); *id.* at 428–31 (Alito, J., concurring).

"[w]hether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier."[68]

To obtain a warrant for using a "tracking device" (defined broadly as "an electronic or mechanical device which permits the tracking of the movement of a person or object"[69]), Federal Rule of Criminal Procedure 41 stipulates certain specific requirements, particularly relating to the period of installing a device (within 10 days) and the period of execution (an extensible period of at most 45 days).[70] Also, Rule 41 (and Fourth Amendment case law) requires probable cause to obtain a tracking warrant.[71]

II. TYPES OF TRACKING

In this section, we discuss how lawmakers have regulated different forms of location tracking, with particular focus on the categories and criteria used to determine the level of privacy infringement. Due to scope limitations, we do not discuss all jurisdictions from our comparative study for each type of tracking; rather, we focus on the most illustrative examples.

A. Human Observation

The most classic form of location tracking is simply following a person while she moves around. Tailing someone usually happens covertly and is generally limited to public and publicly available places, since following someone into private spaces would often be noticeable by the followed person and thus thwart the purpose of tracking someone's movement pattern. Since this form of tracking is physical and involves close proximity between the follower and the followed, tracking is closely related to visual observation; consequently, most jurisdictions regulate tracking in the same way as visual observation.

Human observation is generally considered only a minor privacy intrusion, or sometimes even no intrusion, across the jurisdictions we studied. Poland provides the widest scope to the police, allowing human observation in publicly accessible places without approval of a prosecutor or court and without formal time limits[72]; also, use of perception-enhancing devices and even visual and aural recordings are allowed with no additional requirements compared to naked-eye observation.[73] Similarly, in Czechia, there are no time or approval restrictions on human observation by police.[74] Although the law distinguishes observation using perception-enhancing tools that enable observation at a distance, such as

68. Carpenter v. United States, 138 S. Ct. 2206 at 2217 (2018).
69. 18 U.S.C. § 3117(b) (2012).
70. *Id.* § 3117(e)(2)(C).
71. *See, e.g.*, *id.* § 3117(d)(1).
72. Police Act (Art. 15/1990) (Pol.).
73. *Id.* Art. 15(5a).
74. Trestní řád [Criminal Procedure Code], Zákon č. 141/1961 Sb. § 158d(1) (Czech).

binoculars,[75] from classical physical observation by police officers,[76] there is legally no difference between the two forms. However, in contrast to Poland, Czech law requires written approval of the prosecutor if recordings are made of what is being observed.[77]

U.K. law does not distinguish between naked-eye observation and recording, but it instead applies criteria of covertness and focus. Visual observation, whether accomplished by the unaided eye or through the use of video surveillance cameras, is subject to RIPA's authorisation requirements only when it is covert[78] and carried out as part of a specific investigation into a person or group of persons (i.e., "directed" surveillance).[79] However, as in Poland, authorisation from a prosecutor or judge is not needed. Instead, approval can be obtained from a designated official of a public body, which can be an appointee within the police services, usually a superintendent.[80]

Poland and Czechia apply stricter conditions when people are observed or followed in non-public places.[81] The U.K. also applies stricter conditions for observation in residential premises, which is termed "intrusive surveillance,"[82] limiting it to cases where the surveillance is necessary for the purpose of preventing or detecting serious crime,[83] and requiring permission by a higher authority (including a chief constable), although not a judicial one.[84]

---

75. Šámal, *supra* note 25, at 2004.

76. *Id.* at 2005.

77. Trestní řád [Criminal Procedure Code], Zákon č. 141/1961 Sb. § 158d(2) (Czech).

78. As defined in Regulation of Investigatory Powers Act 2000, c. 23, § 26(9)(a) (UK), surveillance is covert "if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place."

79. Exceptions to the authorization requirement apply in emergencies or other situations where obtaining an authorization is unpractical, among other situations. *See* HOME OFFICE, *supra* note 59, at 18–25.

80. Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010, § 30 (UK).

81. Police Act (Art. 19/1990) (Pol.) (requiring judicial authorization for observation and recording of people's image in dwellings, means of transport and non-public places. The application for judicial authorization must be submitted by a public prosecutor); Trestní řád [Criminal Procedure Code], Zákon č. 141/1961 Sb. § 158d(3) (Czech) (requiring judicial authorization if the observation interferes with the inviolability of the home, and allowing entry of dwellings only to place technical devices).

82. Regulation of Investigatory Powers Act 2000, ch. 23, § 26(3) (UK) (defining covert surveillance as intrusive when "carried out in relation to anything taking place on any residential premises or in any private vehicle; and [involving] the presence of an individual on the premises or in the vehicle or [being] carried out by means of a surveillance device"). Regulation of Investigatory Powers Act 2000, ch. 23, § 26(5) (UK) specifies that surveillance is not intrusive if it "is carried out without [the surveillance] device being present on the premises or in the vehicle," but will be considered intrusive if "the device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle."

83. Regulation of Investigatory Powers Act 2000, ch. 23, § 32(3)(b) (UK).

84. Intrusive surveillance requires authorization from a "senior authorising officer" (Regulation of Investigatory Powers Act 2000, ch. 23, § 32(1) (UK)), which is usually a chief constable of police (Regulation of Investigatory Powers Act 2000, ch. 23, § 32(6) (UK)).

Rather similarly, but applying a more flexible yardstick, Canadian and U.S. law consider visual observation by the police—including the use of technical devices—to constitute an unreasonable search only when it intrudes upon a person's reasonable expectation of privacy.[85] Visual surveillance in public places to track a suspect is generally considered reasonable, because—as one Quebec court put it—such a suspect cannot expect any privacy or intimacy there ("ne pouvait prétendre à aucun droit d'intimité"),[86] or, in the U.S. Tenth Circuit Court of Appeals' terms, "[t]he use of video equipment and cameras to record activity visible to the naked eye does not ordinarily violate the Fourth Amendment."[87] This conclusion is supported by lower court decisions in Canada holding that no reasonable expectation of privacy exists in the entrance lobby of an apartment building[88] or in the public areas of a public bathroom.[89] However, a reasonable expectation of privacy does exist in a closed bathroom stall in a public bathroom (unless the suspect exposes himself under the dividing wall so that he is visible from the public areas, in which case any subjective expectation of privacy becomes unreasonable).[90] Similarly, U.S. courts have held that a person cannot maintain a legitimate expectation of privacy in activities that occur outside their home and that are visible to any passersby (for example, from a public road or sidewalk).[91] However, under the Supreme Court's decision in *Kyllo v. United States*, observation conducted by the use of a device that is "not in general public use, to explore details of the home that

85. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281–82 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."); R. v. Wong, [1990] 3 S.C.R. 36 (Can.).

86. R. v. Joyal, [1995] 43 C.R. 4th 317 (Can.) (no reasonable expectation of privacy in the entrance lobby of an apartment building).

87. United States v. Jackson, 213 F.3d 1269, 1280 (10th Cir. 2000), *vacated on other grounds*, 531 U.S. 1033 (2000).

88. R. v. Silva, [1995] 26 O.R. 3d 554 (Can.).

89. R. v. LeBeau, [1988] CanLII 3271 (ON CA) (Can.).

90. *Id.* ¶¶ 49–52.

91. United States v. Houston, 813 F.3d 282, 287–88 (6th Cir. 2016) ("There is no Fourth Amendment violation, because Houston had no reasonable expectation of privacy in video footage recorded by a camera that was located on top of a public utility pole and that captured the same views enjoyed by passersby on public roads."); *see also* California v. Ciraolo, 476 U.S. 207, 213 (1986) ("The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible."). However, in at least one district court, a trial judge has found that extended and warrantless video surveillance of a home can violate a reasonable expectation of privacy. Order Granting Defendant's Motion to Suppress, United States v. Vargas, No. CR-13-6025 EFS (E.D. Wash. Dec. 15, 2014) ("[S]ociety expects that law enforcement's continuous and covert video observation and recording of an individual's front yard must be judicially approved . . . .").

would previously have been unknowable without physical intrusion"[92] could be considered a search for Fourth Amendment purposes.[93]

Italy applies a largely similar framework, since tracking a suspect's movements by *pedinamento* (tailing, etymologically suggesting "following on foot"[94]) falls under the ordinary activities that the police can do without further specific statutory rules or safeguards, at least in public places;[95] additional conditions apply only if the tracking interferes with constitutional rights. Limitations apply particularly if visual recordings are made of a followed person in non-public places. Such recordings cannot be made at all in homes,[96] while they can be made in so-called "reserved places" that are not homes but nevertheless carry a reasonable expectation of privacy: "[I]f a public toilet or a cubicle such as those at issue are not a domicile, they are nevertheless a place which should protect the intimacy and the privacy of the persons, and therefore for the purposes of visual recordings they cannot be treated as a public place or a place exposed to the public."[97] Visual recordings in such reserved places can be made, but only with a motivated decree by a judicial authority, which can be a judge or a public prosecutor.[98]

While the jurisdictions discussed so far distinguish between observation in public and in non-public places, and to some extent depend on the nature of technical devices used, Dutch law employs a more abstract distinction, namely

92. Kyllo v. United States, 533 U.S. 27 (2001).

93. This might include, for example, the use of through-the-wall radar or WiFi signal analysis software, each of which could track movements through walls of a home or other constitutionally protected areas.

94. CLAUDIO MARINELLI, INTERCETTAZIONI PROCESSUALI E NUOVI MEZZI DI RICERCA DELLA PROVA 227 (2007).

95. CODICE DI PROCEDURA PENALE [C.P.P] [CODE OF CRIMINAL PROCEDURE] art. 55 (It.) (defining the task of the police to "conduct the activities necessary to secure the sources of evidence"), CODICE DI PROCEDURA PENALE [C.P.P] [CODE OF CRIMINAL PROCEDURE] arts. 347–348 (It.) (requiring police to report without delay notices of crime to the public prosecutor, and continuing with the activities mentioned in article 55, collecting in particular every element useful to reconstruct the fact and to identify the perpetrator), and CODICE DI PROCEDURA PENALE [C.P.P] [CODE OF CRIMINAL PROCEDURE] art. 370 (It.) (allowing the public prosecutor to avail himself of the judicial police to conduct investigative and specifically delegated acts).

96. Cass., sez. un., 28 luglio 2006, *Dir. pen. proc.*, 2006, 1349 et seq. (It.). The constitutional protection of domiciles (Art. 14 Costituzione [Cost.] (It.)) serves to protect not only the right to include or exclude others from entering the place; it also protects "an intangible sphere of privacy [*riservatezza*], which can also be harmed—through technical devices—without the necessity of physical intrusion," according to GIUSEPPE TABASCO, PROVE NON DISCIPLINATE DALLA LEGGE NEL PROCESSO PENALE. LE 'PROVE ATIPICHE' TRA TEORIA E PRASSI 155 (2011). To infringe this sphere, the Constitution requires a legal basis and a stipulation of legal guarantees, and since these do not exist in Italian law for visual recordings in domiciliary places, the Supreme Court concluded that this is not allowed.

97. CORRADO RIZZO, LO STRUMENTO INVESTIGATIVO DELLE RIPRESE VISIVE 48–49 (2012), referring to Cass., sez. un., 28 luglio 2006, *Dir. pen. proc.*, 2006 (It.). The ground for protecting reserved places that are not domiciles is article 2 of the Constitution, which includes the general right to privacy. *Id.*

98. RIZZO, *supra* note 97, at 49.

between "systematic" and "non-systematic" forms of observation or tracking.[99] Non-systematic observation can be based on the general task description of the police without particular conditions,[100] while systematic observation requires an order of the public prosecutor.[101] The conceptualisation of "systematicness" is the closest that the Dutch lawmaker has come to defining or describing privacy, so it is illuminating to study this criterion in some depth. The generally used definition of systematicness is that it results in "a more or less complete image being obtained of certain aspects of someone's [private] life."[102] Legislative history, case law, and doctrine mention various factors that influence the intensity of the observation and thus, qualification of an observation as systematic. They are neither necessary nor sufficient conditions: generally, a combination of factors will be decisive.[103] The main factors are:[104] 1) use of a technical device that goes beyond binoculars and similar ordinary perception-enhancing devices, such as recording devices;[105] 2) place (observation in public places is a lesser interference than observation in closed or intimate places);[106] 3) intrusiveness, continuity or frequency (the closer, deeper, and more frequent the observation, the higher its intensity; continuous observation will be more intrusive than observation with intervals);[107] 4) duration (the longer the observation, the higher the intensity);[108] and, possibly, 5) the degree of suspicion against the observed person (which might influence the reasonable expectation someone may hold not to be observed by the police).[109] Although analysis using

99. Note, however, that Dutch law generally prohibits visual recordings inside the home (although allowing it in other non-public places). *See Kamerstukken II* 1996/97, 25 403, no. 3, 71 (Neth.). Hence, the distinction between systematic and non-systematic observation comes on top of the basic distinction between homes and non-homes as observation sites.

100. Wet van 12 juli 2012, Stb. 2012, Art. 3 (Neth.).

101. Art. 126g(1), SV (Neth.).

102. *Kamerstukken II* 1996/97, 25 403, no. 3, 26–27 (Neth.). This explanatory memorandum used the term "someone's life," but it is generally presumed that this refers to someone's "private life." *See, e.g.*, T. Blom, *Comment No. 2 on Art. 126g*, *in* TEKST & COMMENTAAR STRAFVORDERING (C.P.M. Cleiren, J.H. Crijns & M.J.M. Verpalen eds., 11th ed. 2015).

103. Blom, *supra* note 102, comment 4(d–e).

104. See Bert-Jaap Koops, *Criminal Investigation and Privacy in Dutch Law* 29 (Tilburg Univ. TILT L. & Tech. Working Paper Series, version 1.0, 2016), http://ssrn.com/abstract=2837483 [https://perma.cc/V23X-DZEF] at 29, for a more detailed overview.

105. The only exception is taking a few photographs, which is considered non-systematic. Blom, *supra* note 102, comment 4(e).

106. Observation of a suspect's behavior in public (such as painting graffiti) does not see to "a situation in which the suspect could expect to be able to be himself uninhibitedly." HR 20 april 2004, NJ 2004, 525 (Neth.).

107. *Kamerstukken II* 1997/98, 25 403, no. 7, 49 (Neth.).

108. Duration seems altogether less relevant than the other factors: a short observation with a device in an intimate place, such as a brothel, is systematic (*Kamerstukken II* 1997/98, 25 403, no. 7, 47 (Neth.)), but an observation over a period 27 months in which the suspect was observed 60 times in public spaces (mainly by humans, although also by one static camera aimed at someone else's dwelling) was not systematic (HR 18 mei 1999, NJ 2000, 104 (Neth.)).

109. Although not usually mentioned in textbooks, some case law has indicated that the degree of suspicion needs to be taken into account in determining whether an observation makes a more than limited infringement on privacy. Hoge Raad 10 april 2001, ECLI:NL:HR:2001:AB0970 (Neth.).

these factors leads to a more fine-grained assessment of privacy intrusions, Dutch law is similar to the above-mentioned jurisdictions in that even systematic observation is considered a relatively unobtrusive investigation power—the only real limitation is that a prosecutor's (but not a court's) authorization is needed for systematic observation.[110]

This contrasts to German law, which is the outlier in our jurisdictions as it has far stricter limitations to human observation. Only limited forms of tracking can be conducted by the police without a warrant: the observation has to take place outside the home and—the strongest limitation—can only be conducted for a maximum of 24 hours.[111] Observations longer than 24 hours require a court warrant.[112] This suggests that location tracking and visual observation, including in public space, are considered substantially more privacy-intrusive in Germany than in the other jurisdictions we studied. The need for adopting specific, and stricter, regulation of longer-term observation in Germany is its perceived potential for considerably interfering with the general personality right and the right to self-determination.[113] Especially in cases where such observation is combined with technical means, it can lead to such an accumulation of investigative means that a clear personality profile of the observed person is created, which intensively interferes with the right to informational self-determination.[114] Due to this potentially high intrusiveness, judicial authorization is required for longer-term observations.[115]

B. GPS Tracking

In most jurisdictions, GPS tracking is considered a form of, or an investigatory method analogous to, observation, as it involves observing the movements of a person or an object. In this section, we discuss differences and similarities between the regulation of GPS tracking and human observation in our jurisdictions.

1. Mainstream: Not More Intrusive than Human Observation

By and large, the jurisdictions we studied consider GPS tracking to be about as intrusive as (technology-facilitated) human observation. Czech and Italian law do not distinguish between the two forms at all and apply the same conditions. In the words of the Italian Supreme Court, GPS tracking is "a modality, technologically typified, of tailing."[116] Dutch law applies the same framework to both forms,[117] implying that GPS tracking can be equally, more, or less intrusive than human

110. Art. 126g(1), SV (Neth.).
111. STRAFPROZESSORDNUNG [StPO] [CODE OF CRIMINAL PROCEDURE] §§ 161, 163 (Ger.).
112. *Id.* § 163f(3).
113. KARLSRUHER KOMMENTAR ZUR STRAFPROZESSORDNUNG [StPO] [KARLSRUHER COMMENTARY ON CRIMINAL PROCEDURE] § 163f (Ger.).
114. *Id.*
115. *Id.*
116. Cass., sez. un., 27 febbraio 2002, no. 16130 (It.).
117. Art. 126g(1), SV (Neth.).

observation, depending on the type of device, duration, intensity, and places of observation.

