Plugins and POPI: A Critical Discussion into the Legal Implications of Social Plugins and the Protection of Personal Information

H Schultz* and W Freedman**

Online ISSN
1727-3781

P·E·R

Pioneer in peer-reviewed, open access online law publications

Authors

Helga Schultz
Warren Freedman

Affiliation

University of KwaZulu-Natal, Pietermaritzburg Campus
South Africa

Email

schultzhelga06@gmail.com
freedman@ukzn.ac.za

Date Submitted

19 March 2023

Date Revised

15 October 2023

Date Accepted

15 October 2023

Date Published

4 March 2024

Editor Mr M Laubscher

How to cite this article

Freedman W, Schultz H "Plugins and POPI: A Critical Discussion into the Legal Implications of Social Plugins and the Protection of Personal Information" *PER / PELJ* 2023(26) - DOI http://dx.doi.org/10.17159/1727-3781/2023/v26i0a15758

DOI
http://dx.doi.org/10.17159/1727-3781/2023/v26i0a15758

Abstract

Social plugins are one of the many trackers used by companies with an online presence. However, under the *Protection of Personal Information Act* 4 of 2013 (POPI), these trackers have certain legal consequences for internet users. The main reason for this is that trackers tend to process personal information without informing internet users that their data are being collected, the reason for the collection or processing thereof, or who the responsible parties are that are collecting and processing the personal information. The article looks at these issues, amongst others, in the light of a 2019 judgment from the Court of Justice of the European Union or CJEU, namely, Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW e.V.* EU:C:2019:629. Due to the fact that it has had data protection legislation for much longer than other countries or legal jurisdictions, including South Africa, the European Union (the EU) has a substantial body of case law interpreting the data protection legislation of the EU itself as well as that of the individual member states. One of the main instruments used as guidance by the drafters of POPI was *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* (hereafter Directive 95/46). Directive 95/46 was previously considered the gold standard, before *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* (*General Data Protection Regulation*) (hereafter the GDPR) was enacted and Directive 95/46/EC was finally repealed. Since Directive 95/46 was one of the main guiding documents used in drafting POPI, one may expect that the South African courts may turn to the EU and consider how the CJEU has interpreted the similar provisions contained in Directive 95/46, especially since there is very little South African jurisprudence available on POPI. The four main issues under discussion are: who, other than the internet users, has the locus standi to bring an application in terms of POPI? Second, what are the responsibilities of joint responsible parties towards internet users? Third, where there are joint responsible parties, do both need a legitimate interest to process personal information? Lastly, who will be responsible for obtaining the necessary consent to process the personal data?

Keywords

POPI; social plugins; Directive 95/46/EC; GDPR; internet trackers; joint responsible parties; legitimate interests; consent; processing of personal information.

.....

1 Introduction

Internet users frequently search for products online. For example, internet users may be interested in a generator – they click on the various links and look at the various offers. Thereafter, the internet user may move to their favourite news website. As the internet user continues to scroll through the news of the day, adverts appear, showing exactly the same generators that were clicked on in the earlier search. The internet user may open a social media account such as Facebook or Instagram, and there, on the feed, the adverts appear again. This is an example of tracking.[1]

Tracking is a big part of the marketing and advertising strategy of many businesses, companies and other retail outlets. It is a common practice and often occurs automatically.[2] There are different types of trackers that may be utilised by businesses. These include cookies, social plugins, canvas fingerprinting, email or app tracking, and so on.[3] These trackers have taken over the automatic functions of collecting and monitoring an internet user's online behaviour, often with the use of the internet user's internet protocol address or IP address.[4] The IP address is the unique identifier that is assigned to a mobile or computer device that is able to access the internet.[5] The IP address facilitates communication between devices.

When an internet user accesses a website, the IP address of the device s/he is using will communicate with the server on which the website is hosted. This server will first transfer the requested data to the device via the IP address, and second store the IP address on the server and thereby track the number of times the IP address accesses that website.[6]

---

* Helga Schultz. LLB LLM (UKZN). PhD Candidate, School of Law, University of KwaZulu-Natal, Pietermaritzburg Campus, South Africa. A special thanks goes to my dad, Dieter Schultz, for his suggestions as well as for editing this article. Email: schultzhelga06@gmail.com. ORCID: https://orcid.org/0009-0004-9132-9983

** Warren Freedman. B Com LLB (Wits) LLM (Natal). Associate Professor, School of Law, University of KwaZulu-Natal, Pietermaritzburg Campus, South Africa. Email: freedman@ukzn.ac.za. ORCID: http://orcid.org/0000-0002-5400-2883.

