When is Personal Data "About" or "Relating to" an Individual? A Comparison of Australian, Canadian, and EU Data Protection and Privacy Laws

Normann Witzleb* & Julian Wagner **

The definition of "personal information" or "personal data" is foundational to the application of data protection laws. One aspect of these definitions is that the information must be linked to an identifiable individual, which is incorporated in the requirement that the information must be "about" or "relating to" an individual. This article examines this requirement in light of recent judicial and legislative developments in Australia, Canada and the European Union. In particular, it contrasts the decisions rendered by the Federal Court of Australia in Privacy Commissioner v Telstra Corporation Ltd *and by the European Court of Justice decisions in* Scarlet Extended *and* Patrick Breyer v Bundesrepublik Deutschland *as well as the new* General Data Protection Regulation *with Canadian law. This article also compares how the three jurisdictions deal with the vexed issue of IP addresses as personal information where the connection between the IP address and a particular individual often raises particular problems.*

---

* Normann Witzleb (Dr, LLB) is an Associate Professor at the Faculty of Law, Monash University, Melbourne, Australia. His research focus is on Australian and European private law, and in particular, the area of privacy rights, torts and remedies.

** Julian Wagner (Dr, LLM Eur.) is a Lecturer at the Faculty of Law (Chair of Prof Dr Spiecker gen. Döhmann, LLM), Goethe University, Frankfurt am Main, Germany. His research focuses on European law, environmental law and privacy law. His work was supported by a postdoc fellowship of the German Academic Exchange Service (DAAD).

I. Introduction

Data protection laws aim to protect personal privacy by regulating the collection, processing and transfer of "personal information" (Australia and Canada), "personal data" (European Union) or "personally identifiable information" (United States). While the definitions of these terms vary across jurisdictions, what they have in common is that they are of fundamental significance. Data that does not contain information about an identified or identifiable individual in the sense of the respective definition falls outside the scope of data protection laws.

Differences in the definition of "personal information" have relevance not only for the application of domestic data protection laws but also affect data transfers between countries. Many domestic data protection regimes impose restrictions on the export of personal data to

a third country, particulary if the data protection level in that country is weaker than the law of the exporting state. This is intended to prevent the bypassing of national data protection laws by the transfer of data to a third country without an adequate level of protection. However, even if the substantive data protection laws of a third country provide a comparable level of protection overall, a closer look at the scope of application of its data protection regime may also be necessary. If a third country adopts a narrower understanding of the term "personal data", that country's privacy laws will not apply to some data that would be protected by the laws of the exporting country.

This article will analyse recent developments relating to these definitions in Australia and the European Union and provide a comparison with Canadian data privacy law. The article is prompted by an Australian appellate decision on the definition of "personal information" under the *Privacy Act*.[1] In its decision, *Privacy Commissioner v Telstra Corporation Ltd*,[2] the Full Court of the Federal Court of Australia also considered relevant Canadian jurisprudence. In particular, it referred to the decision of the Federal Court of Appeal in *Canada (Information Commissioner) v Canada (Transportation Accident Investigation & Safety Board)*.[3] This article will also consider recent developments in the European Union and, in particular, the new *General Data Protection Regulation* ("*GDPR*")[4] and two recent decisions of the European Court of Justice. The practical consequences of the differences between the terms will be explained using the example of the classification of Internet Protocol ("IP") addresses as personal information or as personal data, respectively.

---

1. *Privacy Act 1988* (Cth) (Austl) [Austl *Privacy Act*].
2. [2017] FCAFC 4 [*Telstra* FCAFC].
3. 2006 FCA 157 [*Canada (Information Commissioner)*].
4. EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1 [*GDPR*].

II. The Necessary Link between the Information and the Individual

The necessary link between the information in question and the individual differs in Australian, Canadian and European Union law.

A. Australian Law

Australia's federal data protection laws are contained primarily in the *Privacy Act*. The *Act* is informed by the 1980 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[5] and is mirrored in data protection laws in a number of Australian states and territories. The *Privacy Act* contains thirteen Australian Privacy Principles ("APPs"), which govern the collection, use, disclosure and storage of personal and sensitive information and how individuals may access and correct records containing such information. The APPs apply to most commonwealth government agencies and large private sector organisations (the so-called "APP entities").

The current definition of "personal information" in section 6 was inserted into the *Privacy Act* in 2014.[6] It states:

> information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.[7]

This represented a modernisation of the previous definition, which had been unchanged in the legislation since 1988 and defined (also in section 6) "personal information" as follows:

> information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be

5. OECD Council, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, (1980) [OECD Guidelines].
6. The *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) (Austl), took effect from 12 March 2014.
7. Austl *Privacy Act*, *supra* note 1, s 6(1).

ascertained, from the information or opinion.[8]

The new definition followed the recommendation of the Australian Law Reform Commission, which undertook a comprehensive review of Australian privacy laws in 2008.[9] The Explanatory Memorandum to the Amendment Bill explained that the amendment did not significantly change the scope of what is considered to be personal information.[10] In line with international standards, the new definition focuses on "identification" rather than the "identity" of the relevant individual. A related change is that it is no longer a requirement of the current definition that the person's identity must be apparent or reasonably ascertainable "from the information or opinion" itself. Information can now also be personal if it does not itself identify an individual but if it does so when combined with "other" information,[11] provided that the identification is reasonable. On that basis, it is likely that the new definition is "broader in scope than its predecessor".[12]

Most debate surrounding the definition of personal information is related to the issue of when a person is "identified" or "reasonably identifiable".[13] These discussions have become more important in light of

8. *Ibid*, as it appeared in 1988.
9. Austl, Commonwealth, Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108) (ALRC, 2008) [ALRC, *For Your Information*].
10. Austl, Commonwealth, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012 Explanatory Memorandum* (2012) at 53 [Austl, Commonwealth, *Privacy Amendment Bill 2012 Explanatory Memorandum*].
11. Austl, Commonwealth, Office of the Australian Information Commissioner, *What is personal information?* (OAIC, 2017) at 7 [OAIC, *What is personal information?*].
12. Anna von Dietze & Anne-Marie Allgrove, "Australian privacy reforms: an overhauled data protection regime for Australia" (2014) 4:4 International Data Privacy Law 326 at 328.
13. See *e.g.* Anne SY Cheung, "Re-personalizing Personal Data in the Cloud" in Anne SY Cheung & Rolf H Weber, eds, *Privacy and Legal Issues in Cloud Computing* (Cheltenham: Edward Elgar Publishing, 2015) 69 at 69.

significant recent advances in re-identification technologies.[14] While de-identified information falls outside data protection laws, it has become contentious when information is sufficiently de-identified in the sense that, even with the use of re-identification technologies, individuals are no longer "reasonably identifiable".[15] However, this article will focus its attention on another aspect of the definition, *i.e.* the required linkage between the information and the person to which it is said to relate. This has previously been given less attention but was at the centre of the decision of the Australian Federal Court in the *Telstra* matter.