Somewhat similarly, GPS tracking can be more or less intrusive than "ordinary" surveillance under U.K. law, depending on the circumstances. On the one hand, GPS tracking of cars is regulated as "intrusive surveillance" (subject to heightened regulation) if it is "carried out in relation to anything taking place . . . in any private vehicle" and involves the use of a surveillance device in a vehicle.[118] On the other hand, otherwise intrusive surveillance that only involves the use of a surveillance device designed or adapted solely to provide information about the location of a vehicle (and that does not involve physical trespass) is not considered intrusive.[119] The relevant code of practice also presumes that such use of a surveillance device, on its own, may not always constitute directed surveillance, as it may not result in capturing private information about an individual.[120] As such, the limited use of such a tracking device by itself (e.g., to determine the location of a vehicle at one given point in time) may not be subject to regulation at all. However, when the use of the device (including when it is used in conjunction with other forms of investigatory activities) is likely to result in capturing private information (e.g., "monitoring . . . the movements of the occupant(s) of [a] vehicle"), the surveillance must be authorized as a form of directed surveillance under RIPA.[121]

This nuanced regulation of GPS tracking of vehicles in the U.K. suggests, first, that location tracking of goods is not considered privacy-relevant while location tracking of people *is* privacy-relevant. Therefore, privacy relevance depends on whether installing a tracking device on a car has the purpose of following the car or its occupants—a distinction that may be hard to make in practice. Second, the privacy intrusion is considered more severe if installing a GPS device involves entering the vehicle, since this constitutes trespass. This suggests that in the U.K., the privacy of property or of private places is valued more strongly than the behavioral privacy that is at issue when someone's movements are tracked. This is similar to Italy, where the literature on GPS tracking discusses whether the driver-and-passenger compartment of a car is a place of private abode; if so, entering into a car to place a GPS tracker would not be allowed in the absence of specific legislation stipulating the modality and safeguards.[122] A majority of scholarly doctrine considers cars to be a place of private abode (and hence protected), while

118. Regulation of Investigatory Powers Act 2000, c. 23, § 26(3) (UK).

119. *Id.* at c. 23, § 26(4).

120. HOME OFFICE, *supra* note 59, at 17 ("[T]he use of surveillance devices designed or adapted for the purpose of providing information regarding the location of a vehicle is not considered to be intrusive surveillance. The use of such devices alone does not necessarily constitute directed surveillance as they do not necessarily provide private information about any individual, but sometimes only supply information about the location of that particular device at any one time.").

121. *Id.* at 18.

122. *See* Koops, *supra* note 104, at 28–29 (including references).

a majority of case law does not.[123] However, as Bene dryly observes, the discussion is highly academic because technological evolution has enabled the placing of GPS trackers also on the *outside* of vehicles, thus foregoing the problem of having to enter a protected space.[124] (To be sure, this may still constitute an interference with property, but that is a relevant consideration only in the U.S. and the U.K.)[125]

The argument that GPS tracking does not interfere with the inviolability of the home and is limited to tracking people (or objects) in public is also applied in Germany. In an oft-cited decision, the Federal Supreme Court (*Bundesgerichtshof*) judged that the use of GPS technology does not interfere with the constitutional right to inviolability of the home; nor does it touch upon the inviolable core (*Kernbereich*) of the private sphere or the right to informational self-determination.[126] It is altogether a "lesser constitutional rights-interfering surveillance measure, for which the required judicial control takes place in the criminal proceedings," and it is a proportionate interference in light of the considerable interest in investigating and prosecuting crime.[127] We see the same reasoning in U.S. case law prior to *Jones*: automobiles moving about on public roads are exposed to public view and scrutiny, thus diminishing the expectation of privacy a driver or passenger may have in the vehicle's location.[128]

While part of the debate on GPS tracking focuses on spatial privacy, another part discusses it in the context of communicational privacy. Associating GPS technology with cell-phones (which also have a positioning function, although not necessarily GPS), the Italian Supreme Court observed that the constitutional right to secrecy of communications was not at stake, since communications interception does not include

> the investigative activity conducted to follow the movements on the territory of a person, to locate him and therefore to examine—at a distance—not the flow of communications that he himself sends or receives, but his presence at a specific place at a certain moment, as well as the followed itinerary, the encounters that occurred etc.[129]

---

123. MARINELLI, *supra* note 94, at 248.

124. Bene, *supra* note 42, at 360.

125. United States v. Jones, 565 U.S. 400 (2012). In the U.K., GPS tracking will constitute property interference if the tracking device is independently attached to property, such as a vehicle, and sends back location data to the police; in many situations, this will require a separate authorization under the Police Act 1997, besides a RIPA-based authorization for directed surveillance.

126. Bundesgerichtshof [BGH] [Federal Court of Justice] Jan. 24, 2001, OLG DÜSSELDORF, 3 StR 324/00 (Ger.).

127. *Id.*

128. *See e.g.*, Rakas v. Illinois, 439 U.S. 128, 153–54 & n.2 (1978) (Powell, J., concurring); South Dakota v. Opperman, 428 U.S. 364, 368 (1976); Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (plurality opinion); United States v. Hufford, 539 F.2d 32 (9th Cir. 1976) ("One has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects. A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view.").

129. Cass., sez. un., 27 febbraio 2002, no. 16130 (It.).

In a similar vein, the European Court of Human Rights judged "that GPS surveillance must be considered to interfere less with a person's private life than, for instance, telephone tapping,"[130] and found that "GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings."[131] In other words, because GPS tracking of a car only registers a person's movements (in public), it is considered less intrusive than wiretapping and human observation, since only people's bare location coordinates are recorded, rather than what they do, say, or otherwise express through their conduct *in situ*.

In summary, the larger picture is that in statutory and case law, GPS tracking is generally considered not more (and sometimes even less) intrusive than human observation.

2. Undercurrent: More Intrusive than Human Observation

In contrast to the mainstream picture, we observe an undercurrent in case law, and particularly in doctrine, that recognizes a potentially larger privacy intrusion through GPS tracking. A relevant factor is that a GPS tracker records location with high frequency by itself, without humans having to be close to the tracked person or car. The GPS tracking in the *Uzun* case was considered acceptable partly because it was applied only after a less intrusive measure had failed: Uzun and his accomplice had detected and destroyed the transmitters (*Peilsender*) previously installed in the car, "the use of which (other than with the GPS) necessitated the knowledge of where approximately the person to be located could be found" and which was "less intrusive" than GPS surveillance.[132] Similarly, in the only Canadian Supreme Court case on the constitutionality of warrantless location tracking (*R. v. Wise*), the court found that a transmitter (or beeper) was only minimally intrusive because "it was capable of giving only a very rough idea of the vehicle's location. Certainly, it could not be said that the device was capable of tracking the location of a vehicle at all times."[133] Since GPS tracking *is* capable of just that, the *Wise* rationale would not apply, and GPS tracking would therefore probably constitute an unreasonable search in Canada, although the courts have not yet decided this specific question.

A more extensive argument has been made by the Polish District Court in *Suwałki*, judging that using a GPS tracker undoubtedly led to collecting and processing of a much larger, and more precise, set of data about the places the

130. Uzun v. Germany, App. No. 35623/05, Eur. Ct. H.R. § 72 (2010).

131. *Id.* § 52.

132. *Id.* § 78.

133. R. v. Wise, [1992] 1 S.C.R. 527 (Can.). (finding that use of a beeper ("a low power radio transmitter") constituted an unreasonable search because it violated the defendant's reasonable expectation of privacy in the location and movements of his vehicle and because it was installed after the expiration of a valid warrant, but that the search was "only minimally intrusive" and the tracking evidence should not be excluded).

observed person stayed, as well as data on how they moved in public space, than could be obtained by direct observation.[134] Therefore, it constituted a further-reaching interference in private life.[135] Additionally, the covert manner of the operation of a GPS device, combined with the way the device communicated (sending regular messages through a mobile phone network), constituted operational surveillance under Article 19(3) of the Police Act (Poland), which is subject to strict procedural requirements.[136] The District Court rejected the idea that, since anyone can observe a vehicle moving in public space, the information obtained by GPS tracking could be seen as publicly available.[137] The court contrasted such individual bits of information that lead to no significant conclusions about the person, with systematic collection of location data for a longer period, which reveals where the person went, for how long, and where they moved.[138] The latter constitutes surveillance of the person and a violation of freedoms and rights of the person.[139] Interestingly, whereas the wording of Article 19(3) of the Police Act (Poland) at the time was sufficiently technology neutral ("using technical means to covertly obtain information and evidence") to accommodate GPS tracking, the provision has since been split into a list of more specific powers,[140] none of which easily fits GPS tracking. It is therefore questionable whether the new wording of Article 19 of the Police Act (Poland) on operational surveillance, which only mentions *visual* and *aural* observation and recording, still allows for the use of GPS trackers by police.[141]

Using similar arguments as the *Suwałki* court, Italian scholars heavily criticize the Italian (case) law's equation of GPS tracking with human tailing. They provide arguments for why GPS tracking is more invasive than traditional tailing: it can be very precise and continuous, and it can also track people in places that are not visible or readily accessible (where human tailing would be impracticable or not allowed);[142] it has fewer practical obstacles in time and space;[143] and it constitutes a greater privacy infringement than classic tailing because of the thoroughness of the investigation and the possibility to protract it for long periods.[144] On the other hand, authors also observe that a person's movements are tracked only when the tagged car or object is being used, which is less frequent than continuous human tailing.[145]

134. II Ka 267/13 District Court Suwalki, 19 December 2013 (Pol.).
135. *Id.*
136. *Id.*
137. *Id.*
138. *Id.*
139. *Id.*
140. Police Act art. 19 (Pol.).
141. OPALINSKI, ROGALSKI & SZUSTAKIEWICZ, *supra* note 57, at 76.
142. Bene, *supra* note 42, at 352; Marinelli, *supra* note 94, at 237; Stefano Marcolini, *Le cosiddette perquisizioni* on line *(o perquisizioni elettroniche)*, CASSAZIONE PENALE 2855, 2867 (2010).
143. Marinelli, *supra* note 94, at 237; Marcolini, *supra* note 142, at 2867.
144. Daniela Gentile, *Tracking satellitare mediante gps: attività atipica di indagine o intercettazione di dati?*, DIRITTO PENALE E PROCESSO 1464, 1472 (2010).
145. Bene, *supra* note 42, at 352.

Moreover, physical tailing enables police to see the location of others during meetings, which is not possible with electronic tailing unless the other persons are also being electronically monitored.[146] Overall, however, Italian authors tend to consider GPS tracking to constitute a more serious privacy infringement than human tailing, although still less serious than intercepting communications.

Perhaps the most forcible argumentation about the privacy infringement made possible by GPS tracking has been made in *United States v. Maynard* (which later became *Jones* on appeal to the Supreme Court).[147] The judge stressed that the facts of the case, which involved continuous GPS monitoring of the defendant's vehicle over a 28-day period, addressed the question whether "dragnet-type law enforcement practices" such as "'wholesale' or 'mass' electronic surveillance . . . require[] a warrant."[148] The judge held that prolonged GPS monitoring of a vehicle for twenty-eight days amounted to an unreasonable search because the GPS monitoring had obtained information that was "not exposed to the public":

> [U]nlike one's movements during a single journey, the whole of one's movements over the course of a month is not actually exposed to the public because the likelihood anyone will observe all those movements is effectively nil. Second, the whole of one's movements is not exposed constructively even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts.[149]

And, according to the judge, prolonged GPS tracking violated the defendant's reasonable expectation of privacy, in part because

> [p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[150]

---

146. Marinelli, *supra* note 94, at 236–37.
147. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).
148. *Id.* at 556, 558.
149. *Id.* at 558; *see also infra* Section III(B)(3)(b).
150. *Maynard*, 615 F.3d at 562.

This reasoning was later endorsed at the Supreme Court by both of the concurring opinions in *Jones*.[151]

In this undercurrent of arguments, we see a recognition that GPS tracking may have superficial similarities with traditional forms of location tracking but involves a *different* way of tracking. The affordances of GPS differ from human observation: in several respects, location tracking is more fine-grained, easier, and wider in scope than human observation, while in other respects, it may be less detailed. This implies that GPS tracking cannot easily be judged to be *intrinsically* more intrusive than technology-facilitated human observation; nor, however, can it be simply equated with traditional forms of observation. We think this is the main reason why authors, and sometimes judges, have proposed different normative frames to evaluate the intrusiveness of GPS tracking, such as the mosaic theory[152] or a right not to be localized[153]—frames that have yet to be adopted in mainstream thinking and case law on location tracking, but that have potential for changing the legal evaluation of GPS and other forms of tracking with different affordances than human tailing.

3. Installing GPS Trackers on (Items Worn by) Humans

Some jurisdictions apply special rules for installing and using tracking devices on human bodies, or on items usually carried by humans, as this is considered a graver (or different type of) privacy infringement than tracking cars or other objects. The Netherlands has the most far-reaching limitation: technical devices for observation purposes may not be placed on a person, except with the person's consent.[154] "On a person" means on the body or clothes, including on items carried in clothing, such as a lighter; a tracking device may, however, be placed on a suitcase.[155] This implies that items usually carried in clothes' pockets, such as smartphones, may not be tracked with a tracking device. The distinction between items carried "on" the person and items carried "by" the person seems subtle, but can be explained by the constitutional framework, which contains a separate constitutional right to bodily integrity.[156] Interfering with items carried "on" the person (i.e., on the skin or in clothes) constitutes an interference with the body, while items carried by (but not on) persons, such as bags or suitcases, do not fall

151. United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring); *id.* at 428–31 (Alito, J., concurring).

152. *See infra* Section III(B)(3)(b).

153. *See infra* Section III(B)(3)(a).

154. CPC Art. 126g(3) (Neth.). With the Computer Crime III Act (adopted in June 2018, entry into force 1 March 2019), an exception is made for hacked devices: the police are allowed to hack into a device (such as a smartphone) carried on the body for the purposes of systematic observation (e.g., remotely install location-tracking software or malware to turn on the smartphone's camera). *See Staatsblad* 2018, 322 at 5–6 (Neth.).

155. *Kamerstukken II* 1996/97, 25 403, no. 3 at 71 (Neth.).

156. GW. art. 11.

within the scope of bodily integrity.[157] The prohibition of planting tracking devices on persons is in line with how privacy is generally protected in Dutch criminal procedure: bodily privacy is regarded as the most important aspect of privacy and is generally more strongly protected than spatial or communicational privacy.[158]

The Netherlands is an outlier in this respect, however. In other jurisdictions, persons (and items carried on persons) can be tracked, albeit sometimes under stricter conditions than those that apply to tracking objects. In *Grady v. United States*, the Court held that "a State . . . conducts a search when it attaches a device to a person's body, without consent, for the purpose of tracking that individual's movements."[159] Therefore, a warrant is required for non-consensually installing a tracking device on a person. In Canada, the Canadian Criminal Code distinguishes between two types of tracking warrants.[160] Parliament determined that tracking individuals (or things "usually carried or worn by" individuals, such as cell-phones) was more privacy-invasive than tracking vehicles or the location of transactions and should be based on a higher standard of proof; namely, "reasonable grounds to *believe*"[161] rather than "reasonable grounds to *suspect* that an offence has been or will be committed . . . and that tracking [an individual, thing, or transaction] will assist in the investigation of the offence."[162] Thus, the distinction between installing tracking devices on persons as opposed to objects is far less strict than in the Netherlands: the U.S. has a warrant requirement for both humans and cars, while Canada applies only a stricter condition in terms of the level of suspicion, but not in terms of authorization.[163]

C. Cell-Phone Tracking

Where GPS tracking (of the sort described above, as typified by the facts of *Jones*) depends on the police covertly installing a device to trace movement patterns, a different form of location tracking uses the location data that people themselves

157. Note that placing tracking devices in items (usually) carried by persons will, nevertheless, imply following a person, and therefore (if it crosses the threshold of systematicness) will falls under the power of systematic observation and require a prosecutor's order. *See Kamerstukken II* 1997/98, 25 403, no. 7 at 48 (Neth.).

158. Koops, *supra* note 104 at 52.

159. Grady v. North Carolina, 135 S. Ct. 1368, 1370 (2015). This did not concern criminal investigation, but a state program that mandated satellite-based monitoring of certain recidivist sex offenders after they had completed their sentences.

160. Protecting Canadians from Online Crime Act, S.C. 2014, c 31 (Can.).

161. R.S.C. § 492.1(2) (Can.) (emphasis added).

162. *Id.* § 492.1(1) (emphasis added); *see also* R. v. Grandison, [2016] B.C.S.C. at para. 34.

163. *See also* TAMIR ISRAEL & CHRISTOPHER PARSONS, 2 GONE OPAQUE? AN ANALYSIS OF HYPOTHETICAL IMSI CATCHER OVERUSE IN CANADA 69 (2016), https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf [https://perma.cc/M5D4-9QDY] ("[D]ifferentiation between Object Tracking and Individual Tracking Warrants may be unsustainable since both kinds of surveillance can engage roughly equivalent privacy interests. Tracking an individual's car, for example, can provide a comprehensive picture of that person's location and, over time, of their personal life as it would indicate the stores they visit, the medical clinics they visit, the religious institutions they visit, the people they visit, etc.").

generate (also sometimes by GPS) through their cell-phones. The primary way that police acquire such data is by obtaining and serving a production order on a telecommunications provider, but this can be supplemented by other measures such as the use of stealth SMS or IMSI catchers.[164] Since cell-phones rely on cells to communicate, and cells have a geographic position with a range of tens of miles to some tens of yards (depending on the population density), location data from cell-phones provide an interesting source for tracking people's movements. Additionally, if wireless carriers (or service providers, e.g., Google) also capture and maintain GPS or Wi-Fi location data sourced from their subscribers' cell-phones, location information can be even more precise than cell site location information. And, in contrast to the physical installation of tracking devices considered in the previous section, accessing GPS or other location information through cell-phones or other connected devices can be accomplished remotely, without any physical intrusion.