1 The opening example is loosely based on Kelly 2019 https://blog.mozilla.org/en/internet-culture/mozilla-explains/what-is-a-web-tracker/, but it was given a more local flavour, relevant to our current South African day and age.

2 Ermakova *et al* "Web Tracking" 4732.

3 For a list as well as a description of the various trackers, see Röttgen "Like or Dislike" 74-76, Ermakova *et al* "Web Tracking" 4735-4737; Veale and Zuiderveen Borgesius 2022 *German Law Journal* 227-231.

4 See Larson 2017 *NC J L & Tech* 317-321; *Breyer v Bundesrepublik Deutschland* (C-582/14) EU:C:2016:779 paras 15-16 (hereafter *Breyer*).

5 I.e. this could be a cell phone, tablet, laptop or desk top computer, or any other device with internet capabilities.

6 Larson 2017 *NC J L & Tech* 317-321.

Tracking an internet user via his/her IP address has the potential to form a complete profile of that internet user, even where the user's name or photograph is not included in the information that has been collected. For example, by collecting and monitoring an internet user's online behaviour, a tracker may uncover the user's religious, philosophical, moral or political, affiliations, beliefs or opinions and thus reveal an identifiable human being.[7] It is not surprising, therefore, that trackers, and especially trackers in the form of social plugins, give rise to a number of privacy concerns. One of the more significant of these concerns is that social media websites such as Facebook and Twitter are able to use social plugins to collect personal information from internet users visiting the websites in those cases in which there is a "like" button embedded, even though the internet user has not given Facebook or Twitter consent or permission to collect such personal information and does not subscribe to those social media networks. Srinivasan explains this point as follows:[8]

> Many third-parties, publishers for example, competed with Facebook on the advertising side of the market. They licensed and installed social plugins as a means to distribute their own content. Surveillance of their own readers, however, could be used against them to undercut the value of and pricing power over their own proprietary readers. Specifically, if Facebook could compile a list of people that read the *Journal*, even those who did not use Facebook, it could simply sell the ability to retarget "*Journal* readers" with ads across the internet for a fraction of the cost that the *Journal* charged ... Facebook used these ... connections [with third party websites] to ... surveil the behavior of people that did not even have Facebook accounts.

The legality of this method of collecting personal data was considered by the Court of Justice of the European Union (hereafter the CJEU) in its seminal judgment in *Fashion ID GmbH and Co KG v Verbraucherzentrale NRW e.V.*[9] The purpose of this article is to critically examine this judgment and to consider its possible implications for the protection of personal information in South Africa. Before doing so, however, it will be helpful to briefly explain what social plugins are and how they function.

Social plugins are web-tracking tools that are embedded in websites. When an internet user opens or visits that website, the social plugin forces the "user's browser to fetch content (e.g. images or scripts) from the social network servers, exposing information about the user's visits to the social network operator".[10] In addition, they also transfer the internet user's IP address to their servers and thus store the internet user's browsing habits.

---

7 Gerlitz and Helmond 2013 *New Media and Society* 1352-1353, Truyens 2016 *EDPL* 135.

8 Srinivasan 2019 *Berkeley Bus LJ* 64, 66; also see the discussion at 62-69.

9 *Fashion ID GmbH and Co KG v Verbraucherzentrale NRW e.V.* (C-40/17) EU:C:2019:629.

10 Acar *et al* 2015 https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf 2.

Social plugins usually work together with cookies to track "the internet user's behaviour (so-called coverage analysis/web analytics)". Cookies may be defined as[11]

> small text files stored in the user's browser, assigning information about the site he came from - for example, if he clicked on an advertising banner on another website - the frequency of visits and his behaviour on the website.

Apart from collecting information about the internet user's online behaviour, cookies also assist in the correct functioning and display of the website on the device from which the website is being viewed.[12]

Social plugins that are embedded in a website often take the form of social network site "like" buttons, e.g. a Facebook "like" button. An important characteristic of social plugins is that they can track an internet user's behaviour irrespective of whether that user has joined the social network site or not, and irrespective of whether that user clicked on the "like" button or not.[13] This is because social plugins may be automatically triggered whenever a website is opened or visited.[14] A troubling consequence of this feature is that an internet user merely needs to open the website for his/her information to be collected.