While the OECD Guidelines define personal data as "information relating to an identified or identifiable individual",[16] the Australian definitions — in their previous and current versions — refer to information "about" an individual. The Australian Law Reform Commission did not recommend a change to this formulation, noting that:

> although a number of international instruments use the term 'relates to', the *Privacy Act* terminology is consistent with the APEC Privacy Framework and reflects that fact that the information must be about an identified or reasonably identifiable individual.[17]

It has long been a matter of contention whether this formulation "about an individual" required a more direct link between the data and the individual than the formulation "relating to an … individual".[18] Any differences in meaning may be relevant in cases where information has

14. Jane Henriksen-Bulmer & Sheridan Jeary, "Re-identification Attacks—A Systematic Literature Review" (2016) 36:6 International Journal of Information Management 1184.
15. Council of Europe, Article 29 Data Protection Working Party, *Opinion 05/2014 on Anonymisation Techniques*, (2014) 0829/14/EN, WP216; Information and Privacy Commissioner, Ontario, Canada, "Big Data and Innovation, Setting the Record Straight: De-identification *Does* Work" , by Ann Cavoukian & Daniel Castro (Toronto: IPC, ITIF, 16 June 2014).
16. OECD Council, *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (2013) at Part I, 1. b).
17. ALRC, *For Your Information*, *supra* note 9 at para 6.51.
18. See *e.g.* Mark Burdon & Alissa McKillop, "The Google Street View Wi-Fi Scandal and its Repercussions for Privacy Regulation" (2013) 39:3 Monash University Law Review 702 at 712.

only a tenuous connection with an individual, and in particular where information identifies a device rather than an individual. In the *Telstra* litigation, this issue became central when a technology journalist named Ben Grubb sought access to the personal metadata held by Telstra, his mobile phone service provider. Telstra refused access to mobile network data that could be linked to Mr. Grubb only through cross-matching between the various databases, systems and networks which Telstra operated. The Australian Administrative Tribunal overturned the Privacy Commissioner's determination that the refusal to provide access to such metadata was in breach of privacy principles.[19] This decision was confirmed by the Full Court of the Federal Court.[20]

1. The *Telstra* Determination by the Privacy Commissioner

The *Telstra* decision grappled with the issue of whether the Australian definition contains two cumulative elements: first, that the data must be about a person; secondly, that the data must enable the identification of this person.[21] Before the decision of the Full Federal Court, the definition of personal information was considered in the 2008 inquiry by the Australian Law Reform Commission into Privacy Law and Practice[22] in

19. *Telstra Corporation Ltd v Privacy Commissioner*, [2015] AATA 991 [*Telstra* AAT].
20. *Telstra* FCAFC, *supra* note 2.
21. *Re Grubb and Telstra Corp Ltd*, [2015] AICmr 35 (Austl) [*Re Grubb*].
22. ALRC, *For Your Information*, *supra* note 9, ch 6.

a number of decisions of the Australian Administrative Tribunal[23] and in guidance notes of the Privacy Commissioner.[24] However, the notion of personal information had not been the subject of judicial analysis at the appellate level in Australia.

The opportunity for obtaining authoritative guidance arose from a privacy complaint by Mr. Grubb against Telstra. In 2013, when Australia's metadata retention legislation was being debated, Mr. Grubb sought access to all metadata that Telstra held about his mobile phone service. At that time, the (former) National Privacy Principle ("NPP") 6.1 in the *Privacy Act* gave individuals the right to access, subject to some exceptions, their own personal information held by an organisation, such as Telstra.[25]

When Telstra refused to provide access to all data requested, Mr. Grubb filed a complaint under section 36 of the *Privacy Act*. During an investigation by the Privacy Commissioner, Telstra provided access to further call data contained in billing records but continued to refuse access to some mobile network data, such as IP address information,[26]

---

23. *Re Lobo and Department of Immigration and Citizenship*, [2011] AATA 705 (concerning the definition of personal information in the *Freedom of Information Act 1982* (Cth) (Austl)); *Re Denehy and Superannuation Complaints Tribunal*, [2012] AATA 608. See also *WL v Randwick City Council (GD)*, [2007] NSWADTAP 58 (Austl) (concerning the definition in the *Privacy and Personal Information Protection Act 1998* (NSW) (Austl)); *WL v La Trobe University (General)*, [2005] VCAT 2592 (Austl) (concerning the definition in the (former) *Information Privacy Act 2000* (Vic) (Austl)); Mark Burdon & Paul Telford, "The Conceptual Basis of Personal Information in Australian Privacy Law" (2010) 17:1 Murdoch University Electronic Journal of Law 1.
24. Office of the Australian Information Commissioner, "APP guidelines" (February 2014) at paras B.79-B.88, online: OAIC <https://www.oaic.gov.au/resources/agencies-and-organisations/app-guidelines/archived/chapter-b-app-guidelines-v1.pdf>.
25. Austl *Privacy Act*, *supra* note 1 in the pre-2014 version.
26. That is a number that is assigned to and identifies Mr. Grubb's mobile device when it communicates with the internet.

Uniform Resource Locator ("URL") information[27] and cell tower data.[28] Telstra argued that "the metadata in dispute, which [sat] on its network management systems, [was] not personal information as defined under [section 6 of] the *Privacy Act*".[29] Telstra submitted that Mr. Grubb's identity was neither "apparent nor [could] it reasonably be ascertained from that data"[30] because it could allegedly only be linked to him through difficult and expensive cross-matching between the various databases, systems and networks Telstra operated. In May 2015, the Privacy Commissioner made a determination against Telstra under section 52 of the *Privacy Act*. The Commissioner held that Telstra's ability to provide this kind of data to law enforcement in a large number of cases was "indicative of its ability to ascertain with accuracy an individual's identity from metadata linked to that individual"[31] and further that, in light of Telstra's extensive resources, it was also reasonably able to ascertain it. On that basis, the Privacy Commissioner determined that the metadata in question was "personal information" and the refusal to provide access to it was "in breach of NPP 6.1".[32]

2. The AAT Decision in *Telstra*

On application by Telstra, the Administrative Appeals Tribunal ("AAT") of Australia set aside the Commissioner's determination. In a decision of December 2015, Deputy President Forgie did not primarily engage with the issue of whether Mr. Grubb was reasonably identifiable from the metadata held in Telstra's mobile network systems. Instead, she considered that the words "about an individual" in the definition of personal information raised a threshold issue. She stated that:

> the first step is to ask whether the information or opinion is about an individual. If it is not, that is an end of the matter. If it is, the second step in the

27. That is information that identifies the websites Mr. Grubb visited.
28. That is geo-location data that identifies from where Mr. Grubb used his mobile phone service.
29. *Re Grubb*, *supra* note 21 at para 34.
30. *Ibid*.
31. *Ibid* at para 83.
32. *Ibid* at para 106.

> characterisation process is to ask whether the identity of that individual "… is apparent or can reasonably be ascertained, from the information or opinion".[33]

This finding was surprising because both parties appeared to have proceeded on the basis that the determinative issue was whether Mr. Grubb's identity was apparent or could be reasonably ascertained from the information he sought access to. This assumption was in line with academic commentary that suggested that:

> in most cases, it may not be appropriate to talk of two separate (although cumulative) conditions for making data 'personal'; the first condition can be embraced by the second, in the sense that data will normally relate to, or concern, a person if it enables that person's identification. In other words, the basic criterion appearing in these definitions is that of identifiability – that is, the potential of data to enable [the] identification of a person.[34]

As a result of the *Telstra* litigation, this conventional wisdom no longer applies to Australia.

Forgie DP identified the required characterisation task with the following question: "Is the information about an individual being, in this case, Mr. Grubb or is it about something else"?[35] Adopting this approach, the Deputy President considered that the mobile network data generated by Mr. Grubb's calls or messages was "information about the service it provides to Mr. Grubb but not about him"[36] — notwithstanding the fact that the individual who obtained the service was ascertainable from this information. Such a binary characterisation appeared to disregard the possibility that information — just as it can be about more than one individual — can also be both about an individual and about a service provided to that individual. The decision did not elucidate how the distinction between information about an individual and information about something else was to be drawn, for example, when information is

---

33. *Telstra* AAT, *supra* note 19 at para 97 [emphasis in original].
34. Lee A Bygrave, *Data Privacy Law: An International Perspective* (Oxford: Oxford University Press, 2014) at 129–30 (generally on the definitions of personal in international instruments).
35. *Telstra* AAT, *supra* note 19 at para 111.
36. *Ibid* at para 112 (this was despite the fact that, as the Deputy President accepted, the mobile network data may identify Mr. Grubb when combined with other data).

sufficiently related to an individual so as to be regarded as being "about the individual".