In *Carpenter*, the U.S. Supreme Court cited its earlier decision in *Riley v. California*,[165] noting that tracking the location of a cell-phone presents significant privacy concerns because cell-phones have become "almost a 'feature of human anatomy,'" so that "when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user."[166] In the subsections that follow, we discuss the regulation of cell-phone tracking in the jurisdictions in our sample.

1. Production Order to Telecoms Providers of Cell Phone Location Data

a. Historical Data

All jurisdictions in our study consider cell-phone location data to be part of, or similar to, the metadata (or traffic data) that can be requested from telecoms providers,[167] and generally, these jurisdictions treat metadata as less privacy-

164. *See* Brad Heath, *Police Secretly Tracking Cellphones to Solve Routine Crimes*, USA TODAY, Aug. 23, 2015, https://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/ [https://perma.cc/2GJZ-DD7Y].

165. Riley v. California, 134 S. Ct. 2473 (2014).

166. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018) (citing *Riley*, 134 S. Ct. at 2484); *see also* discussion *infra* Section II(C)(1)(a).

167. *See, e.g.*, s. 66(3) of Act No. 273/2008 Sb. on the Police (Czech) (mentioning location data alongside traffic data that can be requested from public communications providers); CPC art. 254-bis (It.) (including location data (*data di ubicazione*) among the data stored with informatics, telematics, and telecommunications providers that can be acquired through seizure); art. 2 Besluit vorderen gegevens telecommunicatie 2004, Stb. 2004, 394 (Neth.) (including cell location in the mobile network among traffic data of which production can be ordered); Judgement of the Constitutional Court, 30 July 2014, sign. K 23/11, OTK ZU 2014, nr 7, poz. 180 (Pol.) (including data allowing the identification of the geographical location of the communication parties among metadata); United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016) (obtaining cell tower locational data from defendants' wireless carrier is similar to obtaining metadata as regulated by the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*); RIPA § 21(6)(a) (Eng.) (defining location data as within the definition of "traffic data," which is obtainable subject to "authorisation" under RIPA § 23). For additional analysis of UK law, see SIMON MCKAY,

sensitive than communications content.[168] As a result, not all jurisdictions require a warrant for a location-data or metadata production order. A warrant is required to acquire historical CSLI in Germany[169] and—after *Carpenter*—in the U.S. In Czechia, a warrant is required for traffic data "that are subject to telecommunications secrecy or the protection of personal and intermediation data,"[170] but not for traffic and location data that are not subject to such protection—these latter data can be ordered by the police.[171] In Canada, a production order can be given to telecom providers to disclose historical tracking data, which requires authorization by a justice or judge and "reasonable grounds to suspect that an offence has been or will be committed . . . and the tracking data is in the person's possession or control and will assist in the investigation of the offence."[172]

In contrast, Italy, the Netherlands, and Poland consider authorization from a public prosecutor sufficient.[173] Moreover, the Italian Supreme Court has also ruled that the absence of an authorisation from a public prosecutor does not render produced traffic data unusable as evidence, given the limited intrusion into the private sphere and given that it does not fall under the strict norms for interception.[174]

In the U.S., the legal status of CSLI changed considerably with *Carpenter*. In prior cases involving police accessing historical location information from cellular service providers under the Stored Communications Act,[175] courts generally held that no search had occurred, citing the third-party doctrine and equating location information with non-content information (such as that captured by pen registers) that attracts lesser constitutional protection.[176] Under the Stored Communications

---

COVERT POLICING: LAW AND PRACTICE 127–29 (2nd ed., Oxford University Press 2015). Note that Canada has separate powers for the production of transmission data (i.e., metadata) (section 487.016 CC) and production of tracking data (i.e., location data) (section 487.017 CC), but the requirements are the same and both orders use the same form (Form 5.007).

168. *See, e.g.*, Cass., Sez. V, 10 marzo 2010, n. 9667 (It.), as discussed in Gentile, *supra* note 144 (holding that obtaining traffic data constitutes a limited intrusion into the private sphere and does not fall under the strict norms for interception); *Kamerstukken II* 2013/14, 33 989, No. 3 at 19 (Neth.) (holding that there is no justification to accord all traffic data the same level of constitutional protection as communications content); *see also* Smith v. Maryland, 442 U.S. 735, 745 (1979) (finding numbers dialed on a phone less protection-worthy than content).

169. CPC § 100g *juncto* §§ 101a, 100e (Ger.); *see also* Benjamin Vogel, Patrick Köppen & Thomas Wahl, *Germany*, *in* ACCESS TO TELECOMMUNICATION DATA IN CRIMINAL JUSTICE 499, 545 (Ulrich Sieber & Nicolas von zur Mühlen eds., 2016).

170. CPC § 88a(1) (Czech).

171. § 66(3) Act No 273/2008 Sb. on the Police (Czech); *see* Radim Polcák, *Czech Republic Slovakia*, *in* ACCESS TO TELECOMMUNICATION DATA IN CRIMINAL JUSTICE 387 (Ulrich Sieber and Nicolas von zur Mühlen eds., 2016).

172. CC [CRIMINAL CODE] § 487.017 (Can.).

173. DATA PROTECTION ACT Art. 132(3) (It.); CPC art. 126n(1) (Neth.); CPC art. 218(1) (Pol.).

174. Cass., Sez. V, 10 marzo 2010, n. 9667, as discussed in Gentile, *supra* note 144.

175. 18 U.S.C. §§ 2701 *et seq*.

176. United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016) (stating that government did not conduct a "search" for Fourth Amendment purposes when it obtained cell tower locational data from defendants' wireless carrier—based on the non-content/metadata distinction and the third-party

Act, the government could access such records so long as it demonstrated "reasonable grounds" to believe that the records were "relevant and material to an ongoing investigation,"[177] a lesser standard than the probable cause required for a warrant. (Note, however, that at the state level, a warrant may have been required for obtaining some cell-phone location information, even prior to *Carpenter*.)[178]

However, in *Carpenter*, a majority of the Supreme Court held that "the ability to chronicle a person's past movements through the record of his cell phone signals" provided police with information that was "detailed, encyclopedic, and effortlessly compiled"[179]—thus implicating Fourth Amendment scrutiny. In doing so, the Court ruled that police could not rely on less-demanding court orders under the Stored Communications Act to acquire such information from service providers and that the third-party doctrine did not apply to the acquisition of historical CSLI.[180] In fact, the Court noted that "historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*,"[181] precisely because,

> [u]nlike the bugged container in *Knotts* or the car in *Jones*, a cell phone . . . tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales.[182]

Besides authorization requirements, some jurisdictions limit the power to order location-data production to relatively serious crimes: crimes with a maximum penalty of at least three (Czechia) or four (Netherlands) years' imprisonment, or serious crimes (Germany).[183] Other jurisdictions, however, have no such limitation in type or seriousness of offenses.

---

doctrine); United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (stating that cell-site tracking without a warrant did not violate the Fourth Amendment due to the third-party doctrine), *overruling* United States v. Graham, 796 F.3d 332 (4th Cir. 2015); United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (obtaining CSLI under the SCA not a "search" for Fourth Amendment purposes), *overruled* 754 F.3d 1205 (2014).

177. 18 U.S.C. § 2703(d).

178. Peter Cihon, *Status of Location Privacy Legislation in the States: 2015*, ACLU (Aug. 26, 2015), https://www.aclu.org/blog/free-future/status-location-privacy-legislation-states-2015 [https://perma.cc/QT6Q-3WVP] (mentioning six states protecting both historical and real-time location information from warrantless search).

179. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

180. *Id.* at 2217.

181. *Id.* at 2218.

182. *Id.* (citations omitted).

183. Trestní řád [Criminal Procedure Code], Zákon č. 88a/2012 Sb. (Czech) (for traffic data that are subject to the protection of personal and intermediation data); STRAFPROZESSORDNUNG [StPO] [CODE OF CRIMINAL PROCEDURE] § 100g (Ger.) (translation at *The German Code of Criminal Procedure StPO*, BUNDESMINISTERIUM DER JUSTIZ UND FÜR VERBRAUCHERSCHUTZ, http://www.gesetze-im-internet.de/englisch_stpo/index.html [https://perma.cc/D46U-V3KD] (last visited Feb. 3, 2019)); Art. 126n para. 1 Sv (Neth.).

Overall, then (with notable exceptions), a production order for location data seems to constitute a moderate to intermediate form of privacy intrusion—certainly not negligible, but also definitely not as intrusive as communications interception. This state of the law is criticized by general literature arguing that the distinction between metadata and content is outdated (in the normative sense, since collecting metadata can be at least as intrusive as interception)[184] and specific literature claiming that national law on traffic data collection has too few safeguards.[185] However, with few exceptions,[186] such criticism has not yet induced lawmakers or judges to revise the way they assess the intrusiveness of metadata production orders.

Specifically, for *location* metadata (as opposed to metadata in general), some courts have advanced interesting arguments to assess the privacy intrusion, also in comparison with other forms of tracking. As framed by the U.S. Supreme Court in *Carpenter* (using reasoning drawn from the concurring opinions in *Jones*), historical CSLI

> provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through

184. *See, e.g.*, BERT-JAAP KOOPS & JAN SMITS, VERKEERSGEGEVENS EN ARTIKEL 13 GRONDWET, EEN TECHNISCHE EN JURIDISCHE ANALYSE VAN HET ONDERSCHEID TUSSEN VERKEERSGEGEVENS EN INHOUD VAN COMMUNICATIE 140–41 (2014) (arguing that traffic data provide ever more insight into private life and that there is less reason nowadays to protect (only or particularly) communications content); Bryce Clayton Newell & Joseph T. Tennis, *Me, My Metadata, and the NSA: Privacy and Government Metadata Surveillance Programs*, *in* ICONFERENCE 2014 PROCEEDINGS 345, 346 (2014) ("[M]etadata surveillance can be highly intrusive to personal privacy – even more revealing than the content of our communications in some cases . . . ."); Sophie Stalla-Bourdillon, Evangelia Papadaki & Tim Chown, *Metadata, Traffic Data, Communications Data, Service Use Information. . . What Is the Difference? Does the Difference Matter? An Interdisciplinary View from the UK*, *in* DATA PROTECTION ON THE MOVE 437, 461 (Serge Gutwirth, Ronald Leenes & Paul De Hert eds., 2016) (arguing that application-level metadata should be protected in the same way as communications content); Vogel et al., *supra* note 169, at 515–16 (observing that "traffic data serve to paint an ever clearer picture of communication participants" and that "the access to mere traffic data (without even targeting communication content) is in and of itself viewed as a significant encroachment on the secrecy of telecommunication"). *But see* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1029 (2010) (arguing that the content/non-content distinction "reflect[s] an essential underlying dynamic of the switch from the physical world to the network environment" and should be confirmed in future decisions).

185. *See, e.g.*, Filippo Raffaele Dinacci, *Localizzazione attraverso celle telefoniche*, *in* LE INDAGINI ATIPICHE 369 (Adolfo Scalfati ed., 2014) (arguing that the Italian law, in allowing traffic data production on the basis of art. 256 C.p.c. (It.), is effectively unconstitutional, given that a mere authorization from the Public Prosecutor suffices and in light of the lack of any other legal safeguards); Maciej Rogalski, *Udostępnianie danych telekomunikacyjnych sądom i prokuraturom*, PROKURATURA I PRAWO, 2015, no. 12, at 68 (criticizing the Polish provisions for lack of subsidiarity requirements and for disproportionately affecting individuals who have no connection to the crime).

186. *See* Carpenter v. United States, 138 S. Ct. 2206, 2206 (2018) (requiring warrants for access to historical CSLI and ruling that the third-party doctrine does not apply to such data); U.S. v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.").

> them his familial, political, professional, religious, and sexual associations. These location records hold for many Americans the 'privacies of life.' And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.[187]

In finding a greater privacy intrusion that necessitated greater protection for location information (in relation to other forms of metadata), the *Carpenter* court specifically addressed how "the retrospective quality" of CSLI could provide the police with

> access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices [sic] of the wireless carriers, which currently maintain records for up to five years.[188]

Additionally, the Court repeatedly noted its assessment that CSLI granted law enforcement something akin to "perfect surveillance":[189]

> [B]ecause location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone. Unlike with the GPS device in *Jones,* police need not even know in advance whether they want to follow a particular individual, or when. Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.[190]

Even prior to *Carpenter*, other courts had compared CSLI to GPS and other forms of tracking. For example, in 2010, a district judge in the Southern District of Texas compared historical CSLI to GPS tracking.[191] Acknowledging differences in timing (CSLI being recorded historical data, GPS tracking involving prospective data) and initiative (the police being responsible for creating GPS data, but not for creating historical CSLI data), the Texas judge considered CSLI to be more invasive than GPS in that it could also monitor indoors (in contrast to GPS tracking of cars) and reveal more since the cell-phone is carried on the person.[192] As a result, and

---

187. *Carpenter*, 138 S. Ct. at 2217–18 (citations omitted).
188. *Id.* at 2218.
189. *Id.* at 2210.
190. *Id.* at 2218.
191. Jeremy H. Rothstein, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489, 505–06 (2012) (referring to *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827 (S.D. Tex. 2010)).
192. *Id.*

following *Maynard's* reasoning, the judge held that (even imprecise and intermittent) warrantless CSLI was unconstitutional.[193] Under state law (involving higher protection than the Fourth Amendment), the New Jersey Supreme Court observed, in 2013, that "[w]ith increasing accuracy, cell phones can now trace our daily movements and disclose not only where individuals are located at a point in time but also which shops, doctors, religious services, and political events they go to, and with whom they choose to associate."[194] Thus, "the cell site locations of telephone calls made and received may yield a treasure trove of very detailed and extensive information about the individual's 'comings and goings' in both public and private places."[195]

b. Future Data, or Real-Time Cell Phone Location Tracking

Most jurisdictions in our study not only allow police, through the collection of cell-phone location data, to acquire historical traffic data (i.e., data about movements in the past), but they also allow police to acquire future or real-time traffic data (i.e., data about future movements, usually under the same, or only slightly stricter, conditions). This turns a data production order into a power analogous to covert surveillance to track a person's movements, such as tailing or GPS tracking.

For instance, Dutch electronic communications providers can be ordered to produce incoming, future data for a period of up to three months, which have to be provided real-time.[196] (This applies, however, only to location data when the phone is used for an actual or attempted communication and not to location data generated when the phone is merely in stand-by mode.)[197] Similarly, the German provision on location-data production includes the situation that location data are provided in real time, in cases of serious crime and if it is necessary for the investigation,[198] and the Czech provision on traffic and location data requests by police can involve "remote and continuous access."[199]

While these countries treat real-time cell-phone location tracking under the general power for real-time provisioning of cell-phone metadata, Canada separates these explicitly.[200] Bill C-13 from 2014 removed "location" from the power to

193. *Id.*

194. State v. Earls, 70 A.3d 630, 632 (N.J. 2013) (quoted in Susan Freiwald, *Light in the Darkness: How the LEATPR Standards Guide Legislators in Regulating Law Enforcement Access to Cell Site Location Records*, 66 OKLA. L. REV. 877, 883 (2014)).

195. Commonwealth v. Augustine, 4 N.E.3d 846, 863 (Mass. 2014) (quoted in Freiwald, *supra* note 194, at 883–84).

196. Art. 126n ¶¶ 1–3 Sv (Neth.).

197. *Kamerstukken II* 2001/02, 28 059, No 3 at 8 (Neth.). Location data of phones in stand-by mode might be requested on the basis of art. 126ng Sv (Neth.), but this applies only to stored data, not to real-time provisioning of incoming location data.

198. STRAFPROZESSORDNUNG [StPO] [CODE OF CRIMINAL PROCEDURE] § 100g, para. 1 (Ger.) (translation at *The German Code of Criminal Procedure StPO*, *supra* note 183).

199. Zákon o Policii České republiky [Police Act], Zákon č. 273/2008 Sb., § 66(3) (Czech).

200. *See* Israel & Parsons, *supra* note 163, at 66.

obtain transmission data and explicitly prohibits its use as a tracking power;[201] instead, location data are included in the "more protective"[202] power to obtain tracking data.[203] A tracking warrant "may contain any conditions that the justice or judge considers appropriate, including conditions to protect a person's interests"[204]—a provision that the transmission data recording warrant lacks. A tracking warrant targeted at a specific individual, for "identifying the location of a thing that is usually carried or worn by the individual," applies a higher standard of proof[205] than the standard for transmission-data warrants or for tracking warrants targeted at transactions or things. A tracking warrant can be combined with an "assistance order"[206] designed to ensure, for example, that a telecommunications provider assist law enforcement in tracking a device, such as a cell-phone, by providing data or access to data required for such purposes.

