EDITORIAL

Key Privacy Concepts in the EU and Canada

As in each new edition, I am pleased to present the articles published in this issue of Global Privacy Law Review (GPLR).

The *Articles* section contains two interesting and relevant pieces. They address some of the fundamental concepts of data privacy laws in Canada and the EU, respectively.

Kicking things off, Xavier Dionne of the University of Montreal analyses and aims to define the concept of 'collection of personal information' in Canada.[1] He considers recent amendments to privacy laws, case law, and investigations by privacy commissioners.

Canada's privacy laws are comprised of a complex set of federal and provincial laws. Some are of general application, while others are sector-specific, such as health privacy, anti-spam, and consumer protection laws. Accordingly, the definitions differ across sectors and territories.

The concept of 'collection' of personal information has no consistent definition in Canada. The federal Personal Information Protection and Electronic Documents Act (PIPEDA) defines personal information as 'information about an identifiable individual (*renseignement personnel*)'.[2] It includes any factual or subjective information, recorded or not, about an identifiable individual.[3] However, the 'collection' of personal information is not defined under the PIPEDA. Conversely, under Alberta's Health Information Act 'collect' means to 'gather, acquire, receive or obtain health information'.[4]

Further, Canadian privacy commissioners interpret the concept differently. For instance, Dionne notes that, under Alberta's Freedom of Information and Protection of Privacy Act,[5] the Office of the Information and Privacy Commissioner of Alberta concluded that the concepts of 'collection', 'in its custody or under its control', and 'held by a public body' have the same meaning.[6] Whereas, according to the Information and Privacy Commissioner of Ontario, 'collecting' and 'obtaining and compiling' personal information have different scope and meaning.[7]

Dionne goes on to analyse investigations by the Canadian privacy commissioners and court rulings, to extract a definition of 'collection' of personal information. In particular, he identifies and focusses on three components of the concept: (1) acquisition, (2) intent, and (3) control. He also considers different data collection methods: (1) active primary collection, (2) passive primary collection, and (3) secondary collection.

Accordingly, the author proposes to define the concept as 'gaining control over someone else's personal information, regardless of the collecting party's intent'.[8] This would include 'obtaining, receiving, inferring, or creating, by any means, any personal information', including any unsolicited and unrecorded personal information.[9]

Dionne argues that this broad definition is in line with the purpose of privacy laws, which is to ensure that 'individuals can control their personal information, which is intimately connected to their individual autonomy, dignity and privacy'.[10]

Notes

1 Xavier Dionne, *Collection of Personal Information in Canadian Law*, in this issue at 66.

2 Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5).

3 The Office of the Privacy Commissioner of Canada (OPC), *PIPEDA in Brief* (May 2019), www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief (accessed 17 Apr. 2023).

4 Revised Statutes of Alberta 2000 Ch. H-5, s. 1(1)d.

5 Revised Statutes of Alberta 2000 Ch. F-25.

6 Dionne, *supra* n. 1, at 3.2.1.

7 *Ibid.*, citing Ord. 98-001; Alberta (Justice), 1998 CanLII 18629.

8 *Ibid.*, at 80.

9 *Ibid.*, at 81.

10 *Ibid.*

He also demonstrates that the definition of 'collection' of personal information also has important practical implications and is not only theoretical.

Similarly, in the second article, António Barreto Menezes Cordeiro of the University of Lisbon analyses the meaning of 'personal data', the equivalent of 'personal information', under the European Union's (EU's) General Data Protection Regulation (GDPR).[11]

While the definition of 'personal data' has already been subject to extensive research and case law in the EU, it remains of vital importance for determining whether the GDPR applies to the processing of any set of data.[12] Prof. Menezes also notes that the exact boundaries of personal data continue to raise questions from an application point of view, particularly with regard to the element of 'identifiability'.[13]

The GDPR defines personal data as[14]:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person