3. The Full Federal Court Decision in *Telstra*

The Privacy Commissioner formed the view that the AAT decision left too much uncertainty regarding the definition of "personal information" and appealed to the Federal Court. Privacy advocates welcomed this move because it provided the prospect of detailed judicial guidance by the Federal Court on this basic concept in Australia's privacy legislation. It was also hoped that the hearing would provide a forum to consider the extensive case law that has developed internationally on the meaning of personal information, and particularly in relation to metadata.

However, in a decision published in January 2017, the Full Court gave short shrift to the Privacy Commissioner's appeal, as well as to the application by two privacy organisations to be heard as *amici curiae*. The main judgment, delivered by Justices Kenny and Edelman (the latter now a judge of the High Court of Australia), held that the appeal concerned only one very "narrow question of statutory interpretation".[37] This was, whether the words "about an individual", in the pre-2014 version of section 6, had any substantive operation. Contrary to the submission on behalf of the Privacy Commissioner, the Court unanimously held that they did.[38] In doing so, Kenny and Edelman JJ (with whom Justice Dowsett agreed in a short judgment) endorsed the view of Forgie DP that the *Privacy Act* establishes a two-stage test for determining that information is personal information.

The Court did not examine whether the AAT had erred in its application of this definition to the facts, because in its view, no appeal ground had raised this for consideration.[39]As a result, it was not reviewed which of Mr. Grubb's mobile phone metadata was personal

37. *Telstra* FCAFC, *supra* note 2 at para 73.
38. *Ibid* at para 80.
39. *Ibid*.

information because it was "about" Mr. Grubb.[40] The fact that the Federal Court concentrated on a narrow, technical point dashed the expectations of privacy professionals that the decision might become a landmark judgment that would fully resolve the issues raised in the AAT decision. Nevertheless, the Court provided some observations on how the definition of "personal information" operates in practice. The Privacy Commissioner decided not to appeal the matter to the High Court, which makes it pertinent to review these comments on the operation of the definition.

Kenny and Edelman JJ stated:

> [t]he words "about an individual" direct attention to the need for the individual to be a subject matter of the information or opinion. This requirement might not be difficult to satisfy. Information and opinions can have multiple subject matters. Further, on the assumption that the information refers to the totality of the information requested, then even if a single piece of information is not "about an individual" it might be about the individual when combined with other information. However, in every case it is necessary to consider whether each item of personal information requested, individually or in combination with other items, is about an individual. This will require an evaluative conclusion, depending upon the facts of any individual case, just as a determination of whether the identity can reasonably be ascertained will require an evaluative conclusion.[41]

4. Practical Consequences of the *Telstra* Litigation

The clarification by the Full Court in *Telstra* that information can have multiple subject matters is welcome because, as discussed above, the approach adopted by the AAT appeared to suggest that the characterisation task is black-or-white — *i.e.* that information will be either about an individual or about something else. The judgment of Kenny and Edelman

---

40. The enactment of the mandatory data retention legislation through the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) (Austl) has put this question beyond doubt because the *Telecommunications (Interception and Access) Act 1979* (Cth) (Austl) now contains an express provision (s 187LA) that metadata required to be retained by the telecommunications provider is taken to be "personal information" for the purposes of the *Privacy Act*.
41. *Telstra* FCAFC, *supra* note 2 at para 63.

JJ also clarifies that the assessment of whether the individual's identity is apparent or can be ascertained must take into account other information with which the information in question can be combined.[42]

However, because of the way the appeal was argued, the Federal Court was not obliged to provide further assistance on how the evaluative task is to be undertaken.[43] In particular, the Court left open, just as the AAT did, the approach to determining the issue of when the link between information and an individual is so tenuous that it cannot be said that the information is "about an individual". Kenny and Edelman JJ gave as an example that the colour of Mr. Grubb's mobile phone was not information they considered to be about him, but they did not explain *why* this was not the case.[44]

The difficulties posed by the characterisation task can be illustrated with the common example of IP addresses. IP addresses were part of the metadata requested by Mr. Grubb, and their characterisation as personal data is a vexed issue also in other jurisdictions. An IP address is allocated by the Internet Service Provider ("ISP") to a subscriber's device so that a particular communication on the internet can be delivered to that device. It is standard practice for many website operators to log the IP addresses of webpage visitors, which raises the question of whether these data logs are personal information and, therefore, fall under data protection legislation. Most connections rely on dynamic IP addresses, which are assigned by the ISP whenever the device connects to the internet and which change regularly. An IP address identifies a specific network device rather than the individual using that device, and dynamic IP addresses may change over time. On that basis, Forgie DP held that a dynamic IP address is not information about an individual because "[t]he connection between the person using a mobile device and an IP address is … ephemeral".[45] The Deputy President did not consider, however, that information, even when it is not directly about an individual, may become personal if it may be linked to an individual through indirect means, such

42. *Telstra* FCAFC, *supra* note 2.
43. *Ibid*.
44. *Ibid*.
45. *Telstra* AAT, *supra* note 19 at para 113.

as through the interrogation of and matching across multiple databases. The decision of the Federal Court suggests that a more nuanced approach may be needed, in particular one that considers whether the information, in combination with other information, is to be regarded as being "about an individual".[46]

It is important to note that the judgment of the Federal Court concerned the definition of "personal information" as it applied before March 12, 2014. Since that date, the definition has been amended to "… information or an opinion about an identified individual, or an individual who is reasonably identifiable …", so as to align it more closely with international legal instruments.[47] NPP 6.1 has been replaced by Australian Privacy Principle 12.1, which adopts different language but is otherwise similar. Despite these changes in the wording, the Court's reasoning is likely to remain applicable because the current definition retains that the information or opinion must be "about an … individual".[48] A key difference between the old and the current definition of personal information is that the individual no longer needs to be identifiable "from the information or opinion". In relation to the old definition, Kenny and Edelman JJ stated that:

> whether information is "about an individual" might depend upon the breadth that is given to the expression "from the information or opinion". In other words, the more loose the causal connection required by the word "from", the greater the amount of information which could potentially be "personal information" and the more likely it will be that the words "about an individual" will exclude some of that information from National Privacy Principle 6.1.[49]

It is unclear what significance these comments have for the purposes of

---

46. As will be discussed below, this is also the position taken under the equivalent provisions in the European Union. See *e.g.* the recent decision of the European Court of Justice in the case of *Patrick Breyer v Bundesrepublik Deutschland*, [2016] EUECJ C-582/14 [*Breyer*] (in relation to website operators) and previously *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, [2011] EUECJ C-70/10 [*Scarlet Extended*] (in relation to ISP providers).
47. ALRC, *For Your Information*, *supra* note 9 at para 6.53.
48. Austl *Privacy Act*, *supra* note 1, s 6(1).
49. *Telstra* FCAFC, *supra* note 2 at para 64 [emphasis in original].

the new definition, which no longer contains the limiting expression "from the information or opinion". It would be concerning if this was understood to attribute an even more significant exclusionary function to the words "about an individual".