In the United States, CSLI can also be ordered in real time—so-called "prospective CSLI,"[207] and the *Carpenter* court explicitly did not address real-time CSLI.[208] Some courts have held that prospective or real-time CSLI should be granted less liberally than historical CSLI, given that Congressional intent when passing the Stored Communications Act was more in line with historical data; other courts have held that the two should be treated identically.[209] In real-time CSLI cases, courts have also applied the reasoning from *Knotts* to determine that defendants did not have legitimate expectations of privacy in their location while they moved about in publicly accessible places, such as public highways,[210] or phone tracking has been justified under the authority of warrants or other court orders, and as such, has not been unreasonable.[211] On the other hand, a district judge

---

201. Criminal Code, R.S.C.1985, c. C-46, § 492.2(3) (Can.) ("No warrant shall be issued under this section for the purpose of obtaining tracking data.").

202. ISRAEL & PARSONS, *supra* note 163, at 68.

203. Criminal Code, R.S.C. 1985, ch. C-46, § 492.1 (Can.). See R. v. Grandison, 2016 BCSC 1712 (Can. B.C.) and surrounding text.

204. Criminal Code, R.S.C. 1985, ch. C-46, § 492.1(4) (Can.).

205. *See* Criminal Code, R.S.C. 1985, ch. C-46, § 492.1(1)–(2) (Can.); *Grandison*, 2016 BCSC at para. 34 and surrounding text.

206. Criminal Code, R.S.C. 1985, ch. C-46, § 487.02 (Can.).

207. Rothstein, *supra* note 191, at 494 (referring to *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 835–36 (S.D. Tex. 2010)).

208. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval).").

209. Rothstein, *supra* note 191, at 505.

210. *See, e.g.*, United States v. Forest, 355 F.3d 942 (6th Cir. 2004) (interception of cellular phone data revealed defendant's general location while traveling on public highways. The Court applied *Knotts*, finding "no legitimate expectation of privacy in the cell-site data because the DEA agents could have obtained the same information by following Garner's car").

211. *See, e.g.*, United States v. Luna-Santillanes, 554 F. App'x. 402 (6th Cir. 2014); *see also* United States v. Turner, 781 F.3d 374 (8th Cir. 2015) (finding that exclusion of evidence was not proper remedy for government's failure to comply with procedural requirements for preparing, executing, and returning a warrant for a tracking device, namely precise location information from defendant's cell phone).

offered interesting arguments to support the view that prospective CSLI, if conducted for a period of up to thirty days, is privacy-intrusive and not comparable to surveillance of movements in public. This is so, in the judge's view, because the police will not know in advance whether the target is in a constitutionally protected place, such as a home, and users tend to keep their cell-phones on (or close to) their persons.[212] And, unlike cars, "it is 'almost unimaginable' that a cell phone would remain entirely within public spaces."[213] The judge also argued that, for the purposes of arresting someone, continued tracking provides "different and arguably more" information than a place-based search, revealing intimate details of a person's life that entering someone's home need not reveal.[214] In the end, however, the reasoning in *Carpenter* and *Jones* seems to imply that the acquisition of CSLI (in any form, historical or future) would need to be supported by a warrant because it intrudes on reasonable expectations of privacy[215]—although, presumably, it may depend on the period over which future or real-time CSLI would be collected before it equals the broad historical "encyclopedia" of information at issue in *Carpenter*.

In contrast to the countries that allow prospective cell-phone location tracking, Poland does not seem to have a provision providing a possibility for real-time collection of traffic data.[216]

2. Stealth SMS and GPS Ping

The usefulness of a production order of cell-phone traffic data to track someone's movements (or rather, their phone's movements) is dependent on the number of times the phone is actually used. After all, telecom providers usually only store traffic data of actual communications (or communication attempts), and location data of phones in stand-by mode may not be possible to collect in real time from providers, at least in the Netherlands[217] and possibly in the United States.[218] (However, this may differ for other types of service providers, such as producers of applications installed on a user's smartphone, which might collect location data

212. *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526 (D. Md. 2011) [hereinafter *Specified Wireless Tel.*] (citing a study that 65 percent of U.S. adults have slept with their phone nearby), *discussed in* Rothstein, *supra* note 191, at 518.

213. Rothstein, *supra* note 191, at 519 (citing *Specified Wireless Tel.*, *supra* note 212, at 543).

214. *Id.* at 519–20 (citing *Specified Wireless Tel.*, *supra* note 212, at 550).

215. For instance, in *Carpenter v. United States.*, 138 S. Ct. 2206, 2217 (2018), the court held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI" does not seem to be, on its face, limited to historical CSLI.

216. ANDRZEJ ADAMSKI, CYBERCRIME LEGISLATION IN POLAND 39 (2015), https://www.researchgate.net/publication/279191115_CYBERCRIME_LEGISLATION_IN_POLAND [https://perma.cc/KM6F-4TYE].

217. *Kamerstukken II*, *supra* note 197.

218. Rothstein, *supra* note 191, at 504 (citing a minority of courts that held that federal statute allowed CLSI acquisition only when the target made and received calls).

more continuously and when devices are not being used.)[219] To ensure that sufficient location data are generated to be able to track a cell-phone's movements with considerable precision, police have employed a method referred to as "stealth SMS" or "silent SMS" (SMS, or short messaging service, being the original technology used for texting).[220] These stealthy text messages remain hidden from the mobile phone's user but do generate traffic data (since an actual communication, albeit covert, occurs).[221]

Police use of stealth SMS has been discussed in Germany and the Netherlands, and to some extent in the United States; presumably, police in other countries may also be using this method, but it has, to our knowledge, not yet been tested in Supreme Court cases or discussed in mainstream literature in the other jurisdictions in our study. In Germany, it is used very frequently: several federal law-enforcement agencies sent over 150,000 silent SMS messages in the first half of 2014 alone.[222] The statutory basis for it has "not yet been conclusively settled." However, the discussion revolves around the question of whether, or to what extent, sections 100a *et seq.* of the German Criminal Code, possibly in combination with the general investigative clauses in section 163(1) and section 161(1), "can be used beyond their respective wording for not only passively accessing data generated independent of investigation authorities, but also for actively inducing such a generation of data."[223] Some authors argue that silent SMS can be based on section 100h(1)(2), which allows special technical devices for observation purposes to be used against suspects (or against others if there are grounds to believe they have contacts with the suspect and the measure will lead to establishing the suspect's location), for crimes of substantial significance, and "silent SMS" can be interpreted as such a special technical observation device.[224]

In the Netherlands, the use of stealth SMS to locate a suspect is also "frequently" used.[225] It has been accepted on the basis of Article 3 of the Police Act of 2012—the general task description of the police, on which minor privacy

219. *See e.g.*, Keith Collins, *Google Collects Android Users' Locations Even When Location Services Are Disabled*, QUARTZ (Nov. 21, 2017), https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/ [https://perma.cc/G8QC-7CQA].

220. *See Text Messaging*, WIKIPEDIA, https://en.wikipedia.org/wiki/Text_messaging [https://perma.cc/V6Y8-LQSH] (last visited Feb. 3, 2019); *SMS*, WIKIPEDIA, https://en.wikipedia.org/wiki/SMS [https://perma.cc/4TTN-YNA6] (last visited Feb. 3, 2019).

221. *See* Vogel et al., *supra* note 169, at 550–51.

222. *Id.* at 551 (referring to DEUTSCHER BUNDESTAG: DRUCKSACHEN [BT] 18/2257, 9 (Ger.)).

223. *Id.* at 551; Ulrich Eisenberg & Tobias Singelnstein, *Zur Unzulässigkeit der heimlichen Ortung per „stiller SMS"*, 25 NSTZ NEUE ZEITSCHRIFT FÜR STRAFRECHT 62 (2005) (observing that generation of the data is the core feature of the measure of silent SMS, as this enables creating a precise movement profile independent from the user's behavior, and arguing that the measure for this reason is intrusive and lacks the required specific legal basis).

224. Sigrid Hegmann, *StPO § 100h Weitere Maßnahmen außerhalb von Wohnraum*, *in* BECKOK STPO WITH RISTBV AND MISTRA, para. 6 (Jürgen Peter Graf et al. eds., 30th ed. 2018) (Ger.).

225. G. ODINOT ET AL., HET GEBRUIK VAN DE TELEFOON- EN INTERNETTAP IN DE OPSPORING 131 (2012).

intrusions can be based without a specific statutory basis in the Code of Criminal Procedure.[226] The Supreme Court has deemed stealth SMS to involve a minor privacy intrusion.[227] The circumstances of the case are relevant, however, given that the Court argued that the duration and frequency (ninety messages in five days) were such as to create only a limited image of the phone user's movements. Additionally, the court stated, there was authorization from the public prosecutor and an order for systematic observation and communications interception had already been given to enable other investigation methods. And, despite flaws in reporting, sufficient clarity had been acquired about how the method had been used.[228] In other situations—for instance, if used for a longer period or with very high frequency—use of stealth SMS is likely to be deemed to constitute more than only a minor privacy intrusion, given that someone's movements recorded over a longer period of time or with very high frequency are likely to result in a more or less complete image of certain aspects of someone's private life.[229] Therefore, in these circumstances, the public prosecutor would be required to authorize an order for systematic observation (Article 126g of the Dutch Criminal Code) or, in the proposed new Code, an order for systematic determination of location.[230]

In the United States, a slightly different form is discussed in the literature, in which law enforcement obtains a court order to have a service provider "ping" a cellular phone at particular times or intervals that enables the provider to calculate the phone's location based on its GPS coordinates, which are more precise than ordinary cell-site information.[231] In multiple cases, the Sixth Circuit has held that pinging GPS coordinates of a phone is not a Fourth Amendment search since it does not constitute a trespass or invade a reasonable expectation of privacy.[232] Importantly, this reasoning has emerged from cases where the tracking was for a relatively short period of time (less than that at issue in *Jones*). In such cases, the third-party doctrine would also not seem to apply, since the data are generated at law enforcement's initiative and not voluntarily transmitted by the user.[233]

---

226. M.J. Borgers, *Normering van 'lichte' opsporingshandelingen*, 15 DELIKT & DELINKWENT 143, 143 (2015).

227. HR 1 juli 2014, ECLI:NL:HR:2014:1569 (Neth.).

228. *Id.* See Borgers, *supra* note 226, for an extensive discussion.

229. *Cf.* Hof 's-Hertogenbosch 20 juni 2013, ECLI:NL:GHSHE:2013:2579 § I(D.2) (Neth.).

230. Proposed art. 2.8.2.10.1, *Concept Wetsvoorstel Boek 2* (Neth.), *supra* note 48; *see also Memorie van Toelichting* 23–24 (Feb. 2017), https://www.rijksoverheid.nl/documenten/kamerstukken/2017/02/07/memorie-van-toelichting-vaststellingswet-boek-2-van-het-nieuwe-wetboek-van-strafvordering-het-opsporingsonderzoek [https://perma.cc/7G3V-PUAA] (Neth.).

231. Rothstein, *supra* note 193, at 495.

232. *See, e.g.*, United States v. Skinner, 690 F.3d 772 (6th Cir. 2012); United States v. Forest, 355 F.3d 942 (6th Cir. 2004).

233. Rothstein, *supra* note 193, at 510 (referring to United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004), *cert. granted, judgment vacated on other grounds sub nom.* Garner v. United States, 543 U.S. 1050 (2005), which determined that the third-party doctrine does not apply if police dial the subject's cell phone to generate CSLI).

3. IMSI Catchers (Stingrays)

An International Mobile Subscriber Identity (IMSI) catcher (sometimes also called a Stingray) is a cell-site simulator, that is, a device that resembles a cell-phone base station and attracts the traffic of mobile phones in its vicinity.[234] It is usually used to acquire someone's unknown telephone number (or IMSI number) by operating the IMSI catcher in the vicinity of the target so that the target's phone makes contact with the simulator (if done at a few different places, this will usually enable uniquely identifying the target's number). However, an IMSI catcher can also be used to locate a suspect's phone if the number is already known. For instance, U.S. police used an IMSI catcher in *United States v. Rigmaiden*[235] (a fraud case) to trace a prepaid data card connected to a laptop, of which they only had an IP address; the telecom provider had been able to locate the data card within a quarter-square-mile area, but could provide no more precise location, and the IMSI catcher was used to track the card exactly to the suspect's apartment.[236]

Police use of IMSI catchers is specifically regulated in Germany and the Netherlands. Germany enables both functionalities of identifying an unknown number[237] and establishing the location of a mobile device.[238] The measure requires a warrant[239] and an offense of substantial significance,[240] and it can be ordered for at most six months (which can be prolonged repeatedly with six-month periods).[241] Data of third persons can only be collected if it is technically inevitable; these can only be used for data mining to retrieve the sought-after number and must be deleted immediately afterward.[242]

In the Netherlands, Article 126nb of the Dutch Criminal Code regulates use of an IMSI catcher, but this is limited to the purpose of acquiring identification information; Article 126nb cannot be used to collect location or other metadata. An IMSI catcher may nevertheless also be used as a tracking device, to determine where the phone user is located. The Supreme Court has allowed this in a specific case on the basis of Article 3 of the Police Act of 2012 (the general provision allowing minor privacy intrusions, without specific safeguards), in light of the short duration of its use in the present case and the authorization of the public prosecutor, and the fact that it only revealed the phone's (user's) location, but not what the user does or

234. *See IMSI-catcher*, WIKIPEDIA, https://en.wikipedia.org/wiki/IMSI-catcher [https://perma.cc/AK74-8AQ5] (last visited Feb. 3, 2019).

235. United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012).

236. Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1, 29–30 (2014).

237. STRAFPROZESSORDNUNG [STPO] [CODE OF CRIMINAL PROCEDURE] § 100i(1)(1) (Ger.).

238. *Id.* § 100i(1)(2).

239. *Id.* §§ 100i(3), 100b(1).

240. *Id.* § 100i(1).

241. *Id.* § 100i(3).

242. *Id.* § 100i(2).

says.[243] It added, however, that, in general, if the duration, intensity, and frequency are such as to enable acquiring a more or less complete image of a part of someone's private life, IMSI catcher localization cannot be based on Article 3 of the Police Act of 2012 and requires a specific statutory basis;[244] this could be systematic observation (Article 126g of the Dutch Criminal Code) or, in the proposed new Code, an order for systematic determination of location,[245] both of which require an authorization from the public prosecutor, but not a warrant.

In other countries, IMSI catchers are also used, but the legal status is somewhat less clear. In Czechia, IMSI catchers (nicknamed "Agáta") seem to be used by police, but we have not found any legal discussion of this. We assume the measure can be based on section 158d(2) of the Czech Code of Criminal Procedure (observation), which allows covert obtaining of information about persons and objects by technical means.[246] While this is the same type of measure as the German provision, it requires authorization from a public prosecutor, not a judge.[247]

In the United States, cases challenging the use of these devices are as yet relatively scarce. Although law enforcement has argued since 2001 that an IMSI catcher can be based on pen register or trap and trace orders (to record traffic data),[248] several judges have denied applications because the pen/trap statute does not see to recording traffic data from *unidentified* devices.[249] In *United States v. Patrick*,[250] the Seventh Circuit held that the warrantless use of an IMSI catcher to locate a suspect with an outstanding warrant did not require exclusion of evidence when it was used to locate the suspect in a public space.[251] However, the court explicitly avoided a full analysis of whether the use of the simulator was itself a search for Fourth Amendment purposes, leaving that analysis for future cases.[252] In another more recent Seventh Circuit case, *United States v. Sanchez-Jara*,[253] Judge Easterbrook held that an IMSI catcher could be effectively authorized by a warrant under section 2703(d) of the Stored Communications Act (when issued upon a finding of probable cause), but only insofar as the device used would not capture "information that would require a wiretap warrant" under 18

243. HR 1 juli 2014, ECLI:NL:HR:2014:1562 (Neth.). The exact duration is not mentioned in the judgement, but was at most three days (the IMSI catcher was used on April 26, 2010 to narrow down the geographic location of the phone, and the suspect was arrested on April 28).

244. *Id.*

245. *Concept Wetsvoorstel Boek 2* (Neth.), *supra* note 48 (proposed Art. 2.8.2.10.1).

246. Trestní řád [Criminal Procedure Code], Zákon č. 141/1961 Sb., § 158d(1)–(2) (Czech).

247. *Id.* § 158d(2).

248. Pell & Soghoian, *supra* note 236, at 27.

249. *Id.* at 21 (referring to *In re* Application of United States for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. 197, 200 (C.D. Cal. 1995)); *id.* at 29 (referring to *In re* Application of United States for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747,751 (S.D. Tex. 2012)).

250. United States v. Patrick, 842 F.3d 542 (7th Cir. 2016).

251. *Id.* at 545.