According to a report prepared for the Data Protection Commission in Belgium, social networks like Facebook regularly make use of social plugins because of their unique ability to link the real identity of an internet user who subscribes to a social network to the user's browsing behaviour; i.e. they link a social network user's browsing (or internet) behaviour to the user's social network account.[15] Put differently, a social plugin is able to connect a social network user's profile with the user's activities on the internet.[16] This is also referred to as third-party tracking.[17] It is important to note, however, that third-party tracking of social network users is not the only concern that data protection authorities have with social plugins. Another and even more pressing concern is that social plugins may be used to track the online behaviour of internet users who do not subscribe to social networks, often without the internet user's consent or knowledge.[18] Where social networking sites track non-subscribed internet users through social plugins through the third-party website, they may not have access to that internet user's name

11 Röttgen "Like or Dislike" 74.
12 Röttgen "Like or Dislike" 74.
13 Röttgen "Like or Dislike" 74, 76-78.
14 Röttgen "Like or Dislike" 74.
15 Acar *et al* 2015 https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf 2. Also see *Fashion ID GmbH and Co KG v Verbraucherzentrale NRW e.V.* (C-40/17) EU:C:2019:629 para 26.
16 Strauß and Nentwich 2013 *Science and Public Policy* 726-727 and 728-729.
17 Gerlitz and Helmond 2013 *New Media and Society* 1352, Acar *et al* 2015 https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf 2.
18 Gerlitz and Helmond 2013 *New Media and Society* 1352-1354.

or any other personal information that the third-party website processes. They will, however, have access to the non-subscribed internet user's IP address and, through that IP address, they will also have access to the user's browsing habits, and possibly his/her location, all of which may be collected, processed and stored by the social network site.[19] As Larson explains, once a social network has a non-subscribed internet user's IP address, it can easily track that internet user by locating where the IP address is situated and, in turn, this can lead to an identifiable individual.[20]

As the brief discussion set out above indicates, social plugins have the potential to infringe on an individual's right to privacy and especially the right to privacy of personal data or information. Personal data protection laws have been passed in an increasing number of jurisdictions, including the European Union (hereafter the EU) and South Africa, in order to give effect to this right. The extent to which social plugins comply with key aspects of the EU data protection laws and thus the legal consequences of these trackers for data subjects (in this case, internet users) and controllers was considered by the CJEU's second chamber in *Fashion ID*.[21] As already mentioned, the legal implications of this judgment for the protection of personal privacy in South Africa are discussed in this article.

Apart from the introduction, this article is divided into four sections. The legislative framework governing the protection of personal data in the European Union is set out and briefly discussed in the second section. This brief discussion is followed in section three with a detailed examination of the facts and findings of the CJEU in *Fashion ID*. After examining the judgment in *Fashion ID*, the article turns its focus onto South African law. The relevant provisions of the *Protection of Personal Information Act* are set out in section four and then applied to the issues raised in *Fashion ID* in section five. Some concluding remarks are made in section six.

2 Directive 95/46 and the GDPR

In 1995 the European Parliament and the Council of the European Union enacted Directive 95/46.[22] This Directive was aimed, *inter alia*, at protecting the right to privacy and especially the right to the privacy of personal data by creating a standardised framework that Member States could transpose

19 Srinivasan 2019 *Berkeley Bus LJ* 62-69.

20 Larson 2017 *NC J L & Tech* 318-319. Also see Strauß and Nentwich 2013 *Science and Public Policy* 727.

21 *Fashion ID GmbH and Co KG v Verbraucherzentrale NRW e.V.* (C-40/17) EU:C:2019:629 (hereafter *Fashion ID*).

22 *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) (hereafter Directive 95/46).

into their own respective legal jurisdictions.[23] More than twenty years later, in 2018, Directive 95/46 was repealed and replaced with the GDPR, which remains in force.[24] The purpose of this section is not to discuss the two legislative instruments in detail, but rather to focus on their overall objectives. The scope and content of the definition of "personal data" in each legislative instrument will also be discussed.

When the application under *Fashion ID* was launched Directive 95/46 was still in force and consequently the CJEU based its decision primarily on this legislative instrument. Given, however, that Directive 95/46 had been repealed and replaced by GDPR by the time the matter was heard and the judgment was handed down, the CJEU relied on the GDPR to support the manner in which it interpreted some of the provisions of Directive 95/46. Even though the CJEU referred to the GDPR, it is important to note that the GDPR does not apply retrospectively and that the CJEU's final findings were limited to Directive 95/46.