Unfortunately, the *Telstra* litigation has provided few new insights on when information is to be considered "personal information" under the *Privacy Act*. In many cases, information will fall clearly either within or outside the definition of "personal information". As far as metadata held by telecommunications providers under the mandatory data retention laws is concerned, the matter was put beyond doubt through statutory deeming provisions. The issue remains live in other contexts, however, such as when businesses or other organisations employ cookie technology to record the IP addresses of website visitors.[50] The classification also continues to be difficult when information (such as internal business data) does not directly identify any individual but can be linked to individuals through indirect means, such as data matching across databases.[51] In cases of doubt, the Office of the Australian Information Commissioner advises organisations and agencies in updated guidance notes to err on the side of caution and treat this information as personal information.[52] This recommendation confirms that the definition of "personal information" — described by the Privacy Commissioner as "arguably the most important term in the *Privacy Act*"[53] — remains in significant respects uncertain.

The Explanatory Memorandum to the *Privacy Enhancement Bill* stated that the amendment "also brings the definition in line with

50. See Robert Slattery & Marilyn Krawitz, "Mark Zuckerberg, the Cookie Monster – Australian Privacy Law and Internet Cookies" (2014) 16:1 Flinders Law Journal 1.
51. See *e.g. Waters v Transport for NSW*, [2018] NSWCATAD 40 (Austl) (considering the collection of personal information by Transport for NSW users of the electronic travel card system "Opal").
52. OAIC, *What is personal information?*, *supra* note 11 at 17.
53. Timothy Pilgrim, "Privacy Awareness Week Launch 2016" Office of the Australian Information Commissioner (16 May 2016), online: OAIC <https://www.oaic.gov.au/media-and-speeches/speeches/privacy-awareness-week-launch-2016>.

international standards and precedents".[54] On that basis, it was expected that the revised definition of personal information would be "interpreted with regard to its counterparts in the EU and elsewhere".[55] This, however, did not occur in *Telstra* FCAFC.[56] In fact, the Full Court was highly critical of the submission of the prospective *amici curiae* that sought to draw the Court's attention to international data protection sources. The Court took particular issue with reliance on overseas materials which concerned "legislation which was worded differently, and based upon a different context and background even though ultimately deriving from the same broadly worded international instruments".[57] Unfortunately, the decision of the Full Court does not seem to acknowledge the degree of international consensus on the basic definitions of data privacy legislation and the fact that Australia's legislation was expressly intended to reflect settled international practice.

It is correct that the international instruments have varying character. The OECD Guidelines maintain a high degree of flexibility and do not seek to provide the adoption of a particular approach. In their Explanatory Memorandum, it is stated that the "precise dividing line between personal data in the sense of information relating to identified or identifiable individuals and anonymous data may be difficult to draw and must be left to the regulation of each Member country".[58]

The next section of the article will explore the Canadian definition of personal information. Of all of the international material presented to the Full Court, the Court was most drawn to Canadian jurisprudence. In particular, the decision in *Canada (Information Commissioner)*[59] was described as "the most relevant, indeed the only potentially relevant, authority".[60] The next section will, therefore, analyse the Canadian

54. Austl, Commonwealth, *Privacy Amendment Bill 2012 Explanatory Memorandum*, *supra* note 10 at 53.
55. Dietze & Allgrove, *supra* note 12 at 328.
56. *Telstra* FCAFC, *supra* note 2 at para 71.
57. *Ibid*.
58. OECD Guidelines, *supra* note 5 at 41.
59. *Canada (Information Commissioner)*, *supra* note 3.
60. *Telstra* FCAFC, *supra* note 2 at para 74.

definition of personal information.

B. Personal Information Under Canadian Law

In Canada, the right to privacy is protected under section 8 of the *Canadian Charter of Rights and Freedoms* ("*Charter*"), which creates a right to be secure against unreasonable search or seizure.[61] There are a number of mechanisms at the federal and provincial level that protect information privacy. The most important federal statutes are the *Privacy Act*[62] and the *Personal Information Protection and Electronic Documents Act*[63] ("*PIPEDA*"). The *Privacy Act* governs the personal information handled by federal government institutions, whereas the *PIPEDA* applies to private sector entities that collect, use or disclose personal information in the course of commercial activities.[64] Both *Acts* define personal information as "information about an identifiable individual",[65] or, in the equally binding French language version, as "tout renseignement concernant un individu identifiable".[66] One of the drivers of the introduction of the

61. The *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11, s 8 [*Charter*].
62. *Privacy Act*, RSC 1985, c P-21 [Canada *Privacy Act*].
63. *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*].
64. There are also a number of provincial statutes, including the *Personal Information Protection Act*, SBC 2003, c 63; *Personal Health Information Protection* Act, SO 2004, c 3, Schedule A; *Loi sur* la protection des *renseignements personnels dans* le *secteur* prive, CQLR c P-39.1.
65. Canada *Privacy Act*, *supra* note 62, s 3 contains further specification for the purposes of this Act, including that the information is "recorded in any form". The definition wording, "information about an identifiable individual that is recorded in any form" is also contained in the *Model Code for the Protection of Personal Information, National Standard of Canada* CAN/CSA-Q830-96 at 1.
66. *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5, s 2(1) [*LPRDE*].

PIPEDA was the European Data Protection Directive,[67] which prohibits the transfer of personal data to third countries that do not have adequate levels of privacy protection for personal information.[68]

The definition of personal information has been central in a number of judicial decisions and determinations of data protection commissioners. In *Dagg v Canada (Minister of Finance)*, Justice La Forest described the definition in the *Privacy Act* as "undeniably expansive" and intending "to capture *any* information about a specific person, subject only to specific exceptions".[69] According to the Privacy Commissioner, the word "about" in the *PIPEDA* definition of personal information means that the information is "not just the subject of something but also *relates* to or *concerns* the subject".[70] Initially, the Privacy Commissioner interpreted this requirement rather narrowly. In a finding released in 2001, the Office of the Privacy Commissioner ("OPC") determined that the information contained in an individual prescription was not associated sufficiently with the physician who wrote it to qualify as

67. EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] OJ, L 281/31 [EC, *Directive 95/46/EC*].

68. See *AT v Globe24h.com*, 2017 FC 114 at para 49; Council of Europe, Article 29 Data Protection Working Party, *Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act*, (2001) 5109/00/EN, WP39.

69. *Dagg v Canada (Minister of Finance)*, [1997] 2 SCR 403 at paras 68–69 [emphasis in original]; see also *Canada (Information Commissioner) v Canada (Commissioner of the Royal Canadian Mounted Police)*, 2003 SCC 8 at para 23 [emphasis in original].