252. *Id.*

253. United States v. Sanchez-Jara, 889 F.3d 418 (7th Cir. 2018).

U.S.C. sections 2510–2522 (such as the contents of communications).[254] In *Rigmaiden* (a district court decision), the government acknowledged that an IMSI catcher's use to locate a data card constituted a Fourth Amendment search and had in fact obtained a search warrant pursuant to Rule 41(b).[255] Relevant in this case is that the card turned out to be inside a residence, a possibility that law enforcement had foreseen—as a prosecutor stated in a hearing:

> It's not the nature of the data; it's the nature of the interest. And the—the nature of the—the legal interests, the Fourth Amendment—you know, where you have an expectation of privacy is where we would recommend using the search warrant as opposed to just a pen register order.[256]

Indeed, as Pell and Soghoian observe, use of IMSI catchers in many cases "necessarily involves sending signals through the walls of homes and apartment buildings or penetrating briefcases, purses, and pockets in order to identify the phones contained within."[257] In that light, it makes sense that the policy guidance adopted by the U.S. Department of Justice in 2015 on IMSI catchers states that, as a matter of policy, law enforcement must (except in emergencies or exceptional circumstances) obtain a search warrant supported by probable cause and issued pursuant to Rule 41 (along with pen/register authorization).[258] Although the policy states that cases of exceptional circumstances that make obtaining a search warrant impracticable are expected "to be very limited," and agents still need approval from the agency's executive-level personnel, the relevant U.S. Attorney, and a Criminal Division DAAG,[259] the "questionably broad definition of exceptional situations" has been called a "central weakness" in the policy.[260]

The situation in Canada is less clear, although Canadian agencies are apparently using IMSI catchers.[261] According to Israel and Parsons, the Criminal Code contains "a patchwork of overlapping electronic surveillance powers that could potentially apply to IMSI Catcher use, each with varying levels of safeguards."[262] They argue that the use of IMSI catchers is most similar to individual-targeted tracking and should therefore comply with "Individual

---

254. *Id.* at 421 ("Given the district judge's finding of probable cause—a finding that carries a strong presumption of correctness this warrant suffices to support use of a cell-site simulator that does not gather information that would require a wiretap warrant.") (internal citations omitted).

255. Pell and Soghoian, *supra* note 236, at 30 (referring to United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *14 (D. Ariz. May 8, 2013)).

256. *Id.* at 31 (quoting Reporter's Transcript of Proceedings: Motion Hearing at 61, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC)).

257. *Id.* at 32.

258. U.S. DEP'T OF JUSTICE, DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY 3 (2015), http://www.justice.gov/opa/file/767321/download [https://perma.cc/A7YD-RKHU].

259. *Id.* at 4.

260. Israel & Parsons, *supra* note 163, at 54.

261. *Id.* at 57.

262. *Id.*

Tracking" warrants, "[g]iven the capacity of IMSI Catcher-obtained data to reveal the movements of individuals, now and in the future . . . ."[263]

D. Automated License Plate Recognition (ALPR)

Automated license/number plate recognition (ALPR) is used in many countries to scan license plates of cars on public roads, often on a large scale with static cameras or mobile cameras. Images can be retained in a database for a certain period, to enable data mining and *ex post* searches, or recognition can take place in real-time based on a hit list of sought-after license plates without images being necessarily stored.[264] ALPR is used for a wide range of law enforcement and other government purposes; we discuss here only briefly its use in criminal investigation.

In Germany, ALPR can be used to locate an accused during police checks on the basis of section 163e of the German Criminal Code (police observation), in cases of offenses of substantial significance and where other means of establishing the facts or determining the perpetrator's whereabouts would offer much less prospect of success or be much more difficult.[265] It can be used against other persons only if it can be assumed that they are linked to the perpetrator, that the measure will lead to determination of the perpetrator's whereabouts, and that using other means would offer much less prospect of success or be much more difficult.[266] Additional plates can be included in the observation if the car is registered to or used by the accused or by a thus far not identified person who is suspected of a crime of substantial significance.[267] The use of ALPR under section 163e requires authorization from a judge.[268]

In contrast to Germany, ALPR does not fall under the Dutch power of systematic observation, as it does not involve systematic *following* of a person. ALPR might be based on Article 3 of the Police Act of 2012 if the police are looking for particular cars with known license plate numbers from a reference database, which are automatically matched with the plate numbers of cars passing by, and the photograph and plate number of an observed car is recorded only if a match is found.[269] The general use of ALPR cameras on highways to record passing traffic

---

263. *Id.* at 69–70; *cf.* the argumentation in Elizabeth E. Joh, *The Undue Influence of Surveillance Technology Companies on Policing*, 92 N.Y.U. L. REV. ONLINE 101, 109–10 (2017) (observing that "the use of a device to force a person's cellphone to provide the police with precise locational data—in some cases within two meters of the cellphone—echoes similar legal debates about whether the Fourth Amendment governs the government's collection of vast amounts of locational data, even in public spaces," with reference to the concurring opinions in *Jones*).

264. Roger Clarke, The Covert Implementation of Mass Vehicle Surveillance in Australia (Mar. 19, 2009) (unpublished manuscript), http://www.rogerclarke.com/DV/ANPR-Surv.html [https://perma.cc/FE5D-6CZA] (distinguishing two ANPR architectures: the "mass surveillance" and "blacklist-in-camera" approaches).

265. STRAFPROZESSORDNUNG [STPO] [CODE OF CRIMINAL PROCEDURE] § 163e(1) (Ger.).

266. *Id.* § 163e(1); *see also* Urs Kindhäuser, STRAFPROZESSRECHT § 8, Rn. 18–19 (4th ed. 2016).

267. STRAFPROZESSORDNUNG [STPO] [CODE OF CRIMINAL PROCEDURE] § 163e(2) (Ger.).

268. *Id.* § 163e(4).

269. CORSTENS & BORGERS, *supra* note 47, at 333.

is not allowed for criminal investigation purposes; it has been used in the past by several police units, with recordings being stored for weeks or months, but the Data Protection Authority determined that this lacked a legal basis.[270] A bill is now pending in the Senate to allow large-scale ALPR registration, with a storage period of four weeks.[271] Investigation officers would be able to consult the ALPR database in cases that involve investigations of relatively serious crimes (generally those carrying a maximum imprisonment of at least four years) or in cases of fugitive suspects (this requires an order from the public prosecutor).[272] In terms of privacy safeguards, Article 5 of the proposed Order in Council to further regulate ALPR is interesting: it stipulates that only public places can be monitored and that measures must be taken to prevent images of car users being consulted; thus, "ANPR cameras must be focused and fine-tuned in such a way as to prevent as much as possible the recognizable presence of non-public places or persons on the photos of the vehicle."[273] Since such recording could nevertheless happen, the officer accessing the database should remove the photo or make the place or person unrecognizable before giving it to the requesting officer.[274]

The possibilities for accessing the central ALPR database are considerably broader in the U.K. Records can be kept up to two years and consulted up to 90 days after their creation for ordinary crimes—up to one year for "serious investigations" (such as blackmail, perverting justice, or rape) or "major investigations" (such as murder or kidnapping).[275] For major investigations, records can also be requested after one year with written authority of an inspector.[276] In Canada, ALPR data fall under the definition of "personal information" for purposes of federal and provincial privacy acts but is generally not subject to the Canadian Charter's prohibitions on unreasonable searches.[277] Specifically, the British Columbia Privacy Commissioner has held that the retention (but not the initial

270. College Bescherming Persoonsgegevens, Onderzoek naar de verwerking van no-hits bij de inzet van Automatic Number Plate Recognition Regionaal politiekorps IJsselland (Jan. 2010); College Bescherming Persoonsgegevens, Onderzoek naar de verwerking van no-hits bij de inzet van Automatic Number Plate Recognition Regionaal politiekorps Rotterdam-Rijnmond (Jan. 2010).

271. *Kamerstukken I* 2016/17, 33 542, No. A (Neth.).

272. *Id.* (proposed Art. 126jj SV).

273. Art. 5(3) Besluit inzake het vastleggen en bewaren van kentekengegevens van het Wetboek van Strafvordering door de politie (draft), *Kamerstukken I* 2016/17, 33 542, appendix to No. C (Neth.).

274. *Id.* at Art. 5(4).

275. *See* HOME OFFICE, NATIONAL ANPR STANDARDS FOR POLICING. PART 3 – DATA ACCESS AND MANAGEMENT STANDARDS art. 5–6, apps. B–C (2016), http://www.npcc.police.uk/RMH/Part3.pdf [https://web.archive.org/web/20171222105413/http://www.npcc.police.uk/RMH/Part3.pdf].

276. *Id.*

277. *See* Bryce Clayton Newell, *Local Law Enforcement Jumps on The Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, And Access to Government Information*, 66 ME. L. REV. 397, 411 (2014). *But see* INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO (ICPO), GUIDANCE ON THE USE OF AUTOMATED LICENCE PLATE RECOGNITION SYSTEMS BY POLICE SERVICES (2017), https://www.ipc.on.ca/wp-content/uploads/2016/09/alpr_systems.pdf [https://perma.cc/3URE-UR8Z] (urging police services to ensure that their ANPR programs respect Charter-protected privacy rights).

collection) of certain obsolete and "non-hit" information violated provincial privacy law.[278] In the United States, a number of states have regulated the use of ALPR, but there is no applicable federal law (including the Fourth Amendment, as long as the scanning happens in publicly accessible places where persons are deemed to not have a reasonable expectation of privacy) to regulate such surveillance more broadly or consistently across the country.[279]

E. Other Forms of Location Tracking

While (technology-enhanced) human observation, GPS tracking, cell-phone tracking, and ALPR are the most widely used forms of location tracking by police in the jurisdictions we studied, law enforcement can and do use a wide variety of other forms of tracking. In this section, we highlight some interesting alternative tracking methods we encountered in our research, typically in the context of a particular jurisdiction. The description here is not comparative. Rather, it is illustrative, designed to show how specific jurisdictions incorporate new or alternative tracking methods in their legal system.

Cars and cell-phones leave traces of people's movements, but electronic transactions in banks, ATMs, and shops can also provide insight into someone's whereabouts. The Canadian Criminal Code explicitly includes such data in the regulation of tracking production orders;[280] section 487.017 allows the police to make *ex parte* applications for court orders requiring third parties to produce documents containing tracking data, defined as "data that relates to the location of a *transaction*, individual or thing."[281] Similarly, based on the Czech Police Act, police can, without authorization, request data about time and place of used electronic payment methods from banks or data about place and time of provided health services from health insurance companies and healthcare providers, but only to search for missing or searched persons, not for evidence-gathering in general.[282] Although location data are not explicitly mentioned, they may also fall under the data that can be ordered from service providers in other jurisdictions; for instance, Dutch police can, with authorization from the Public Prosecutor and for relatively serious crimes, order production of any data from someone likely to store it,[283] which will include transaction data. If ordered data are likely to include "sensitive" data (i.e., on religion, race, health, political views, sex life, or trade-union

278. Newell, *supra* note 277, at 411 (citing Elizabeth Denham, Office of Info. & Privacy Comm'r of B.C., *Investigation Report F12-04: Use of Automated Licence Plate Recognition Technology by the Victoria Police Department* 10–11 (Nov. 15, 2012), http://www.oipc.bc.ca/investigation-reports/1480 [https://perma.cc/597B-H2LB]); *see also* ICPO, *supra* note 277, at 9 (similar finding under Ontario's privacy act).

279. For a discussion and analysis of these state laws (current as of 2014), see Newell, *supra* note 277, at 404–10.

280. *See supra* notes 20–24 and accompanying text.

281. Criminal Code, R.S.C. 1985, c C-46, § 487.011 (Can.) (emphasis added).

282. Zákon o Policii [Police Act], Zákon č. 273/2008 Sb., § 68 (Czech).

283. Art. 126nd SV (Neth.).

membership), the police must obtain a warrant and the offense being investigated must be a particularly serious crime.[284]

Another way to trace a known suspect whose whereabouts are unknown is the classic method of publishing their description or picture in the hope that someone recognizes them and asking the public to inform the police accordingly. This is explicitly regulated in Germany, where section 131a of the German Code of Criminal Procedure (Notice to Determine Whereabouts) allows notices to be published in newspapers or otherwise broadcasted, in cases involving an offense of substantial significance and a high level of suspicion (*dringend verdächtig*). This measure can be used if other measures to determine the whereabouts are considerably less likely to succeed.[285] The published notice may include pictures.[286] Such notices can also be used to trace witnesses, but the notice has to make clear that the sought person is not the accused. Furthermore, witness pictures can only be published if alternative tracking methods are hopeless or substantially more difficult and there is an absence of preponderant protection-worthy interests of the witness.[287] Pictures can also be published on the basis of section 131b of the Code of Criminal Procedure, particularly in cases where the suspects' or witnesses' identities are unknown, under generally similar conditions.[288]

A more recently developed method is the use of directional Wi-Fi tracking antennas and associated software to trace unknown users of an unprotected Wi-Fi network. In the United States, defendants in a growing number of (primarily) district court decisions have challenged the investigatory use of this method.[289] Generally, police have used these technologies to identify locations where child pornography or other illicit material is being downloaded via Wi-Fi routers. In *United States v. Stanley*,[290] police knew child pornography was being shared from a particular IP address, but a warrant-based search of the home associated with the IP address was unsuccessful (because the suspect was "piggybacking" on an open Wi-Fi network).[291] With the consent of the homeowner, police used MoocherHunter software, which measures the distance between the router and the computer connecting to it, and by moving the antenna of the wireless router, police could trace the computer to a specific apartment.[292] According to the court, this did not constitute a Fourth Amendment search since the defendant "did not have a reasonable expectation of privacy in the wireless signal he caused to emanate from

284. Art. 126nf SV (Neth.).
285. STRAFPROZESSORDNUNG [STPO] [CODE OF CRIMINAL PROCEDURE] § 131a(3) (Ger.).
286. *Id.* §§ 131(4), 131a(4).
287. *Id.* § 131a(4).
288. *Id.* § 131b.
289. *See, e.g.,* United States v. Stanley, 753 F.3d 114 (3d Cir. 2014).
290. *Id.*
291. *Id.* at 117.
292. *Id.* at 116–17.

his computer."[293] Although the defendant invoked *Kyllo*, arguing that the software was not in general public use and was used to discover his computer inside his home, the court distinguished Wi-Fi tracking from thermal imaging because, in contrast to *Kyllo* who did not send the heat to a third party and tried to contain it in his garage, Stanley had "voluntarily caused a signal to be sent directly to [the] wireless router" of a neighbor and therewith "voluntarily conveyed [the signal] to a third party."[294] Besides using directional antennas to physically locate the source of Wi-Fi transmissions, police have frequently located computers based on IP addresses.[295]

Similarly sophisticated but more physical in character, Dutch police have applied the so-called "flock fiber method" (*flockvezelmethode*) to investigate a large number of burglaries in remotely located houses and farms.[296] This involved spraying the seats in a suspect's car with a specially developed microfiber spray (similar to what is called "synthetic DNA" spray)[297] and a fluorescent substance; the fibers attach themselves to the clothes of those sitting in the seats. If these fibers (which are uniquely identifiable) are found at a crime-scene, this provides evidence of a link between the car owner and the crime.[298] The method was not comprehensively tested in court, due to legal-technical issues; the Court of Appeal found that the method did not infringe the right to a fair trial to such an extent that the public prosecutor should be declared inadmissible in prosecuting the case, and the Supreme Court agreed.[299] The advocate general, in his advice to the Supreme Court, offered an interesting reflection on this method. He argued that privacy was not as such an issue here, given that the spray did not establish a complete trail of movements, but only linked the suspect with the location of the crime scene, "which is not a space where the burglar can reasonably be himself uninhibitedly."[300] Rather, the seriousness of the method consisted, according to the advocate general, in the intrusiveness of breaking into the car to apply the spray, which was questionable in light of Article 3 of the Police Act of 2012 (which only allows minor privacy intrusions) and in causing the suspect to be the carrier of artificial traces, which was problematic in light of the regulation of systematic observation (which prohibits putting a tracking device on a person[301]).[302]

---

293. United States v. Stanley, No. CRIM. 11-272, 2012 WL 55129987, at *12 (W.D. Pa. Nov. 14, 2012).

294. *Id.* at *16–17.

295. *See, e.g.*, United States v. Reynolds, 626 F. App'x 610 (6th Cir. 2015).

296. Conclusie A-G Aben 12 maart 2013, ECLI:NL:PHR:2013:229, § 3.2 (Neth.).

297. *See, e.g.*, Francisca Grommé, *Provocation: Technology, Resistance and Surveillance in Public Space*, 34 ENV'T & PLANNING D: SOC. & SPACE 1007 (2016) (discussing the introduction of a marker spray in Dutch urban public transport to conceptualize the role of technology in everyday resistances against surveillance).

298. Conclusie A-G Aben 12 maart 2013, ECLI:NL:PHR:2013:229, § 3.2 (Neth.).

299. HR 3 mei 2013, ECLI:NL:HR:2013:462 (Neth.).

300. Conclusie A-G Aben 12 maart 2013, ECLI:NL:PHR:2013:229, § 4 (Neth.).

301. *See supra* note 154 and accompanying text.

302. Conclusie A-G Aben 12 maart 2013, ECLI:NL:PHR:2013:229, § 4 (Neth.).

III. ANALYSIS AND DISCUSSION

As the previous section's overview has shown, law enforcement agencies use various methods of location tracking, often on the basis of different statutory powers or conditioned by different legal-protection regimes. In this section, we analyze whether patterns can be discerned in the ways in which the countries we studied deal with the privacy implications associated with these manifold tracking methods. The analysis proceeds from two perspectives. First, we discuss the factors that courts or lawmakers use to assess the intrusiveness of a particular tracking method or case, which should give some insight into how privacy is protected in this context. Second, we discuss how privacy is framed in the argumentation, which reveals the underlying conceptualizations of privacy that seem to inform courts' and lawmakers' assessment of tracking's intrusiveness. This offers insight into the nature of the privacy interest(s) at issue in police tracking. Together, these perspectives provide insight into how privacy is protected in the context of police tracking and how boundaries between lesser and more serious privacy intrusions are drawn.