2.1 Directive 95/46

The aims and objectives of Directive 95/46 are set out in the preamble, which contains a long list of recitals. The main objective was to protect the fundamental rights and freedoms of data subjects,[25] especially the right to privacy. Apart from protecting the right to the privacy of data subjects, another key objective was to create a framework in terms of which the legitimate processing[26] and the cross-border transfer[27] of personal data could take place. These objectives are expressed most clearly in recitals 2 and 10 of Directive 95/46, which read as follows:

> Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute

---

23 Recitals 3, 4, 7, and 10 of Directive 95/46. Regarding the transposition of directives, see generally Duina 1997 *Int'l J Soc L* 155-156.

24 *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* (2016) (*General Data Protection Regulation*) (hereafter the GDPR).

25 Ironically, Directive 95/46 and the GDPR do not directly define "data subject". Both legislative instruments combine the definition of "data subject" with "personal data". The relevant part of both reads as follows: "information relating to an identified or identifiable natural person ('data subject')", see Art 2(a) of Directive 95/46, Art 4(1) of the GDPR. Hence, it is safe to conclude, for the purposes of Directive 95/46 and the GDPR, that a data subject can only be an identifiable natural person, unlike s 1 of the *Protection of Personal Information Act* 4 of 2013 (hereafter POPI), which defines "data subject" to include both natural and juristic persons.

26 Recital 2 of Directive 95/46.

27 Article 1 of Directive 95/46. Also see *Rechnungshof v Österreichischer Rundfunk and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk* (C-465/00, C-138/01 & C-139/01) EU:C:2003:294; *Lindqvist* (C-101/01) EU:C:2003:596.

> to economic and social progress, trade expansion and the well-being of individuals; ...
>
> Whereas ... the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of [EU] law ... .

Recital 10 requires that the EU Member States must ensure the protection of the right to privacy as provided in Article 8 of the *European Convention for the Protection of Human Rights and Fundamental Freedoms*.[28] Article 8(1) of the Convention provides in this respect that "[e]veryone has the right to respect for his private and family life, his home and his correspondence". Article 8(2) goes on to provide that these rights may be limited in terms of the law, where it is necessary in a democratic society, and where it is in the interests of "national security, public safety or the economic well-being of the country", the "prevention of disorder and crime", the "protection of health or morals", or the "protection of the rights and freedoms of others".

The main thrust of Directive 95/46 was the lawful processing of personal data,[29] whilst still protecting the privacy of data subjects. It also made provision for a number of safeguards as well as penalties in cases where those processes were breached and the rights of data subjects were infringed.[30] Directive 95/46 also promoted the unhindered flow of data between EU Member States and between EU Member States and non-EU Member States.[31] Further important features to note are that key concepts were defined, along with the functions of all of the key role-players. The

---

28 *European Convention for the Protection of Human Rights and Fundamental Freedoms* (1950) (hereafter the European Convention).

29 The lawful or legitimate processing of personal data/information encompasses two aspects. First, processing refers to all actions or activities or operations or sets of operations which are executed on/involve personal data, irrespective of whether these processes are automatic or not. These activities include but are not limited to collecting, receiving, recording, organising, collating, storing, updating, modifying, retrieving, altering, consulting, using, disseminating (i.e. transmitting, distributing, or making available), merging, linking, restricting, degrading, erasing or destroying information. See the definitions in Art 2(b) of Directive 95/46, Art 4(2) of the GDPR and s 1 of POPI. Also see De Stadler *et al Over-Thinking the Protection of Personal Information Act* 84. Second, lawful or legitimate processing occurs where the person processing the personal data/information (referred to as the controller, processor or responsible party) adheres to the conditions or principles or rules as provided in either Directive 95/46, the GDPR or POPI (depending on where the person processing is situated, i.e. the European Union (EU) or South Africa) when processing the personal information or data. These conditions or principles include accountability, processing limitation, purpose specific, further processing limitation, information quality, openness, security safeguards, and data subject participation. See s 4(1) of POPI.

30 However, there are limited exceptions, which need not necessarily be discussed in this article. See Art 13 of Directive 95/46, which contains the exceptions or exemptions.

31 Recital 8 of Directive 95/46.

Directive also provided that data subjects must be notified when their personal data are being processed.