70. Office of the Privacy Commissioner of Canada, "PIPEDA Interpretation Bulletin: Personal Information" (October 2013), online: OPC <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/> [emphasis added].

personal information "about" the physician himself.[71] This conclusion drew heavily on the consideration that a prescription is the outcome of a professional interaction between the involved physician and the treated patient, rather than a description of the physician himself or his activities apart from the fact that he issued the prescription.[72] The OPC further referred to the purpose of the *PIPEDA*, as laid down in section 3, as an *Act* to recognise the right of privacy of individuals which, according to the OPC, does not, when balanced against legitimate commercial purposes, cover information that is only the result of the work activity of an individual.[73] But subsequently, the OPC altered its position to a wider, contextual approach on the scope of the term "about". Apart from the context of information production, the OPC now also takes into account the context of the information collection, its use and disclosure.[74]

In 2003, the OPC decided that sales statistics of individual employees are not only part of the company information a company generates but also reveal the on-the-job performance of individuals and, therefore, also qualify as personal information under the *PIPEDA*.[75] In a comparable case in 2005, the OPC decided that the sales records of independent real estate agents were commercial information connected with their conducted business as well as personal information concerning the individual real

71. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2001-15" (2 October 2001), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2001/wn_011002/>.
72. *Ibid*.
73. *Ibid*.
74. Office of the Privacy Commissioner of Canada, "The Privacy Commissioner of Canada's Position at the Conclusion of the Hearings on the Statutory Review of PIPEDA" (November 2006), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2007/sub_070222_03/> [PCC, "The Privacy Commissioner of Canada's Position"].
75. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2003-220" (15 September 2003), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2003/pipeda-2003-220/>.

estate agent.[76] The OPC also decided that information about property is personal information if it reveals something of a personal nature about an individual.[77] For example, the purchase price of real estate in post-sale advertising could reveal personal traits of the buyer, such as her abilities to pay or to bargain.[78]

Of the judicial determinations, the decision in *Canada (Information Commissioner)*, which the Australian Federal Court referred to, stands out. The matter concerned refusals by the Canadian Transportation Accident Investigation and Safety Board to disclose records in reliance on the "personal information" exception in section 19 of the *Access to Information Act*.[79] Subsection 19(1) of the *Act* prohibits the disclosure of "personal information as defined in section 3 of the *Privacy Act*".[80] The records in question were recordings and/or transcripts of air traffic control communications relating to four aviation occurrences, which were subject to investigations and public reports by the Safety Board.

Justice Desjardins (with whom Chief Justice Richard and Justice Evans agreed) conducted a two-tier test to determine whether data is "personal information".[81] Firstly, the data has to be about an individual. Secondly, the data has to permit or lead to the possible identification of the individual. The two elements "about" and "identifiable individual" have to be met cumulatively for any data to be seen as personal information

---

76. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2005-303" (31 May 2005), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2005/pipeda-2005-303/>.
77. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2006-349" (24 August 2006), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2006/pipeda-2006-349/>.
78. Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2009-002" (20 February 2009), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/pipeda-2009-002/>.
79. *Access to Information Act*, RSC 1985, c A-1.
80. *Ibid*, s 19(1).
81. *Canada (Information Commissioner)*, *supra* note 3.

under Canadian law.[82] In Desjardins JA's view, the two words "about" and "concernant" "shed little light on the precise nature of the information which relates to the individual".[83] However, her Ladyship added that the term "personal information" has to be understood "as equivalent to information falling within the individual's right of privacy" because the purpose of data protection laws is to protect this right of privacy of individuals.[84] Hence, any information can only be understood as "about" an individual when it involves subjects that "engage [an individual's] right to privacy",[85] which is said to connote "concepts of intimacy, identity, dignity and integrity of the individual".[86]

In a statement reminiscent of the Australian Full Court decision, Desjardins JA observed:

> [t]he information at issue is not "about" an individual … the content of the communications is limited to the safety and navigation of aircraft, the general operation of the aircraft, and the exchange of messages on behalf of the public. They contain information about the status of the aircraft, weather conditions, matters associated with air traffic control and the utterances of the pilots and controllers. These are not subjects that engage the right of privacy of individuals.[87]

In *Canada (Information Commissioner)*, the Court ruled that the disputed recordings and transcripts of air traffic control communications indeed enabled the identification of individual people and assisted in a determination as to how they performed their specific tasks in a certain situation. However, the information did not thereby qualify as personal information because the content of the information only affected their

---

82. However, the subsequent decision of Gibson J in *Gordon v Canada (Health)*, 2008 FC 258 appears to elide the two cumulative requirements when it states that ("information [is] "about" a particular individual if it "permits" or "leads" to the possible identification of the individual, whether alone or when combined with information from sources "otherwise available" including sources publicly available" at para 33).
83. *Canada (Information Commissioner)*, *supra* note 3 at para 43.
84. *Ibid* at paras 44–48.
85. *Ibid* at para 53.
86. *Ibid* at para 52.
87. *Ibid* at para 53.

"professional and non-personal nature"[88] and therefore "[did] not match the concept of "privacy" and the values that concept [was] meant to protect".[89] Access to the recordings could therefore not be withheld on the basis of the "personal information" exception. There are also a number of access of information cases at the provincial level that made a distinction between information "about" an individual and information "about" something else,[90] in particular where the information related to an individual acting in their professional or official capacity.

However, another access to information decision of the Federal Court of Appeal a year later demonstrates that these determinations can include fine distinctions. In *Janssen-Ortho Inc v Canada (Minister of Health)*,[91] the Court held that the documents revealing the names and business contact information of employees of the appellant company, as well as the views they expressed to Health Canada on the withdrawal of a prescription drug from the Canadian market, constituted the personal information of these employees. In *Husky Oil Operations Limited v Canada-Newfoundland and Labrador Offshore Petroleum Board*,[92] the Federal Court of Appeal recently suggested that these two decisions are not inconsistent but can be explained by differences in the nature of the information concerned. Justice Montigny (Justice Wood concurring) also affirmed that a purposive approach "best carries out Parliament's intent in adopting the *Access Act* and the *Privacy Act*".[93] However, each of the Acts using the definition of personal information, the *Access to Information Act*, the *Privacy Act* and *PIPEDA* differ in their statutory objectives, particularly in relation to the balance between personal privacy and the

88. *Ibid* at para 54.
89. *Ibid*.
90. See further, Teresa Scassa, "Geographical Information as 'Personal Information'" (2010) 10:2 Oxford University Commonwealth Law Journal 185 at 194–96.
91. *Janssen-Ortho Inc v Canada (Minister of Health),* 2007 FCA 252 aff'd in *Information Commissioner of Canada v Canada (Natural Resources)*, 2014 FC 917.
92. *Husky Oil Operations Limited v Canada-Newfoundland and Labrador Offshore Petroleum Board*, 2018 FCA 10.
93. *Ibid* at para 45.

other objectives they need to be fulfilled. Under a purposive approach to the definition of personal information, it can be argued that the degree of connection required between the information and the individual may need to differ between privacy and access-to-information cases,[94] despite the fact that the *Access to Information Act* adopts the definition in the *Privacy Act*.

In conclusion, the Canadian definitions of personal information in the *Privacy Act* and the *PIPEDA* have the cumulative requirements that the information allows the identification of an individual and that it is also "about" an individual, which requires an evaluation of the link between the information and the individual. The evaluative task is to be undertaken by reference to the purpose of the legislation. Where information does not involve subject-matter that engages an individual's privacy rights, the information is not personal information, even if it may identify an individual. However, this determination can make difficulties in some cases, particularly where it is unclear whether the information affects an individual in a personal capacity.

C. European Union Law

It has been acknowledged that the European Data Protection Directive ("DPD"),[95] which was in force from 1995 until its replacement with the General Data Protection Regulation in May 2018, had a "major transformational impact" on Canadian privacy law.[96] One of the main indicators of the influence of the European Union data privacy regime on Canada is the similarity of the definitions used in the DPD and the *PIPEDA*. According to the Canadian Privacy Commissioner, the "key goal in drafting the definition of personal information in the *PIPEDA* was to ensure that Canadian law was harmonized with European law".[97] The harmonisation of Canadian and European Union law through the

94. Scassa, *supra* note 90 at 197–98 and 209–10.
95. EC, *Directive 95/46/EC*, *supra* note 67.
96. Jennifer McClennan & Vadim Schick, "'O, Privacy' Canada's Importance in the Development of the International Data Privacy Regime" (2006) 38:3 Georgetown Journal of International Law 669 at 671.
97. PCC, "The Privacy Commissioner of Canada's Position", *supra* note 74.

adoption of similar terminology and a similar level of protection was intended to avoid obstacles for transatlantic trade.[98]

The definition of personal information in section 2(1) of the *PIPEDA* as "information about an identifiable individual"[99] picks up not only on the Canadian *Privacy Act* but also on the DPD.