A. Which Factors Influence the Seriousness of Privacy Infringements?

A useful starting point for discussing factors used in assessing how seriously some form of location tracing interferes with privacy is the list of factors emerging from the Dutch conceptualization of "systematicness."[303] Most of these factors also turn up in several other jurisdictions, which also apply some additional factors. Overall, then, we can discern eight relevant factors. As in Dutch law,[304] none of these will constitute a necessary or a sufficient condition on its own in any of our jurisdictions: generally, a combination of factors will be decisive.

1. Use of a Technical Device

Courts and lawmakers often recognize that technological affordances matter, especially since technology-facilitated surveillance will often have greater impact than mere human perception-based surveillance. Nevertheless, use of a technical device in itself is not necessarily determinative. In the German *Uzun* judgment, the court observed that section 163f of the Criminal Code on "longer observation" only contains an element of duration, and hence applies to all "longer" forms of observation regardless of whether they are executed with a technical device.[305] And the Dutch lawmaker takes a nuanced approach:

> In observation, technical devices reinforce and support human functions. From that perspective, observation with technical devices is not a separate category [from human observation]. (. . .) The turning point is not whether or not a technical device is used, but the intensity of the observation. Still, observation with a device that is a little more sophisticated than

303. *See supra* notes 102–09 and accompanying text.
304. Blom, *supra* note 102, comment 4(d)–(e).
305. BGH Jan. 24 2001, 3 StR 324/00 (Ger.).

> common-or-garden binoculars, will in practice soon have sufficient intensity or frequency to be systematic.[306]

Thus, the main factor is not technology use as such, but whether a technical device merely enhances or facilitates what humans can perceive anyway (or goes beyond that). Ordinary devices that merely enhance human senses, such as binoculars, do not in themselves, in Dutch law, lead to "systematic" observation, but stronger forms of human-sense enhancement, such as using a telescope, may result in it.[307] The Polish District Court in *Suwałki* observed that a GPS tracker facilitated a much larger and more precise insight into someone's movements than is possible with direct human observation,[308] much like the concurring opinions of Justices Sotomayor and Alito of the U.S. Supreme Court in *Jones*. However, courts may also argue that technology-based tracking does not go significantly beyond human perception, as had several U.S. decisions decided prior to *Jones* and *Carpenter*. For example, in *Knotts*, the U.S. Supreme Court held that the use of a beeper merely augmented the visual surveillance capabilities that police could generally use. As such, it did not alter the Court's conclusion that surveillance on public roads and in "open fields" did not attract Fourth Amendment protections because the suspects voluntarily exposed their movements in such places to third parties. And "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[309] In a similar vein, the Sixth Circuit in *United States v. Forest*[310] observed that there was "no legitimate expectation of privacy in the cell-site data because the DEA agents could have obtained the same information by following Garner's car."[311] Altogether, the assessment of location tracking's intrusiveness seems to require a fine-grained analysis of the particular affordances of technical devices at issue and nuanced argumentation regarding how it compares to human observation. Beepers give less comprehensive insight in movement patterns than GPS trackers and, similarly, telescopes are more intrusive than binoculars. There is, apparently, a fine line between devices that merely strengthen but do not really alter the possibilities of human perception, and those that augment human perception to the extent that they do make a qualitative difference. And this fine line between mere perception-strengthening and qualitative enhancement may also shift over time.[312]

Another aspect of technology that makes a qualitative difference is recording. While Czech law does not distinguish between human and technical tracking as

---

306. *Kamerstukken II* 1996/97, 25 403, No. 3 at 70 (Neth.).

307. Blom, *supra* note 102, comment 4(e).

308. *See supra* note 136 and accompanying text.

309. United States v. Knotts, 460 U.S. 276, 282 (1983).

310. United States v. Forest, 355 F.3d 942 (6th Cir. 2004), *vacated*, 543 U.S. 1100 (2005).

311. *Id.* at 951.

312. *Cf.* Uzun v. Germany, 2010-VI Eur. Ct. H.R. 1, 21 (holding that surveillance law must be "particularly precise, especially as the technology available for use is continually becoming more sophisticated").

such, written approval of the prosecutor is required as soon as recordings are made of what is being observed.[313] In Dutch law, any recording of the observed will make the observation "systematic," even during a short period, as this facilitates exact and complete reproduction of the observed at any later moment, which is not possible with human senses. The only exception to this general rule is taking a few photographs, which is considered non-systematic.[314] And, in Canadian law, it appears that the long-term *retention* of ALPR scan data enabled by recording capabilities crosses the relevant threshold for legality. Polish law seems to be an outlier in this respect, as it does not consider recording to be a relevant factor as such.[315]

2. Place

The place(s) where someone's movements are tracked is a second important factor. It often matters whether location tracking concerns movements in public places or (also) in private places, such as homes. Tracking in public is often considered to only constitute a minor interference with privacy as such,[316] while tracking in private places is often considered intrinsically intrusive.[317] Certain other factors can alter this assessment, such as sophisticated technology use[318] and intensity,[319] but not always easily so. Duration, for example, often seems less important than place. In Dutch law, for instance, a lengthy observation of someone in places where his behavior could be observed by anyone will not result in the person feeling limited in his right to undisturbed privacy,[320] but a short observation with a device in an intimate place, such as a brothel, is already considered systematic.[321] In the United States, this distinction was recognized (but not applicable) in *Knotts*, and it was dispositive in *United States v. Karo*, where police tracked cans of ether into the suspects' homes using a beeper, violating the Fourth Amendment.[322] Thus, the publicness of a place is a major factor in the reasonable expectation of privacy analysis in the United States.

313. *See* Trestní řád [Criminal Procedure Code], Zákon č. 141/1961 Sb. § 158d(2) (Czech).

314. Blom, *supra* note 102, comment 4(e); *see also* Uzun v. Germany, 2010-VI Eur. Ct. H.R. 1, 16 (observing that technologically monitoring a scene in public is of a similar character as human observation, but that privacy considerations may arise "once any systematic or permanent record comes into existence").

315. Art. 15(5a) Police Act (Pol.) (allowing both observation and recording).

316. *See, e.g., supra* notes 86–89, 106, 127–28, 210, 249, 272 and accompanying text.

317. *See infra* Section III.B.1.b.

318. *See supra* Section III.A.1.

319. *See infra* Section III.A.3.

320. HR 18 mei 1999, NJ 2000, 104 m.nt. TMS § 5.3 (Neth.).

321. *Kamerstukken II* 1997/98, 25 403, No. 7 at 47 (Neth.).

322. United States v. Karo, 468 U.S. 705, 719 (1984).

3. Intensity: Depth, Continuity, and Frequency

The third factor in the Dutch list is the intensity of observation, which is an amalgam of closely related sub-factors, such as the depth, continuity, and frequency of surveillance. The closer, deeper, more continuous, or more frequent the observation, the higher its intensity. Continuous observation will be more intrusive than observation with intervals.[323] This factor also informed the court's assessment in *Maynard*, where the judge argued that while the GPS-tracked car may have moved in public, its movements were not *actually* exposed to the public over the period of 28 days "because the likelihood anyone will observe all those movements is effectively nil." Additionally, the continuity of tracking over this period resulted in an overall picture that was more intense than individual observations at discrete points in time could reveal.[324] Thus, the court found that the combination of *duration* and *intensity* outweighed the fact that the tracking occurred in public places. Similar arguments emphasizing the high intensity of (longer-term) GPS tracking as compared to human tailing are advanced in Italian doctrine, although not yet in in Italian case law itself.[325] At the same time, Italian authors also point out that GPS tracking is less intense than human tailing in some respects,[326] again demonstrating that a fine-grained analysis of how particular tracking technologies afford more or less intrusive insight into people's movements and behavior is required.

4. Duration

The duration of tracking is a fourth factor. Although evidently relevant—tracking someone for a year is obviously more intrusive than doing the same for a day—duration is a highly fluid factor, and the length of observation will usually only matter to the degree that other factors (such as place[327] and intensity[328]) make it more or less intrusive. The only exception in our sample is Germany, which considers any form of observation longer than 24 hours to be intrusive.[329] In other jurisdictions, the fluidity of duration can be seen in highly divergent assessments of the intrusiveness of tracking over various periods of time: 28 days of (continuous) GPS tracking of a car was considered sufficiently intrusive as to require a warrant in *Jones*,[330] but three months of (non-continuous) GPS-based car tracking was considered "a relatively short period of time" in *Uzun*.[331] Thirty days was considered

323. *Kamerstukken II* 1997/98, 25 403, No. 7 at 49 (Neth.); *cf.* Uzun v. Germany, 2010-VI Eur. Ct. H.R. 1, 27 (observing that the tracking occurred essentially only at weekends and when traveling in accomplice's car); R. v. Wise, [1992] 1 S.C.R. 527, 534 (Can.) ("Certainly, it could not be said that the device was capable of tracking the location of a vehicle at all times.").

324. *See supra* notes 147–49 and accompanying text.

325. *See supra* notes 142–44 and accompanying text.

326. *See supra* notes 145–46 and accompanying text.

327. *See, e.g., supra* notes 319–20 and accompanying text.

328. *See, e.g., supra* note 323 and accompanying text.

329. *See* STRAFPROZESSORDNUNG [STPO] [CODE OF CRIMINAL PROCEDURE] § 163f(1) (Ger.).

330. *See supra* notes 66–67, 151.

331. Uzun v. Germany, 2010-VI Eur. Ct. H.R. 1, 27.

reasonable by the Canadian Supreme Court, especially given the "the urgent need to protect the community" from a suspected serial killer.[332] While such evaluative differences may relate to differences in countries' legal systems, we think they more likely result from the influence of other factors, such as the different intensity (continuous as opposed to interval-based tracking) in *Jones* and *Uzun*. This is corroborated by the role duration plays *within* single jurisdictions: Dutch law, for instance, treats tracking someone's location in or near a brothel for a day or so as systematic,[333] as is (continuous) "observation lasting for nine months,"[334] yet observation over a period of 27 months in which the suspect was observed 60 times in public spaces (mainly by humans, although also by one static camera aimed at someone else's dwelling) was considered non-systematic.[335] Also, we encounter different assessments of duration in relation to different tracking technologies: car tracking for one or two days would likely not be considered particularly privacy-intrusive in the United States, but some scholars consider location records, in the context of law-enforcement access to third-party records, "highly private" if they cover more than 24 hours.[336] This suggests that the intensity of what location tracking can reveal colors the interpretation of the tracking's duration, rather than the other way around. The relativity of duration as a factor is, finally, also visible in the European Court of Human Right's observation in *Uzun* that the lack of a fixed statutory limit on the duration of monitoring was compensated by the general requirement of proportionality.[337]

5. Degree of Suspicion

A minor factor in the Dutch list, not mentioned in textbooks but occasionally applied in case law, is the degree of suspicion against someone.[338] In a few cases, Dutch courts have observed that someone engaging in criminal activity (such as spraying graffiti) or being associated with a burglary crime-scene cannot have a reasonable expectation to not be observed by the police.[339] Similarly, a U.S. court

332. R. v. Wise, [1992] 1 S.C.R. 527, 538 (Can.).

333. *See* HR 18 mei 1999, NJ 2000, 104 m.nt. TMS § 5.3 (Neth.).

334. *Kamerstukken II* 1997/98, 25 403, No. 7 at 50 (Neth.).

335. HR 18 mei 1999, NJ 2000, 104 m.nt. TMS (Neth.) (before art. 126g Dutch CPC was in force, but the judgement is still a touchstone in the interpretation of systematic observation, according to Blom, *supra* note 102, comment 4(e)).

336. *See* Freiwald, *supra* note 194, at 913 (referring to Stephen E. Henderson, *Real-Time and Historic Location Surveillance After* United States v. Jones*: An Administrable, Mildly Mosaic Approach*, 103 J. CRIM. L. & CRIMINOLOGY 803, 819 (2013) and agreeing with his conclusion that, in Freiwald's summary, "most location records would fall under the highly private category," while "information for a period of up to twenty-four hours [is] moderately private, and information for a single point in time [is] not private." (footnotes omitted)).

337. Uzun v. Germany, 2010-VI Eur. Ct. H.R. 1, 23.

338. This is also a factor influencing the *acceptability* of privacy intrusions, as seen in statutory or case law requirements for a certain level of suspicion to be met, but here we discuss it as a factor influencing the *seriousness* of the privacy intrusion.

339. *See supra* notes 106, 301; *see also* HR 10 April 2001, NJ 2001, 424 m.nt. § 3.4 (Neth.) (finding that degree of suspicion can be considered when assessing the lawfulness of observation).

held that contraband, by its very nature as something that a suspect has no legal right to possess in the first place, cannot attract a legitimate expectation of privacy; thus, tracking it cannot violate a Fourth Amendment interest.[340] Such argumentation suggests that if there is a high likelihood that someone is involved in criminal activity, they have a lower reasonable expectation not to be tracked by police, which apparently (at least in some cases) will diminish the seriousness of the privacy intrusion.

6. Object of Tracking

Not included in the Dutch list of intrusiveness-influencing factors as such, but quite prominent in the Dutch statutory regulation of observation, is the *object* of tracking—a factor that we also find in other jurisdictions. Generally, tracking a thing is less intrusive than tracking a person (except, as noted, if something is tracked into someone's home). Placing (non-consensually) a tracking device on a person (i.e., on the body or clothes, or on items typically carried in clothing, such as smartphones) is prohibited in Dutch law and is regulated more strictly in Canada and the United States.[341] Similarly, in U.K. law, location tracking of goods is not considered privacy-relevant, while location tracking of people is; as a consequence, it depends whether installing a tracking device on a car has the purpose of following the car or its occupants[342]—a distinction also made in the Dutch regulation of ALPR recordings, which only allows photographing (license-plate carrying parts of) cars but not people.[343]

Prior to *Carpenter*, lower-court judges in the United States had similarly argued that acquiring cell-site location information is intrusive because cell-phones are worn on or kept close to the body, both for historical[344] and for prospective[345] CSLI. This holding was confirmed by the Supreme Court (at least for historical records) in *Carpenter*. Because of the close association of cell-phones with persons, Canadian scholars also have argued that IMSI catchers for location tracking require an "Individual Tracking" warrant, not a warrant to track a thing.[346]

Altogether, then, it matters in several jurisdictions whether location tracking uses a method that interferes with bodily privacy or yields location information closely associated with a physical person, as opposed to methods that track the location of things not usually carried on or close to the human body.

---

340. United States v. Moore, 562 F.2d 106, 111 (1st Cir. 1976).

341. *See supra* Section II.B.3.

342. *See supra* notes 120–21 and accompanying text.

343. *See supra* notes 272–73.

344. *See* ROTHSTEIN, *supra* note 193.

345. *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526 (D. Md. 2011) [hereinafter *Specified Wireless Tel.*] (citing a study that 65 percent of U.S. adults have slept with their phone nearby), *discussed in* Rothstein, *supra* note 191, at 518.

346. *See* Israel & Parsons, *supra* note 163, at 57.

7. Covertness

The Dutch list of factors does not include covertness: although it may not usually be useful for police to track someone overtly, Dutch law considers this equally intrusive as covert tracking if done in a systematic way (i.e., depending on technology use, place, intensity, and duration).[347] In contrast, covertness is a primary factor in the U.K. regulation of surveillance, since visual observation is subject to RIPA's authorization requirements only when it is covert.[348] Polish law does not distinguish between overt and covert observation in public places,[349] but the *Suwałki* District Court found the covert nature of GPS tracking to be a relevant factor for applying stricter procedural requirements.[350]

Somewhat remarkably, covertness works the other way around in the Italian framework for GPS tracking, where overt tracking turns out to be considered more intrusive than covert tracking. Since GPS tracking is not specifically regulated, it counts as an atypical means of searching for evidence (Article 189 of the Italian Criminal Code), implying that results can be admitted by the judge if they are suitable for proving the facts and do not prejudice the moral liberty of the person; the latter is only the case when persons are affected in their mental freedom to choose. Since GPS tracking is a covert measure, unnoticed by the subject, and the resulting data are not statements (expressions of the mind), the followed person's mental self-determination is not at stake. Thus, the results of GPS tracking can be used as evidence.[351] Here, we see that the intrusiveness of location tracking has multiple dimensions and that interference with physical or behavioural privacy may—at least in this Italian case—be considered less important than interference with mental privacy.

Altogether then, we find that covertness is sometimes considered a factor of importance when assessing location tracking's privacy-intrusiveness. However, in many cases, it does not seem to play a significant role.

8. Active Generation of Data

A final factor, absent in Dutch law but prominent particularly in the United States, is whether police passively acquire or receive data that is generated anyway (particularly by those under investigation) or cause data to be generated at their own initiative. The latter is considered more intrusive, while the former is generally

347. *Kamerstukken II* 1996/97, 25 403, No. 3 at 70 (Neth.) (stating that the "description of observation does not include that the observation is covert" and that "[s]ystematic forms of non-covert observation are also covered by the description, although in practice these have limited meaning").

348. As defined in Regulation of Investigatory Powers Act 2000, c. 23, § 26(9)(a) (UK), surveillance is covert "if, and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place."

349. *See* OPALINSKI, ROGALSKI & SZUSTAKIEWICZ, *supra* note 57.