Insofar as the concept of "personal data" itself was concerned, Directive 95/46 defined this notion as[32]

> any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Apart from the fact that the concept of personal data applied only to natural persons, it is important to note that the EU defined the concept of "personal data" as widely as possible, as can be seen from the inclusion of the words "any information" in the definition. This broad definition was embraced by CJEU so as to provide the widest possible protection for a data subject's personal data,[33] as can be seen in *Breyer v Bundesrepublik Deutschland*. In this case the CJEU held that even though they were not specifically listed in the Directive, online identifiers such as IP addresses fell within the definition of personal data and thus within the scope of the Directive.[34]

2.2 GDPR

As mentioned above, Directive 95/46 was replaced by the GDPR in 2018. Some of the GDPR's provisions overlap with those in Directive 95/46, while others go further and expand on the Directive. The GDPR also contains some entirely new provisions. The origin of the GDPR may also be traced back to the increasing emphasis placed on the uniform application of data protection laws throughout the EU.[35] This goal is highlighted in recital 3 of the GDPR, which states that it seeks "to *harmonise* the protection of fundamental rights and freedoms of natural persons in respect of processing activities" (own emphasis).[36]

The GDPR has essentially the same aims and objectives as Directive 95/46. These are formulated most clearly in recital 4 of the GDPR, which reads as follows:

---

32 Article 2(a) of Directive 95/46. Note, Art 4(1) of the GDPR has a similar definition for "personal data".

33 A complete discussion of this topic is beyond the scope of this document. For a summary of the cases that deal with the concept of "personal data", see Docksey and Hijmans 2019 *EDPL* 302-304.

34 *Breyer* paras 15-16.

35 Recitals 9 and 13 of the GDPR. In recital 9 the EU legislators recognised the original sound approach that was taken in Directive 95/46, however, application throughout the EU was fragmented, which led to uncertainty and "significant risks" where the protection of natural persons was concerned, especially in the light of online activities.

36 Recital 3 of the GDPR.

> The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.

Unlike Directive 95/46, the GDPR does not refer to the European Convention, but rather to the subsequently enacted EU Charter.[37] While Article 7 of the EU Charter guarantees the right to "respect for private and family life" along the same lines as Article 8 of the European Convention, Article 8 of the EU Charter goes a step further and also guarantees the right to "protection of personal data". It provides in this respect that an individual's personal data may be processed only in terms of a fair and specified process based on consent and other legitimate interests, providing for access and the correction of personal data where necessary, and that this must be monitored by an independent authority. Apart from expressly providing for the legitimate processing of personal data, the GDPR also provides a mechanism for the cross-border transfer of data between EU Member States and third countries, like Directive 95/46.[38]

The definition of personal data in Article 4(1) of the GDPR is somewhat similar to that in Directive 95/46. One of the most significant difference is that it includes an expanded list of "identifiers", which are as follows:

> a name, an identification number, location data, an online identifier or … one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[39]

The express inclusion of "online identifiers" as one of the myriad types of personal data in Article 4(1) gives effect to the judgment of the CJEU in *Breyer*. As noted above, in this case the CJEU adopted a broad approach to the phrase "any information" and held that online identifiers, including IP addresses, fall into the definition of personal data in Directive 95/46.[40] The

---

37 *Charter of Fundamental Rights of the European Union* (2000) (hereinafter the EU Charter).

38 Recitals 3 and 10 of the GDPR.

39 This is enough to note for this discussion – it is likely that the courts (i.e. the EU Member States' national courts and both the Court of Justice of the European Union (the CJEU) and the European Human Rights Court) will keep the wide application of the definition of "personal data" to ensure that data subjects' privacy rights are completely protected – see Docksey and Hijmans 2019 *EDPL* 313-316.

40 *Breyer* paras 15-16.

express inclusion of online identifiers in Article 4(1) is also in keeping with recital 6, which recognises the rapid global advancement in technology.

Once again the GDPR protects only natural persons, as the following reference appears in the definition of "personal data", namely "identifiable natural person ('data subject')".[41]

3 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW e.V.*

The appellant, Fashion ID, was a German online clothing retailer. It embedded into its website a social plugin from Facebook Ireland Ltd (hereinafter Facebook) in the form of a "like" button. The button allowed visitors to Fashion ID's website to "like" content and thereby automatically post this on Facebook.[42] Apart from allowing visitors to "like" the content of Fashion ID's website, however, the social plugin automatically collected the IP addresses and browsing habits not only of those visitors who subscribed to Facebook but also of those visitors who did not subscribe to Facebook irrespective of whether they clicked the "like" button or not. In other words, there was no need for a visitor to join Facebook or click the "like" button for that person's data to be collected. After these data had been collected by the social plugin they were transferred to Facebook's servers where they were analysed and stored for commercial purposes.[43]