1. Personal Data Under the European Data Protection Directive

The English language version of Article 2 of the DPD provided that:

> "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly …[100]

This article closely resembled the Canadian definition as described above, even though the wording differs slightly. The *PIPEDA* uses the word "about" to describe the necessary link between the information and the individual, while the DPD uses the term "relating to". The similarity between the Canadian and European definition is even more apparent in the respective versions in the French language. In section 2(1) of the *PIPEDA*, personal information is described as "tout renseignement concernant un individu identifiable",[101] whereas the French version of the DPD defined personal data as "toute information concernant une personne physique identifiée ou identifiable".[102] In other words, both jurisdictions made use of the word "concernant" to describe the necessary link.

This definition of personal data within the DPD shows that European Union law also demanded that the information in question must relate to the individual to qualify as personal data. This is also in line with Article

98. *Ibid*.
99. *PIPEDA*, *supra* note 63, s 2(1).
100. EC, *Directive 95/46/EC*, *supra* note 67, art 2(a).
101. *LPRDE*, *supra* note 66, s 2(1).
102. EC, *Directive 95/46/CE du Parlement européen et du conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, [1995] OJ, L 281/31, art 2(a).

2(a) of the *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* ("*Convention 108*"), which defines "personal data" as "any information relating to an identified or identifiable individual".[103] This *Convention* is a Council of Europe treaty to which all member states of the European Union are bound. The DPD (as well as the new *GDPR*) are considered to be acts implementing the *Convention 108*, as the European Union now exercises the legislative power in the field of privacy law which was previously assigned to its member states.[104]

It is unclear what kind of connection between the information in question and an individual is required under the DPD (and now the *GDPR*) to link the information to the individual being. Some scholars assume that under European Union law, the term "relating to" has no discrete meaning and thus is generally fulfilled if the data reveals an identified or identifiable data subject.[105] However, a closer look reveals a more complex situation. A Working Paper on the concept of personal data issued by the Article 29 Working Party (an advisory body established

103. *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 28 January 1981, Eur TS 108 (entered into force 1 October 1985), art 2(a) [*Convention 108*].

104. On the obligations of the EU in relation to treaties signed by its member states, see *International Fruit Company NV v Produktschap voor Groenten en Fruit*, [1971] EUECJ R-54/71 at para 14 *et seq*.

105. On the DPD, see Bygrave, *supra* note 34 at 129–30; Paul M Schwartz & Daniel P Solove, "Reconciling Personal Information in the United States and European Union" (2014) 102:4 California Law Review 877. On the *GDPR*, see Stefan Ernst in Boris P Paal & Daniel A Pauly, eds, *Datenschutz-Grundverordnung* (Munich: Beck, 2017), art 4 at paras 3 *et seq*; Hans-Hermann Schild in Heinrich A Wolff & Stefan Brink, eds, *Beck'scher Online-Kommentar Datenschutzrecht*, 20 ed (Munich: Beck, 2017) (loose-leaf consulted on 30 August 2017), art 4 at paras 3 *et seq*. Both of these commentaries do not consider the term "relating to" in any detail.

under the DPD[106]) provides further guidance as to how this term shall be interpreted.[107] The Working Party stated that "[i]n general terms, information can be considered to 'relate' to an individual when it is *about* that individual".[108]

The Working Party's Opinion first identifies situations in which it is self-evident that information relates to an individual, such as the information contained in one's personnel file or medical file, or images of a person's video interview. It then deals with situations in which it is more difficult to establish the relationship between information and an individual, such as when the data concerns objects, processes or events in the first place, not individuals.[109] Also, in these cases the information can "indirectly" or "in some circumstances" relate to an individual. The Opinion identifies three key elements — the content element, purpose element and result element — and suggests that at least one element is required to establish the necessary connection.[110]

The "content" element is fulfilled when information is given about a particular individual. To determine if the link between the content of the information is close enough to establish such a connection, one has

106. The Article 29 Working Party was an independent advisory body composed of representatives of the data protection supervisory authorities of each Member State, the European Data Protection Supervisor and the European Commission. Its functions included to advise the European Commission and to contribute the uniform application of data protection rules throughout the European Union: *cf.* recital 65 of the DPD. Upon entry into force of the *GDPR*, it has been replaced by the European Data Protection Board, see art 68.

107. Council of Europe, Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, (2007) Working Paper 136 [Opinion 4/2007].

108. *Ibid* at 9 [emphasis in original].

109. *Ibid*.

110. *Ibid* at 10 *et seq*. Similarly, see Information Commissioner's Office, "Determining what is personal data" (2007), online ICO <https://ico.org.uk/media/for-organisations/documents/1554/determining-what-is-personal-data.pdf>; Martin Eßer in Martin Eßer, Philipp Kramer & Kai von Lewinski, eds, *Auernhammer DSGVO BDSG*, 6 ed (Cologne: Carl Heymanns, 2018), art 4 at paras 10–11.

to take into account all circumstances of the case and the meaning of the word "relate" in the general non-juridical linguistic usage.[111]

The "purpose" element is present when the disputed information is used or is likely to be used with the purpose of evaluating or treating an individual on this basis of this information in comparison to other individuals.[112]

Finally, the "result" element can be considered to exist when the use of the information in question is likely to have an impact on the rights and interests of a certain individual. The result does not necessarily have to be of major impact but rather it is sufficient if the individual may be treated differently compared to other individuals as a result of processing that data.[113]

The Working Party gives the example of data concerning a taxi's location which is collected by the taxi company for the purpose of fleet management, providing a better service to the customers and saving fuel by allocating the closest taxi to the customer. The content of the geolocation data, according to the Working Party, is only connected with the taxi cars, not the drivers, and its purpose is only to enhance business processes. However, because of the necessary link between the geolocation information about a taxi and the person who is driving it, the data allows the monitoring of the performance of the taxi drivers themselves. Therefore, under the application of the purpose element, the data is to be considered personal data of the taxi driver.[114]

The overall conclusion from the Opinion is that the Article 29 Working Party interprets the meaning of the term "concerning", as used in the DPD, in a rather wide sense, especially in comparison to the Australian and Canadian understanding of personal information. It does not only include data that is directly about a particular person but also data that is used for the purpose of differential treatment of that person to another or is otherwise likely to have some impact on the rights of a person.

111. Opinion 4/2007, *supra* note 107.
112. *Ibid*.
113. *Ibid* at 11.
114. *Ibid*.

It is, therefore, sufficient if the data allows any conclusions about an individual to be drawn or if the data is collected with such an objective in mind. A further consequence of this broad notion of personal data is that a specific piece of information can represent the personal data of more than just one person at the same time.[115]

2. Personal Data in the Case Law of the European Court of Justice

The case law of the European Court of Justice ("ECJ") supports, at least indirectly, this broad interpretation given by the Article 29 Working Party. In the two decisions of *Scarlet Extended* and *Breyer*, the ECJ dealt with IP addresses and ruled that they are generally protected personal data.[116] In these decisions, the Court did not touch on the issue of whether IP addresses are information relating only to an electronical device, rather than the human being using the device. Instead, the ECJ focused only on the question of whether an individual can be reasonably identified on the basis of an IP address.[117] The focus in both decisions on the criterion of identifiability in the DPD's legal definition of personal data suggests that the necessary link between the data in question and the individual, as required by the criterion in Article 2 of the DPD that the data must "relate to" the individual, is fairly low.