The test of reasonable likelihood of identification to determine whether a set of data is considered 'personal' and thus subject to the GDPR is further explained in Recital 26 GDPR. Data is not considered personal if it is 'reasonably likely' that it cannot be linked to an identified or identifiable natural person[15]:

> To determine whether a natural person is identifiable, account should be taken of *all the means reasonably likely to be used*, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. [emphasis added]

According to the Court of Justice of the European Union (CJEU)[16]:

> that would not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it *requires a disproportionate effort in terms of time, cost and man-power*, so that the risk of identification appears in reality to be insignificant. [emphasis added]

Menezes Cordeiro revisits the 'objective' or 'absolute' and 'relative' theories of the definition of personal data. He supports a 'gradual conception of the objective theory' by considering 'the means possessed by all third parties, but limiting our analysis to the knowledge that those particular third parties reasonably have at their disposal'.[17] This requires a 'probabilistic analysis' and considering all relevant factors with reference to specific controllers, processors and third parties, rather than merely in the view of any reasonable person.[18]

Menezes Cordeiro further examines the origins of the concept of personal data and analyse its various elements and boundaries under the GDPR.[19]

In the *Case Note* section, Bernadette Zelger of the University of Innsbruck analyses the CJEU ruling of 8 December 2022 in Case C-460/20 *TU and RE v. Google LLC*.[20] The judgment followed a request for a preliminary ruling by the German Federal Court of Justice concerning the right to erasure under Article 17 of the GDPR.

In this case, two managers of a group of investment companies asked Google to dereference search results, based on their names, which provided links to articles criticizing that group's investment model.[21] The managers

Notes

[11] António Barreto Menezes Cordeiro, *The Personal Data Under the GDPR: Concept, Elements, and Boundaries*, in this issue at 82.

[12] *See* e.g., CJEU, Cases C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, judgment of 10 Oct. 2016; C-101/01, Criminal proceedings against Bodil Lindqvist, judgment of 6 Nov. 2003; and C-40/17, *Fashion ID GmbH & Co.KG v. Verbraucherzentrale NRW eV*, judgment of 29 Jul. 2019.

[13] Menezes Cordeiro, *supra* n. 11.

[14] Article 4(1) GDPR.

[15] Recital 26 GDPR.

[16] CJEU, Cases C-582/14, *supra* n. 12, para. 46.

[17] Menezes Cordeiro, *supra* n. 11, at 90.

[18] *Ibid.*, at 92.

[19] *Ibid.*, at 82.

[20] Bernadette Zelger, *Strengthening the Role of Google? Recent Developments in the Right to Be Forgotten Case Law of the CJEU (TU and RE v. Google LLC, C-460/20)*, in this issue at 93.

[21] CJEU, *Press Release No. 197/22* (8 Dec. 2022) – Judgment of the Court in Case C-460/20, curia.europa.eu/jcms/upload/docs/application/pdf/2022-12/cp220197en.pdf (accessed 17 Apr. 2023).

argued that the articles contained inaccurate claims and requested that Google remove their photos, displayed in the form of thumbnails, from image search results based on their names.[22] Google refused, citing the professional context in which those articles and photos were set and arguing that it was unaware of whether the information contained in the articles was accurate or not.[23]

In its judgment, the CJEU recalled that, in accordance with Recital 4 of the GDPR[24]:

> the right to protection of personal data is not an absolute right but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.

Accordingly, the CJEU ruled that the GDPR expressly provides that 'the right to erasure is excluded where processing is necessary for the exercise of the right, in particular, of information'.

The CJEU further noted that the search engine operator 'cannot be required to play an active role in trying to find facts which are not substantiated by the request for de-referencing, for the purposes of determining whether that request is well-founded'. However, 'where the person who has made a request for dereferencing submits relevant and sufficient evidence capable of substantiating his or her request and of establishing the manifest inaccuracy of the information found in the referenced content ... the operator of the search engine is required to accede to that request'.[25]

Zelger argues that this heightens the role and responsibility of online search engine operators in the context of balancing fundamental rights.[26] She gives a succinct analysis of the ruling, which continues the shaping of the CJEU's case law concerning the right to be forgotten under Article 17 of the GDPR.