350. II Ka 267/13 District Court Suwalki, 19 December 2013 (Pol.).

351. ERCOLE APRILE & FILIPPO SPIEZIA, LE INTERCETTAZIONI TELEFONICHE ED AMBIENTALI 158–59 (2004); CLAUDIO MARINELLI, INTERCETTAZIONI PROCESSUALI E NUOVI MEZZI DI RICERCA DELLA PROVA 240–41 (2004); TABASCO, *supra* note 96, at 166.

considered not or less intrusive because of the third-party doctrine, as was most visible in the regulation of cell-site location information in the lead up to *Carpenter* (although, as noted earlier, the Supreme Court held that the third-party doctrine did not apply to the CSLI at issue in that case).[352]

When law enforcement itself initiates the generation of cell-phone metadata (such as with a GPS ping or by dialing the subject's cell-phone), the rationale behind the third-party doctrine would not seem to apply, making the privacy intrusion larger than when acquiring data generated by subjects themselves.[353] Somewhat more complicated is the issue of prospective CSLI, which is considered by some U.S. courts (but not by others) to be more intrusive than historical CSLI.[354] In this line of thinking, an order for prospective data ensures that police will acquire all location data generated in the period following the order, which otherwise might not have been stored by the provider, thus implying a more active role of law enforcement in the data's existence. German law also treats prospective CSLI as somewhat more intrusive than historical CSLI, since it applies some additional requirements,[355] but Dutch and Czech law treat both in the same way,[356] suggesting they do not consider it relevant for the privacy assessment whether law enforcement actively ensures that future location data will be recorded. The distinction between passive registration and active generation of data is also applied in the German regulation of silent SMS,[357] but not in the Dutch legal assessment of the same method,[358] showing consistency in how these countries use the factor of active involvement in data generation in their assessments across different methods of location tracking.

In the United States, this factor also plays a role in the assessment of Wi-Fi tracking: even if police use technology not in general public use (such as MoocherHunter software), identifying the location of someone using an open Wi-Fi router is not considered a Fourth Amendment search because the person voluntarily generates a signal that is broadcast into publicly accessible space outside his home.[359]

---

352. *See supra* note 176 and accompanying text; *see also* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection.").

353. Rothstein, *supra* note 193, at 510 (referring to United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004), *cert. granted, judgment vacated on other grounds sub nom.* Garner v. United States, 543 U.S. 1050 (2005), which determined that the third-party doctrine does not apply if police dial the subject's cell phone to generate CSLI).

354. *See supra* note 209.

355. *See supra* note 198 and accompanying text.

356. *See supra* notes 196, 199 and accompanying text.

357. *See supra* note 223.

358. *See* HR 1 juli 2014, ECLI:NL:HR:2014:1569 (Neth.).

359. *See supra* notes 292–93.

B. How is Privacy Framed?

The previous section showed that many factors can play a role in an assessment of the privacy intrusion of police tracking. There is considerable variation, not only among but also within jurisdictions. Which combination of factors is looked at, and how these are weighed, also depends considerably on the context of the tracking method and how it is applied. Within this large variation, however, it is possible to discern some patterns by looking at the underlying privacy interests at issue. Courts and lawmakers evaluate police tracking's intrusiveness from certain normative perspectives, associated with the privacy concern(s) that they perceive to be at stake. These perspectives function as "frames," that is, windows on the world through which a problem is looked at. Framing plays an important role in defining problems in social policy, and the way a problem is defined—the window through which it is observed—influences the way it is or can be solved: frames have considerable impact on the solution space of a problem.[360] Looking at the frames applied by lawmakers and courts to regulate police tracking gives us insight into how existing conceptualizations of privacy, including classic privacy frames and informational self-determination, are applied in the context of new criminal investigation methods. And interestingly, we see that new privacy frames are being proposed and developed to regulate police tracking, which is indicative of regulators' increasing discomfort with solutions that result from assessments relying on traditional privacy frames.

1. Classic Privacy Frames

Police tracking in its classic form—human tailing and observation—is usually restricted to publicly accessible places and, as it requires considerable time and effort, faces practical obstacles that commonly prevent it from being used very widely or intrusively. As a result, classic police tracking does not interfere with those aspects of the private sphere that are traditionally protected most strongly. However, with increasing technological capabilities allowing more intense forms of following people, police tracking may intrude more deeply into the private sphere. Indeed, we see that courts and lawmakers are particularly concerned with forms of police tracking that interfere with privacy types that are traditionally strongly protected, particularly by constitutional rights. In those cases, the following four classic privacy frames tend to be applied.

a. Secrecy of Communications

Since an important part of tracking people consists of tracking the movements of their cell-phones, the frame of communicational privacy is easily triggered. However, this frame is largely used by lawmakers and courts to argue why location

360. Donald A. Schön, *Generative Metaphor: A Perspective on Problem-Setting in Social Policy*, *in* METAPHOR AND THOUGHT 137 (Andrew Ortony ed., 1993).

tracking is not particularly intrusive, since it only collects metadata, not the content of communications.[361] While this argumentation is criticized in literature because it does not do justice to the intrusiveness of collecting locational metadata,[362] the emphasis on protecting communications content within the frame of communicational privacy still seems prevalent in most jurisdictions, which seems to foreclose arguments for strong privacy protection on the basis of cell-phones being tracked. We also see similar arguments with other forms of location tracking, such as GPS surveillance of cars, where the privacy-intrusiveness is argued to be lower than that of communications interception.[363] Overall, then, the frame of communicational privacy tends to be applied to argue against the need for particular safeguards against location tracking, suggesting a general prioritization of communicational privacy over the behavioral privacy that is associated with people's movements.

b. Home

As we observed, place is an important factor in normative assessments of location tracking[364] because the frame of spatial privacy features one of the traditionally strongest forms of privacy protection, the home. As Freiwald observed in the U.S. context, the "only affirmative constitutional analysis the appellate courts have ratified for determining reasonable expectations of privacy in location data, then, is based on the doctrine that the Fourth Amendment protects our privacy interests in the home and surrounding areas."[365]

Most jurisdictions put considerably stronger safeguards in place when surveillance consists of, or has a likelihood of, tracking someone or something inside the home. For instance, Poland and Czechia apply stricter conditions when people are observed or followed in non-public places, as does the U.K. for residential premises and Germany for (also very short) observations in the home.[366] Dutch law even prohibits visual observation inside the home altogether;[367] however, this prohibition is limited to making *visual recordings* inside the home, so that location tracking inside the home seems simply allowed.

With technological forms of location tracking at a distance, it is not always clear whether or when this will involve following someone into private spaces. Courts in several jurisdictions argue that (*ex post*) an operation involved in-home tracking or (*ex ante*) an operation has considerable likelihood (particularly given a certain duration of tracking) of involving in-home tracking. This argument is

361. *See supra* notes 167–68 and accompanying text.
362. *See supra* notes 184–85.
363. *See supra* notes 129–30 and accompanying text.
364. *See supra* Section III.A.2.
365. Freiwald, *supra* note 194, at 907.
366. *See supra* notes 29, 81–82 and accompanying text.
367. *See supra* note 99.

particularly used in relation to cell-phone tracking,[368] but we also encounter it in GPS tracking cases.[369]

Where the law does not impose specific safeguards on location tracking, it is frequently criticized in literature from the perspective of home protection. Italian authors argue that acquiring cell-phone location data interferes with the inviolability of the home[370] and that GPS tracking of cars is insufficiently regulated, because cars can be parked in an area belonging to protected space (as part of curtilage or private yards).[371]

c. Body

In some countries, tracking items worn on or close to the body is considered more privacy-intrusive than tracking other items; the Netherlands considers it so privacy-intrusive as to prohibit it altogether.[372] The frame of bodily integrity will be triggered more easily in jurisdictions that have specific constitutional protection for privacy of the body, as is the case in the Netherlands.[373] However, other jurisdictions we studied have constitutional protection of (the body of) the person in some form,[374] and one may wonder why, for instance, Germany does not apply stricter safeguards for tracking body-worn devices, given its constitutional right to physical integrity.[375] Possibly, this is because observation for longer than twenty-four hours is already strictly regulated in Germany,[376] and the effort and risk of

368. *See, e.g., supra* notes 212–13, 255 and accompanying text; *see also* Rothstein, *supra* note 193, at 528–29 (observing that the "home is sacrosanct in Fourth Amendment law: all details of the home are intimate details. . . . Precise cell phone tracking, like a beeper, reveals critical facts about the home's interior." (references omitted)).

369. *See, e.g.,* United States v. Karo, 468 U.S. 705, 714–15 (1984) (noting that the Fourth Amendment violation occurred at the moment agents tracked a beeper-equipped can after it entered a private residence, as this allowed the Government "to surreptitiously [employ] an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house").

370. Dinacci, *supra* note 185, at 371 (arguing that "it appears indisputable that the possibility to 'trace' the presence of persons in the home of a subject through acquiring traffic data is equivalent to rendering 'visible' that which the rights-holder intended to remain confidential"); *id.* at 392 (finding that acquiring location data through a cell phone traffic data production order infringes the inviolability of the home, and that the current regulation is not in line with the constitutional requirements).

371. Bene, *supra* note 42, at 361 (arguing that in GPS tracking "for longer periods . . . the risk is more concrete that the subject will park also in places of private abode"); *see also* MARINELLI, *supra* note 94, at 256–57.

372. *See supra* Section II.B.3.

373. GW. [Constitution] art. 11 (Neth.).

374. *See* Koops et al., *supra* note 17, at 529–31 (surveying constitutional protections of the (body of the) person).

375. GRUNDGESETZ [G] [BASIC LAW] , art. 2(2) (Ger.) (translation at *Basic Law for the Federal Republic of Germany*, BUNDESMINISTERIUM DER JUSTIZ UND FÜR VERBRAUCHERSCHUTZ, http://www.gesetze-im-internet.de/englisch_gg/index.html [https://perma.cc/7UDD-5HCP] (last visited Feb. 3, 2019)).

376. *See supra* note 29 and accompanying text.

detection inherent in planting a tracker on body-worn devices will be too high for only short periods of tracking.

d. Property

While bodily integrity is a key privacy frame in the Dutch context, the protection of property and proprietary privacy form an important frame in the common-law context,[377] most visibly in the United States. Significantly, the majority opinion in *Jones* resolved the privacy issues raised by GPS tracking by resorting to the frame of property rather than the reasonable expectation of privacy test;[378] a similar property interest emerges in the U.K.'s regulation of GPS tracking.[379] This focus on property interests, rather than reasonable expectations of privacy, was subjected to criticism by the concurring justices, and has also been characterized as ill-suited for non-trespassory forms of location tracking that are now (increasingly) prevalent in modern society.[380] Occasionally, the property frame may also be useful in civil-law systems to discuss the privacy interests raised by breaking into a car in order to place a tracking device.[381]

2. The Informational Privacy Frame

Informational privacy is, fifty years after Westin and the landmark German decision on informational self-determination,[382] also a classic privacy frame, but we discuss it separately from the previous ones since it is a transversal frame, cutting across all primary types of privacy.[383] While location tracking is frequently discussed within the frame of the privacy of communications, home, or body, we also encounter arguments that connect these, and other aspects of private life, into a narrative that emphasizes the information that can be derived from tracking someone's movements. This informational frame is applied more by doctrinal scholars than by courts or lawmakers.

---

377. *See* Koops et al., *supra* note 17 at 516–18 (surveying constitutional protections of property).

378. *See supra* note 66.

379. *See supra* note 125.

380. *See, e.g.*, Mary G. Leary, *The Missed Opportunity of* United States v. Jones*: Commercial Erosion of Fourth Amendment Protection in a Post-Google Earth World*, 15 U. PA. J. CONST. L. 331, 332–33 (2012) ("[T]he Court's most recent opinion in *United States v. Jones*, where the Court expanded its definition of a search, fails to keep current with technology."); David Gray, *A Collective Right to Be Secure from Unreasonable Tracking*, 48 TEX. TECH. L. REV. 189, 195 (2015) ("[A]s Justice Sotomayor points out in *Jones*, we do not yet have constitutional principles capable of addressing, much less limiting, [many forms of contemporary] surveillance . . . .").

381. *See supra* text accompanying notes 297–301 (the Dutch discussion on the flock fiber method); *cf. supra* notes 122–24 and accompanying text (the Italian discussion whether a car's inside is a protected space), but that discussion fits more in a home frame than a property frame.

382. BVerfGE, 1 BvR 280/66, Oct. 13, 1971 (Ger.) (identifying a right to informational self-determination); ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (defining privacy as the claim to determine when, how, and to what extent information about people is communicated to others).

383. Koops et al., *supra* note 17 at 568–69.

For instance, *Wagnerová et al.* argue that the Czech constitutional protection of private life (Article 10 Charter), and its element of informational self-determination, includes the right to protection from surveillance (being watched or followed in public spaces), especially by public authorities; nevertheless, such powers of the state are not altogether excluded.[384] In Italy, authors criticize the Supreme Court's limiting of its evaluation of GPS tracking to the inviolability of the home, arguing that other fundamental rights are also at stake. Moreover, since the production order for traffic data (which includes location data) has safeguards to protect personal data, similar safeguards should apply to GPS tracking; in particular, a motivated order by the public prosecutor.[385] Rothstein argues that "precise persistent cell phone tracking reveals private facts" and points out that the "private facts" model is often used to evaluate new forms of electronic surveillance,[386] thus emphasizing the usefulness of informational privacy as a frame for assessing location tracking. Similarly, Buruma argues that when the Dutch list of factors relevant for judging the "systematicness" of tracking does not point to a clear outcome, the courts could particularly look at "whether data are collected on 'certain privileged domains of life.'"[387]

While informational privacy is thus frequently used in literature to argue that location tracking is, or can be, considerably intrusive, courts, in contrast, tend to use the frame to argue that certain instances of location tracking are *not* particularly intrusive. The European Court of Human Rights in *Uzun*, for instance, observed that "GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which . . . as a rule . . . disclose more information on a person's conduct, opinions or feelings."[388] The Canadian Supreme Court in *Wise*, like the U.S. Supreme Court in *Knotts*, found that the information obtained through using a tracking beeper "merely assisted the police to gather evidence which, to a great extent, they had [or could have] obtained by visually observing the vehicle."[389] Similarly, the Dutch Supreme Court allowed location tracking with an IMSI catcher on the basis of Article 3 of the Police Act of 2012, partly because of the fact that it only reveals the phone's (or user's) location but not what the user does or says.[390]

While the latter argument may be correct in and of itself—knowing where someone is does not imply that you know what they are doing there—there are, of course, certain correlations between places and behavior. In a few cases, we see courts recognizing that inferences about private life can be drawn from location

384. E. WAGNEROVÁ, I. POSPÍŠIL, T. LANGÁŠEK & V. ŠIMÍČEK, LISTINA ZÁKLADNÍCH PRÁV A SVOBOD, KOMENTÁŘ 285 (2012).

385. GIUSEPPE TABASCO, PROVE NON DISCIPLINATE DALLA LEGGE NEL PROCESSO PENALE 166–67 (2011); *see also* Bene, *supra* note 42, at 366–67; Marinelli, *supra* note 94, at 257.

386. Rothstein, *supra* note 191, at 528.

387. Buruma, *supra* note 48, at 658.

388. Uzun v. Germany, 2010-VI Eur. Ct. H.R. 1, 18.

389. R. v. Wise, [1992] 1 S.C.R. 527, 543 (Can.).

390. *See* HR 1 juli 2014, ECLI:NL:HR:2014:1562 (Neth.).

data and that these inferences may even reveal insight into intimate parts of life. When assessing the gravity of the encroachment connected with an investigation measure, the German Constitutional Court considers

> the processed data's relevance to personality [to be] of special significance. A measure is considered highly invasive in particular when the relevant data allow conclusions about the nature and intensity of interpersonal relationships, personal interests, habits and tendencies, or the content of communication.[391]

Now, because of the increasing digitization of telecommunication, traffic data reveal an ever-clearer picture of communication partners, which implies that increasingly, "communication data allow conclusions to be drawn about their personality, and even the generation of a personality profile becomes a real possibility."[392] The intimate nature of inferences possibly drawn from location data has been most forcefully expounded by the *Maynard* court: location data may reveal whether someone "is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."[393]

Such framing of location tracking is, however, as yet relatively rare among courts in the jurisdictions we studied. We are not aware, for instance, of Canadian courts having used similar arguments related to informational privacy in location-tracking cases (except insofar as Justice La Forest recognized the future potential of pervasive tracking in his dissent in *Wise*), even though Canadian law strongly protects "a biographical core of personal information [including] information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[394] Apparently, courts in Canada, and jurisdictions other than Germany and the United States, have not yet felt the need to draw on the insight that location data collected over a period of time can precisely reveal such intimate details of lifestyle and personal choices that informed the *Maynard* court's decision.

---

391. Vogel et al., *supra* note 169, at 515 (referring to BUNDESVERFASSUNGSGERICHT [BVerfG] [Federal Constitutional Court] Oct. 10, 2007, NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 2464 (2470), 2007 (Ger.) and BUNDESVERFASSUNGSGERICHT [BVerfG] [Federal Constitutional Court] 2006, NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 976 (980), 2006 (Ger.)).

392. *Id.* at 515–16 (referring to BUNDESVERFASSUNGSGERICHT [BVerfG] [Federal Constitutional Court] 2006, NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 976 (980), 2006 (Ger.)).

393. *See supra* note 150 and accompanying text; *see also supra* notes 194, 214 and accompanying text for similar arguments by the New Jersey Supreme Court under state law and by a district judge who observed that continued tracking can reveal intimate details of a person's life that entering someone's home need not reveal.