In its interpretation of the term personal information, the ECJ did not expressly consider comparative materials, despite the fact that the definition has international counterparts including international agreements, such as the *Convention 108* as mentioned above, and the law of Canada. This is, however, in line with the other judgments rendered by the ECJ in which the Court showed a reluctance to engage with third

115. *Ibid* at 12.
116. *Scarlet Extended*, *supra* note 46 at para 51; *Breyer*, *supra* note 46 at paras 38 *et seq*.
117. *Breyer*, *supra* note 46 at para 39.

country law in its reasoning.[118]

3. Changes Under the New General Data Protection Legislation

The DPD has been replaced with the new *General Data Protection Regulation* ("*GDPR*") since May 2018.[119] The main driver for this change was the desire to have a uniform level of data protection between the European Union member states which existed under the old DPD. According to Article 288 paragraph 2 of the *Treaty of the Functioning of the European Union* ("*TFEU*"), a European Union regulation is binding in its entirety and directly applicable in all European Union member states.[120]

The English language version of the definition of personal data in Article 4 paragraph 1 of the new *GDPR* remains largely unchanged compared to the DPD and, in particular, still requires the information to be "relating to" an identifiable natural person.[121] Interestingly, the French definition now utilizes the term "se rapportant" instead of the former "concernant" to describe the necessary connection. Although

---

118. *Cf.* Christopher Kuner, "Third Country Law In The CJEU's Data Protection Judgments" *European Law Blog* (12 July 2017), online: European Law Blog <https://europeanlawblog.eu/2017/07/12/third-country-law-in-the-cjeus-data-protection-judgments/>.
119. *GDPR*, *supra* note 4.
120. *Cf. Ibid* at paras 9–13; Paul de Hert & Vagelis Papakonstantinou, "The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?" (2016) 32:2 Computer Law & Security Review 182; Peter Schantz, "Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht" (2016) 69:26 Neue Juristische Wochenschrift 1841.
121. However, it is worth mentioning that the scope of the definition was expanded by lowering the requirements for the identification of an individual. *Cf.* Bert-Jaap Koops, "The Trouble with European Data Protection Law" (2014) 4:4 International Data Privacy Law 250; Bert van der Sloot, "Do Data Protection Rules Protect the Individual and Should They? An Assessment of the Proposed General Data Protection Regulation" (2014) 4:4 International Data Privacy Law 307; Schwartz & Solove, *supra* note 105.

all language versions are equally authentic in European Union law,[122] and therefore the alteration of the wording of an article in one of the language versions might indicate a different meaning, the proposal for the *GDPR* was originally drafted (only) in English. This suggests that no amendment to the legal definition of personal data was intended by the introduction of the *GDPR*. This view is supported by the fact that the Explanatory Memorandum to the draft of the *GDPR* did not address this modification of the definitional text.[123] Like its predecessor, the *GDPR* does not provide clarification of the term "relating to". Recital 26 of the *GDPR* only repeats recital 26 of the DPD and goes to great lengths to explain how to determine whether a person is identifiable but does not explain when the link between the data and an individual is close enough so that data is "relating to" the person.[124]

In conclusion, the most authoritative guidance on this issue remains the working paper of the Article 29 Working Group referred to above. According to this, data "relates to" an individual under European Union data protection law when the data is likely to have an impact on the individual or her position in comparison to others or the data can be used to describe the individual in one way or another. In doing so, the European Data Protection framework only makes low demands on the necessary link between the data in question and an individual to categorise the data as personal data under European Union law. As the Canadian definition of personal information is derived from the European notion, an argument could be made that this understanding would also be a suitable starting point for the interpretation of the Canadian term. However, this position is currently not reflected by Canadian case law interpreting the *PIPEDA* definition, which does not refer to European Union law or its understanding by the ECJ.

---

122. *Cf. Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health*, [1982] EUECJ R-283/81 at paras 18 *et seq*.
123. EC, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final* at 7.
124. *GDPR*, *supra* note 4.

III. How Do Australia, Canada, and the European Union Deal with IP addresses as Personal Information?

This different understanding of the terms "about" or "relating to" in Australian, Canadian and EU law leads to a different comprehension of personal data, respectively personal information which, in turn, affects the scope of application of the respective data privacy regimes. The stricter the requirements for the connection between the information and the affected individual, the narrower the term of personal data or personal information ought to be understood. This, in turn, results in a narrower scope of application of the respective data protection legislation. Accordingly, the European data protection law which requires only a tenuous connection between the two elements has a broader scope of application than the Canadian and Australian data protection law.

This can be clearly illustrated using the example of IP addresses, which form the backbone of electronic communication. IP addresses are used to allow the clear identification of a device in a network by attaching a unique but mostly temporary number to it.[125] The IP addresses assigned to any electronic device in a computer network allow the transmission of data between devices. The three jurisdictions do not share a common understanding of how and when IP addresses should be classified as personal data, as will be shown in this section.

A. Australian Approach

In *Telstra* AAT, the Administrative Appeals Tribunal ruled "that an IP address is not information about an individual".[126] The AAT expressed the view that IP addresses, where they change regularly over the life of the respective device, only identify the respective device itself but are not information "about" the user of the device, because any connection

125. Information Sciences Institute, *Internet Protocol: DARPA Internet Program Protocol Specification*, University of Southern California Working Paper, RFC 791 (Marina del Rey, California: University of Southern California, 1981) at 5–10.
126. *Telstra* AAT, *supra* note 19 at para 113.

between the IP address and the user would be "ephemeral".[127] As the AAT put it, such IP addresses are "not about the person but about the means by which data is transmitted from a person's mobile device over the internet", and, therefore, they are not considered to be personal information under Australia's privacy regime.[128]

While the Federal Court of Australia upheld the decision of the AAT, the appeal was limited to the interpretation of the definition of "personal information", not its application. The Full Court merely held that the words "about an individual" had meaning and required consideration before the subsequent issue arose of whether this information identified that individual.[129] The Federal Court declined to consider whether the AAT applied its definition correctly because this was not raised in the appeal.[130] The Privacy Commissioner decided not to challenge the Full Court decision any further.[131] In its updated guidance on the meaning of "personal information", the issue of IP addresses is not covered.

However, another recent decision of the AAT, issued after the Full Court decision,[132] specifically adopts the reasoning of *Telstra* AAT. In *Freelancer International Pty Ltd and Australian Information Commissioner*, Freelancer operated a website that required user registration and a login by registered users. Freelancer recorded the login IP addresses and associated these IP addresses with particular registrant accounts, including by displaying the IP address used in a session in a Welcome message to the registrant. Nonetheless, the AAT held that while a user's identity might reasonably be ascertained from the information available to the website operator, the IP address information was "not "about" an invidual. It was information "about" the login itself".[133] Like *Telstra*

127. *Ibid*.
128. *Ibid*.
129. *Telstra* FCAFC*, supra* note 2 at paras 62–65.
130. *Ibid* at para 65.
131. Austl, Commonwealth, Office of the Australian Information Commissioner, *Statement on Privacy Commissioner v Telstra Corporation Limited Federal Court decision* (OAIC, 2017).
132. *Freelancer International Pty Ltd and Australian Information Commissioner*, [2017] AATA 2426.
133. *Ibid* at para 69.

AAT, this decision appears to assume that when information, such as an IP address, is about enabling a communication, it cannot also be about the individual engaged in that communication. This is in contrast to the decision of the Full Court, which did not subscribe to the view that the classification task is binary and stated specifically that information can have more than one subject matter.