Next, Isabelle Brams and Tim Wybitul of Latham & Watkins analyse the CJEU's ruling in Case C-154/21, *RW v. Österreichische Post AG.*[27]

In this case, the CJEU clarified the right of access to personal data and information relating to the processing of such data under Article 15(1) of the GDPR. Under the provision, data subjects have the right to obtain from a data controller information as to[28]:

> *the recipients or categories of recipient* to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations [emphasis added].

The CJEU has ruled that where personal data have been or will be disclosed to recipients, there is an obligation on the part of the controller to provide the data subject, on request, with the actual identity of those recipients.[29]

Brams and Wybitul argue that this has extensive consequences for companies in practice. In particular, the authors note that companies must conduct comprehensive gap analysis and data mapping projects and document such measures to demonstrate compliance.[30]

The CJEU ruled that, as an exception, the controller may indicate only the categories of recipient in question where (1) it is impossible to identify those recipients or (2) the controller demonstrates that the request is manifestly unfounded or excessive.[31]

Brams and Wybitul also warn that this ruling may result in potential mass claims due to alleged violations of the right of access.[32]

Finally, in the *News* column, Alex Roberts of Linklaters put together and edited APAC Privacy News, which tracks significant developments in some of the key Asia-Pacific countries in the area of privacy, data protection, and cybersecurity.[33]

The authors who participated in this piece are David Rountree, David Liao and Eddie Chen (*Allens*) from Brisbane, Australia; Alex Roberts (*Linklaters*) and Tiantian Ke (*Linklaters Zhao Sheng*) from Shanghai, People's Republic of China; Albert Yuen, Yang Fan and Jasmine Yung (*Linklaters*) from Hong Kong SAR; Deepa

Notes

[22] *Ibid.*

[23] *Ibid.*

[24] *Ibid.*

[25] *Ibid.*

[26] Zelger, *supra* n. 20, at 96.

[27] Isabelle Brams & Tim Wybitul, *CJEU Sets Strict Standards for Responding to Data Subject Rights: RW v. Österreichische Post AG, C-154/21*, in this issue at 97.

[28] Article 15(1)(c) of the GDPR.

[29] CJEU, *Press Release No. 4/23* (12 Jan. 2023) – Judgment of the Court in Case C-154/21, curia.europa.eu/jcms/upload/docs/application/pdf/2023-01/cp230004en.pdf (accessed 17 Apr. 2023).

[30] Brams & Wybitul, *supra* n. 27, at 100.

[31] CJEU, *Press Release No. 4/23, supra* n. 29.

[32] Brams & Wybitul, *supra* n. 27, at 100.

[33] Alex Roberts ed., *APAC Privacy News*, in this issue at 101.

Christopher and Anindita Dutta (*Talwar Thakore & Associates*) from Mumbai and Bangalore, India; Yolanda Hutapea, Kevin Eduard Matindas and Salma Izzatii (*Widyawan & Partners*) from Jakarta, Indonesia; Yosuke Unami, Kenji Shimada, Tomohiro Fujii and Kentaro Yamamura (*Linklaters*) from Tokyo, Japan; Adrian Fisher, Jia-Yi Tay and Gabi Lane (*Linklaters*) from Singapore; Sutthipong Koohasaneh, Anuwat Trakulmututa, Nahsinee Luengrattanakorn and Thanasapon Somnuek (*Linklaters*) from Bangkok, Thailand; and Hien Nguyen and Linh Nguyen (*Allens*) from Ho Chi Minh City, Vietnam.

I hope you enjoy reading this new edition of the GPLR!

Ceyhun Necati Pehlivan
Editor-in-Chief