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

3. New Privacy Frames

a. Freedom of Movement, Anonymity, and a Right Not to Be Localized

While informational privacy provides a useful frame for assessing the intrusiveness of location tracking, as it enables looking at the information about persons that can be derived from their movements, it may not be the only relevant frame to do so. In our research, we encountered another novel frame that connects informational privacy with what might be considered the main underlying privacy interest in location tracking, the behavioral privacy that is connected to the freedom of movement. This frame has been adopted by Italian authors, who argue that location tracking affects the liberty of movement, which is safeguarded by Italy's Constitution.[395] *Tabasco* observes that "if the liberty to circulate be understood as liberty to move freely without being spied on by mechanical instruments that do not allow the person to be aware of being 'followed,' it is evident that the activity of GPS tracking, inherent to the localization of an individual, infringes such an inviolable right."[396] Therefore, a "right not to be localized" should exist as a new component of the liberty of movement.[397]

Such a right can be connected to the right to anonymity, which is relevant in public space. Commenting on a 2010 GPS tracking judgment, Gentile observes that in today's society, people expose considerable parts of their life in social interactions outside of the home:

> This undeniable observation can, however, not legitimate any form of intrusion into the private sphere that could engender in the individuals the sensation of being continuously the object of control, generating doubtless prejudicial effects that evoke the so-called panopticon effect, inhibiting the human mind at the moment where it develops the obsession of constantly being under control.[398]

In this context, the right to anonymity (*diritto all'anonimato*) has emerged in Italy. This right protects people from undue and prolonged intrusions into the private individual sphere and also when they voluntarily act in public places.[399] The right to anonymity is recognized in Italy as part of the inviolable rights of the person, protected by Article 2 of the Constitution, and protects "situations and personal

395. Art. 16 Costituzione [Cost.] (It.) ("Every citizen can circulate and stay freely in any part of the national territory, subject to limitations established by law in general for reasons of health or security. No restriction can be determined by political reasons.").

396. Tabasco, *supra* note 96, at 166.

397. *Id.* (referring to A. Camon, *L'acquisizione dei dati sul traffico delle comunicazioni*, 47 RIVISTA ITALIANA DI DIRITTO E PROCEDURA PENALE 594, 633 (2005)); *see also* Bene, *supra* note 124, at 348 (asking whether GPS tracking infringes article 16 Constitution, understood also as a "right not to be localized").

398. Gentile, *supra* note 144, at 1472.

399. *Id.* at 1473.

and family events from public curiosity and knowledge."[400] It is part of the "doctrine of privacy, understood in a new and more advanced form," which helps to safeguard other fundamental liberties (and ultimately individual self-determination). This, Gentile concludes, can point the way to a legislative intervention with detailed norms for GPS tracking.[401]

The frame of free movement, anonymity, and a right not to be localized is, so far, not widely applied outside of Italian scholarship. However, it sometimes pops up in other jurisdictions too, for instance in the U.S. context, where William Herbert has—somewhat provocatively—argued that location monitoring and control "constitutes a vestige and incident of slavery," implying that the Thirteenth Amendment might apply to location tracking.[402] This amendment grants Congress "the power to enact legislation targeted at eliminating those badges and incidents of slavery including the 'privilege to go and come' as one pleases."[403] Therefore, a law could be enacted "to ban the use of tracking devices to dominate and control the location of others."[404]

Another example is a report by the Dutch Rathenau Instituut, which advises Parliament on technology matters. In a report for the Council of Europe on robotics, artificial intelligence, and augmented reality, it observes that pervasive tracking and tracing has the accumulative effect of a "gradual but steady dissolving of privacy and anonymity for the individual."[405] However, people cannot be supposed to simply turn off their mobile devices if they do not want to be tracked or traced. Rather, lawmakers should recognize that in this context, the right to remain anonymous and/or the right to be let alone are at stake, "which in the robot age could be phrased as the right to not be electronically measured, analysed or coached."[406] Therefore, the Rathenau Instituut recommends that the Council of Europe "clarify to what extent in the context of the robot age the right to respect for privacy implies the right to not be measured, analysed or coached."[407] The argument that people should not be forced to turn off their mobile devices if they do not want to be tracked or traced is echoed in the *Carpenter* judgment, where the court argued that "[w]hoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years. . . . Only the few without cell

400. Racc. uff. corte cost., 12 aprile 1973, n. 38, (It.) (quoted in Bene *supra* note 124, at 362). Both Gentile and Bene refer to Gabriella Di Paolo, *Acquisizione dinamica dei dati relativi all'ubicazione del cellulare ed altre forme di localizzazione tecnologicamente assistita. riflessioni a margine dell'esperienza statunitense*, CASSAZIONE PENALE 1219 (2008), who suggested applying the right to anonymity to develop regulation of location tracking.

401. Gentile, *supra* note 144, at 1473.

402. Herbert, *supra* note 11, at 429.

403. *Id.* at 428 (referring to Jones v. Alfred H. Mayer Co, 392 U.S. 409, 430 (1968)).

404. *Id.* at 429.

405. RATHENAU INSTITUUT, HUMAN RIGHTS IN THE ROBOT AGE 43 (2017), https://www.rathenau.nl/en/digitale-samenleving/human-rights-robot-age.

406. *Id.* at 44.

407. *Id.*

phones could escape this tireless and absolute surveillance."[408] From that perspective, these limitations on law enforcement agencies' ability to access historical CSLI might be interpreted (although not phrased as such in the judgment) as expressing the idea that people ought to have a reasonable claim or ability to not be localized.

Thus, while the privacy interest in anonymity and freedom of movement is not yet widely recognized as relevant for assessing location tracking, we think it may become a more prevalent and productive frame in the future, as pervasive location tracking (not only by police, but also by other public and private actors) may be increasingly felt to stifle people's sense that they can freely move around in public space without an inhibitory or panoptic effect of feeling followed.

b. Mosaic Theory

A more broadly applied new frame is that of the privacy interest consisting in the cumulative picture, or mosaic, of disparate pieces of information. Single stones say very little, but put together, a mosaic of many small stones can be quite revealing of someone's private life. As the *Maynard* court expressed, "the whole of one's movements . . . reveals more—sometimes a great deal more—than does the sum of its parts."[409] Here, the judge borrowed from case law related to exemptions to disclosure under the Federal Freedom of Information Act for national security purposes: "What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context."[410]

This reasoning, which is generally referred to as the mosaic theory (endorsed by both concurring opinions in *Jones*[411] and built upon in *Carpenter*),[412] has yet to gain a firm foothold in U.S. case law. Although it is welcomed by several scholars

408. *See supra* note 190.

409. *See supra* note 149 and accompanying text.

410. CIA v. Sims, 471 U.S. 159, 178 (1985) (as quoted in *id.* at 562 (internal citations omitted)). The mosaic theory resembles some principles from moral philosophy. Parfit points out five mistakes in moral mathematics, which include ignoring the effects of sets of acts and ignoring small or imperceptible effects. *See* DEREK PARFIT, REASONS AND PERSONS 70–78 (1984). He claims that "[e]ven if an act harms no one, this act may be wrong because it is one of a *set* of acts that *together* harm other people." *Id.* at 70 (italics in original).

411. *See* United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring); *id.* at 428–31 (Alito, J., concurring).

412. *See* Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (referring to information that was "detailed, *encyclopedic*, and effortlessly compiled" (emphasis added)); *id.* at 2217 (referring to "an *all-encompassing* record" (emphasis added)) (discussing where the metaphors of encyclopedias and all-encompassing records echo the mosaic theory's metaphor of a comprehensive image made up of small items); *see also supra* notes 179, 187 and accompanying text.

as an important new perspective on privacy protection in the context of law enforcement,[413] it is also criticized for vagueness and lack of normative guidance.[414]

Still, it seems significant that similar reasoning is applied in several of our jurisdictions. Although not labeled in terms of the mosaic theory, and phrased in less vivid terms than in *Maynard*, the argumentation in various location-tracking cases demonstrates mosaic argumentation. For instance, the German *Bundesgerichtshof* highlighted that GPS tracking technology should be considered together with other measures: "If the application of 'GPS' goes along with other interventions, each being in itself permissible, and if this leads to a comprehensive surveillance of the person, then this can violate the proportionality principle."[415] In effect, Germany prohibits "total surveillance" (*Totalüberwachung*) or "all around surveillance" (*Rundumüberwachung*) that would lead to a comprehensive personality profile of someone. This is ensured, according to the Constitutional Court, by the general procedural guarantees of subsidiarity and proportionality, which imply that the cumulative effect of different investigation activities needs to be taken into account.[416] The "personality profile" can be seen as a mosaic picture that reveals the core of someone's private life.[417] The German safeguards against "total surveillance" resonate in the U.S. Supreme Court's warrant requirement for the collection of historical CSLI in view of its character as "tireless and absolute surveillance."[418]

---

413. *See, e.g.,* Lance H. Selva, William L. Shulman & Robert B. Rumsey, *Rise of the Mosaic Theory: Implications for Cell Site Location Tracking by Law Enforcement*, 32 J. MARSHALL J. INFO. TECH. & PRIVACY L. 235 (2016) ("[T]he mosaic theory provides the most compelling approach to addressing the challenge . . . to interpret and apply Fourth Amendment principles as originally conceived by the Framers to ever-evolving technologies of surveillance."); Christopher Slobogin, *Making 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); *see also* Stephen E. Henderson, *Real-Time and Historic Location Surveillance After United States v. Jones: An Administrable, Mildly Mosaic Approach*, 103 J. CRIM. L. & CRIMINOLOGY 803 (2013) (outlining "an administrable" approach, informed in part by the mosaic theory); Rothstein, *supra* note 193 at 527 (defending the mosaic theory against Orin Kerr's criticism).

414. *See, e.g.,* Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 209–10 (2015) (finding that survey respondents, as proxies for the subjective expectations of privacy element of the *Katz* test, do not coincide with Justice Alito's arguments in favor of the mosaic theory—particularly the claim that duration of tracking impacts perceived intrusiveness); 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) ("[A]s a normative matter, courts should reject the mosaic theory.").

415. BGH Jan. 24, 2001, 3 StR 324/00, 27 (OLG Düsseldorf) (Ger.).

416. BVerfG, Az. 2 BvR 581/01, Apr. 12, 2005 (Ger.).

417. *Cf.* Vogel et al., *supra* note 169, at 515–16 ("The quantity and the substance of accruing traffic data serve to *paint an ever clearer picture* of communication participants. Increasingly, communication data allow conclusions to be drawn about their personality, and even the generation of a *personality profile* becomes a real possibility." (italics added)).

418. *See* Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

The mosaic metaphor is also visible in the main Dutch frame used to assess the intrusiveness of location tracking: an investigation operation is considered "systematic" if it results in "a more or less *complete image* being obtained of certain aspects of someone's [private] life."[419] The Polish District Court in *Suwałki* also applied mosaic argumentation, where it reasoned that collecting individual bits of information that reveal no significant conclusions about someone is to be distinguished from the systematic collection of location data for a longer time, which reveals far more about the person.[420]

Thus, in GPS-tracking cases, U.S. courts—as well as courts in Germany, the Netherlands, and Poland—have applied the main principle of the mosaic theory, namely that the intrusiveness of a measure should not be judged (only) on the basis of the collection of discrete pieces of information, each of which may reveal little, but (also) on the basis of the cumulative picture emerging from the combination of all these pieces. This is a telltale sign that the traditional privacy frames through which location tracking would normally be assessed, fall short when it comes to tracking persons in public space: apparently, the frame of the home—with its implication that acts in public can be freely observed—does not offer satisfactory solutions, and courts therefore reframe the problem in different terms.

It remains to be seen to what extent the mosaic theory offers concrete guidance to assess the intrusiveness of different forms of location tracking. Yet even if the mosaic theory, in its current embryonic stage of development, lacks a concrete yardstick to judge when the combination of stones is revealing enough to constitute a mosaic, it has added value. This is because in framing the problem of location tracking in terms of accumulated data, it invites looking for solutions that are better suited to contemporary society than the answers offered by the old frame of the public space/private space distinction. In other words, even if the mosaic theory does not provide ready answers, by asking how much information police may gather about someone's private life by tracking their movements, it at least asks a more pertinent question than the old question of whether someone has willingly exposed themselves to being visible in public.

CONCLUSION

The answer to the question "Where have you been?" can be very telling, not only revealing factual information about your exact whereabouts at certain points in time, but also suggestive of your habits and preferences, and ultimately, if sufficient location information is available, of most of your private life. Location tracking may be age-old, but never has technology afforded so much insight into people's personal life as contemporary tracking technologies do. The privacy interest in location information is therefore profound. Is this profound interest recognized in current legal assessment on the intrusiveness of location tracking?

---

419. *See supra* note 102 (emphasis added).
420. *See supra* note 139 and accompanying text.

As this Article shows, there is great variety in technologies and forms of location tracking, and the intrusiveness of location tracking varies accordingly to a substantial extent. Not only does the intrusiveness differ depending on the method and technology, it also depends considerably on the way in which the technology is applied in concrete cases. This implies that, although some general assessment of a tracking method's intrusiveness is possible (ALPR monitoring of cars is generally less intrusive than GPS tracking of body-worn devices), a fine-grained analysis of how particular tracking technologies afford more or less intrusive insight into people's movements and behavior, depending on how they are used, is required. Altogether, this requires a highly context-dependent, and thus case-specific, assessment, in which a number of factors (such as use of particular technical devices; covertness; place, intensity, duration, and object of monitoring; and whether police actively generate or passively receive location data) must be taken into account, none of which is necessary or sufficient in itself.

At a deeper level of analysis, it turns out that it is not only the case that various factors play a role in intrusiveness assessments; the way in which the privacy interest in location tracking is *framed* is also relevant. When confronted with new forms of location tracking, lawmakers and courts—understandably—initially resort to existing privacy frames, that is, the well-established types of privacy that have been firmly established as protection-worthy in legal systems: communications privacy, the spatial privacy of the home, and bodily privacy, as well as informational privacy. Viewed through these frames, location tracking usually does not appear particularly intrusive. Framing the question as "To what extent does location tracking infringe the privacy of communications, home, or body?" invites a prima facie answer, "not very much." The classic frames of communicational privacy and spatial privacy tend to be applied to argue against the need for particular safeguards against location tracking, suggesting a general prioritization of communicational and spatial privacy over the behavioral privacy that is associated with people's movements. Similarly, from an informational privacy perspective, location tracking need not at first sight be very privacy-sensitive since location coordinates reveal where you have been, but not what you have done or said there. This implies that if the question of location tracking's intrusiveness is formulated on the basis of traditional privacy frames, the answer tends to be biased towards downplaying the privacy infringement of location tracking.

As our analysis shows, there is increasing discomfort with the answers thus yielded by the traditional privacy frames. While lawmakers and courts still do resort to these frames, arguing, for example, that GPS tracking is not very intrusive because it is largely limited to public space and that cell-phone tracking does not reveal communications content, scholars (and to some extent, lawmakers and courts) have started to resort to other frames. This shift reflects an increasing recognition that people's locations are strongly correlated to their habits and preferences, and that what people do can reveal as much about their inner life as what they say. But this is, of course, not always the case: it is hard to find objective,

a priori criteria for when behavior can be as revealing as someone's utterances or the details of their domestic life. This perhaps explains the intuitive appeal of the mosaic theory, which is the main novel-privacy frame to emerge from contemporary location-tracking cases. The mosaic theory functions as an important normative addition to the frame of informational privacy by focusing attention on the *accumulation* of information: the picture emerging from putting together discrete pieces of information is more revealing than the sum of its parts. The combination of the informational-privacy frame and the mosaic theory seems well-suited to assess the intrusiveness of location tracking, since it eminently enables a context- and case-specific assessment. Its strength may also be its weakness, since its broad applicability in all cases does not provide a concrete yardstick to measure when a collection of stones, put together, constitutes a mosaic. Yet we think that it has added value over traditional privacy frames since, even if it does not give ready answers, it asks a more pertinent question than those raised within traditional frames of communicational, spatial, and bodily privacy.

The mosaic theory, which is as yet in a rather embryonic stage of conceptualization, should be further developed, as it may assist in regulating twenty-first-century criminal investigation methods that challenge privacy in ways that are hard to address with twentieth-century legal frameworks. Its potential obviously stretches beyond location tracking, since its abstract character may well be applied to all forms of criminal investigation (and, indeed, to the combination of different methods). However, because of its abstractness, the mosaic theory may also turn out to lack normative thrust, at least when it comes to guiding the regulation of specific forms of location tracking. There may be merit, therefore, in also considering the other novel frame emerging from our analysis: the freedom of movement, or the interest in moving around in publicly accessible places in relative anonymity, without (the feeling of) being continuously monitored. This frame is specifically suited to assess the intrusiveness of location tracking, as it connects the informational content of location data to the underlying privacy interest, namely the behavioral privacy of moving around in public space without the inhibitory or panoptic effect of feeling followed. Since quite a few relatively new methods of location tracking, such as real-time cell-phone location tracking, stealth SMS, and IMSI catchers, are now being introduced (or are starting to be applied more broadly) by police in many countries, there is a window of opportunity for lawmakers and courts to consider adopting the frame of anonymity and freedom of movement to assess the intrusiveness of location tracking.

Overall, we conclude that the analysis in this Article demonstrates that legal privacy frameworks developed in the nineteenth and twentieth centuries are not well-suited for assessing the privacy-intrusiveness of contemporary location-tracking investigation methods, particularly since location tracking can have characteristics of "tireless and absolute surveillance." The emergence of novel frameworks for understanding and protecting privacy opens up new pathways for

lawmakers and courts to address the challenge of preserving privacy in the twenty-first century.