In summary, while decisions of the AAT, both before and after *Telstra* FCAFC, suggest that IP addresses of electronic devices do not qualify as "personal information" and, hence, are not subject to Australian privacy legislation, these decisions are not completely free from doubt and potentially open to challenge.

B. Canadian Approach

As pointed out above, the Canadian definition of personal information resembles the Australian approach. Nonetheless, its application in practice appears to differ.

The Privacy Commissioner of Canada outlined that IP addresses do not only constitute the technical base for electronic communication but also provide a potential starting point to unlock additional information about the individual who used the electronic device which identified itself via the IP address in question.[134] A study conducted by the Canadian Privacy Commissioner showed that an IP address enabled the creation of a detailed profile of the device user including the geolocation of the user and other web activities as well as e-mail addresses from the user.[135] Therefore, the Canadian Privacy Commissioner classified IP addresses as being sufficiently linked to the individual using them and, therefore,

134. Office of the Privacy Commissioner of Canada, "What an IP Address Can Reveal About You" (May 2013), online: OPC < https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/>.

135. *Ibid*.

qualified them as personal information under Canadian law.[136] The decision of the Supreme Court of Canada in *R v Spencer*[137] provides further illustration of the link between an IP address and an identifiable user. In that decision, the Court decided that internet users may have a reasonable expectation of privacy over their internet activities and that a warrantless police request that an ISP provided identifying information about a subscriber of a particular IP address amounted to an unlawful search and violated the user's section 8 *Charter* rights.[138] Justice Cromwell, writing for the Court, further considered the application of the *PIPEDA* to subscriber information.[139] His Lordship concluded that there was a reasonable expectation of privacy in the subscriber information as the disclosure of such information "will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous" and, therefore, a request by a government institution to reveal this information "amounts to a search".[140]

C. European Approach

Under European Union data protection law, IP addresses normally fall within the scope of personal data. In 2011, the ECJ ruled in *Scarlet Extended* that IP addresses may allow the precise identification of the

---

136. Office of the Privacy Commissioner of Canada, "Metadata and Privacy: A Technical and Legal Overview" (October 2014), online: OPC <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/>; Office of the Privacy Commissioner of Canada, "PIPEDA Case Summary #2001-25" (20 November 2001), online: OPC < https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2001/pipeda-2001-025/>. See also Eloïse Gratton, "Personalization, Analytics, and Sponsored Services: The Challenges of Applying PIPEDA to Online Tracking and Profiling Activities" (2010) 8:2 Canadian Journal of Law & Technology 299 at 300–05.
137. *R v Spencer*, 2014 SCC 43 [*Spencer*].
138. *Charter*, *supra* note 61, s 8.
139. *Spencer*, *supra* note 137 at paras 52 *et seq*.
140. *Ibid* at para 66.

persons using the addresses and, therefore, qualify as personal data.[141] This ruling adopted the opinion delivered by the European Advocate General, which expressed the view that an IP address "may be classified as personal data inasmuch as it may allow a person to be identified by reference to an identification number or any other information specific to him".[142] However, the decision in *Scarlet Extended* related to the introduction of a system for filtering electronic communications by the ISPs and, therefore, by entities which not only had access to IP addresses but — being the provider — also to the necessary data to link the IP addresses with specific users of the service.

The ECJ later expanded this view to IP addresses held by entities other than the ISPs. In *Breyer*, the ECJ stated that the notion of personal data in Article 2(a) of the DPD does not necessarily require that the data on its own allow the data subject to be identified or that the controller of the data must be able to identify the data subject without the help of a third party.[143] Instead, the ECJ ruled that it is sufficient if the data controller in question "has the means which may likely reasonably be used in order to identify the data subject, with the assistance of other persons, namely the competent authority" and other private entities.[144] This criterion is fulfilled if the data controller "has the *legal means* which enable it to identify the data subject with additional data"[145] held by third parties, as long as this does not require "a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant".[146] The ECJ then applied this test to dynamic IP addresses stored by a website operator and came to the conclusion that such addresses allow the identification of the respective device connecting to the internet under the IP address in question because website operators may gain the necessary additional data from the competent authority

141. *Scarlet Extended*, *supra* note 46 at para 51.
142. EC, *Opinion of Advocate General Cruz Villalón delivered on 14 April 2011*, 2011:255 at paras 74–78.
143. *Breyer*, *supra* note 46 at paras 41 *et seq*.
144. *Ibid* at para 48.
145. *Ibid* at para 49 [emphasis added].
146. *Ibid* at para 46.

or the respective ISP. The ECJ finally concluded that under these circumstances, dynamic IP addresses constitute personal data within the meaning of Article 2(a) of the Data Protection Directive.[147]

This finding by the ECJ was met with approval among European scholars[148] so that the qualification of IP addresses as personal data under European Union law is no longer in serious doubt. As the definition of personal data in the *GDPR* remained virtually unchanged from the definition given by the DPD, the findings by the ECJ must be taken to remain applicable under the *GDPR*.[149] In the recent decision of *Benedik v Slovenia*,[150] the European Court of Human Rights held that subscriber information associated with a dynamic IP address fell within the scope of protection of Article 8 (right to private life) of the European Convention on Human Rights. In doing so, the Court adopted the jurisprudence of the ECJ in the *Scarlet Extended* and *Breyer* decisions and also specifically referred to the factually similar decision of the Canadian Supreme Court in *Spencer*.[151]

IV. Conclusion

Despite employing similar definitions of personal data or personal information in their data protection laws, these terms have been interpreted differently by courts in Australia, Canada and the European Union. Part of these differences may also be due to the fact that the courts across these jurisdictions differ in their willingness to consider international materials in their decisions. As a result, the scope of application of the

147. *Ibid* at para 49.

148. *Cf.* Schild, *supra* note 105 at para 19; Heiko Richter, "Datenschutzrecht: Speicherung von IP-Adressen beim Besuch einer Website" (2016) 27:23 Europäische Zeitschrift für Wirtschaftsrecht 912 at 913; Frederik Zuiderveen Borgesius, "The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition" (2017) 3:1 European Data Protection Law Review 130 at 135. This is in line with the prevailing view in legal literature before the ECJ judgments.

149. Borgesius, *ibid* at 136.

150. *Benedik v Slovenia*, No 62357/14 (24 April 2018).

151. *Scarlet Extended*, *supra* note 46; *Breyer*, *supra* note 46; *Spencer*, *supra* note 137.

respective data protection legislation does not coincide. This has the potential to create friction between these jurisdictions by forming an obstacle to the free flow of personal data as most countries only allow the export of personal data to third jurisdictions if an adequate level of protection is guaranteed. If one country establishes a narrower term of personal data than other countries, thereby constraining the scope of its data protection legislation, the export of such data into this country can become problematic. The lack of uniformity has been demonstrated by the example of IP addresses, which Australian law treats differently to Canada and the European Union..

The lack of harmonised interpretation could be addressed if the jurisdictions put more effort into creating alignment between the legal definitions they employ. Initial approaches exist, such as the *Convention 108*, which aims to create a common framework of data protection for its participating countries.[152] Even apart from international treaties, there are also inherent connections between the different jurisdictions. As shown above, the Canadian *PIPEDA* was enacted also against the background of the European data protection legislation and utilized its formulations. Australian case law, in turn, has made some limited references to a Canadian decision in support of its interpretation of Australia's data protection laws. However, against the background of increasingly global data flows, the time has come to develop these connections more systematically and, as the European Court on Human Rights has done in *Benedik*, to adopt a comparative approach to interpreting the key terms of data protection laws wherever possible.

152. *Convention 108*, *supra* note 103.