The respondent, *Verbraucherzentrale NRW e.V*., was the North Rhine Westphalia's consumer protection centre. It argued that the social plugin breached the provisions of Directive 95/46 and brought legal proceedings against Fashion ID in the *Oberlandesgericht*, Düsseldorf (i.e. the Higher Regional Court, Düsseldorf).[44] The *Oberlandesgericht*, Düsseldorf halted proceedings and referred various questions to the CJEU, requesting

41 Article 4(1) of the GDPR. See the more detailed discussion in the footnotes above, under "2.1 Directive 95/46".

42 Hereafter Facebook.

43 *Fashion ID* paras 25-31. For a general discussion on the case, see Zalnieriute and Churches 2020 *MLR* 861-876.

44 *Fashion ID* para 32.

guidance on the interpretation of Articles 2,[45] 7,[46] 10,[47] and 22 to 24[48] of Directive 95/46 in the light of the facts. As was explained above, the GDPR was enacted as the legal proceedings were taking place.[49] The CJEU answered some of the questions with reference to both Directive 95/46 and the GDPR.[50] Apart from Fashion ID and the *Verbraucherzentrale NRW e.V.*, Facebook[51] participated in the proceedings as an intervening party.[52]

The questions that the *Oberlandesgericht*, Düsseldorf referred to the CJEU were as follows:

First, whether a consumer protection centre had standing to bring a matter before the courts in terms of Directive 95/46.

Second, whether Fashion ID could be classified as a joint controller together with Facebook with respect to the social plugin.

Third, whether Fashion ID's decision to embed the social plugin on its website fulfilled the requirement of a legitimate interest.

---

45 Article 2 of Directive 95/46 provides for the definitions, some of which have been discussed above, as a part of the background, and others that are more related to the issues in *Fashion ID* to be discussed hereunder.

46 Article 7 of the Directive 95/46 provides for the "Criteria for making data processing legitimate". Specifically, *Fashion ID* was concerned with the application of Art 7(a) (i.e. the unambiguous consent of the data subject) and (f) (i.e. the legitimate interests pursued by the controller to process the data, which must be communicated to the data subject) of Directive 95/46.

47 Article 10 of Directive 95/46 is headed "Information in cases of collection of data from the data subject". This article requires that the controllers on collecting the personal data from the data subject that is to be processed must provide to the data subject (a) their identity or the identity of their representative; (b) the reason or purpose for which the personal data will be processed; and (c) further information that is considered necessary, such as whether the personal data will be transmitted to a third party, whether it is compulsory or voluntary to provide the data, and any consequences that follow if the data are not provided, as well as the rights of access to and the rectification of the personal data.

48 Collectively, these three articles are situated in Ch III of Directive 95/46, and they provide first for the judicial remedies of the data subject where the general rules for the lawful processing of data are breached (Art 22), second for the liability of the responsible party to the data subject where the processing rules and data subject's rights are breached (Art 23), and third, the sanctions that may be imposed on the responsible party where it has beached the processing rules or the data subject's rights (Art 24).

49 *Fashion ID* para 3.

50 *Fashion ID* para 1.

51 Specifically, Facebook Ireland Ltd, as the representative in the EU of the United States parent company Facebook Inc (now Meta Platforms Inc).

52 The second intervening party was the *Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*, i.e. the North Rhine-Westphalia Data Protection Authority or the State Data Protection Authority for the German State of North Rhine-Westphalia.

Fourth, whether Fashion ID, as the operator, was obliged to inform visitors to its website that third parties were collecting their data and obtain their consent to do so.

Each question will be discussed in turn.

3.1 Locus standi

As pointed out above, the first issue that the CJEU had to consider was whether a consumer protection centre[53] had standing to bring the matter before the courts in terms of Directive 95/46,[54] even though this was permitted in terms of national German legislation.[55] The CJEU began its analysis by noting that the overall aim of Directive 95/46 was to provide a high level of data protection where personal data are being processed.[56] This high level of data protection, the CJEU held, included national legislation that provides for organisations to monitor and approach courts where they notice that companies are in breach of Directive 95/46.[57] After arriving at this conclusion, the CJEU turned to examine Articles 22 to 24 of Directive 95/46. Following this examination, the CJEU noted that there was nothing in the Directive that precluded consumer protection centres from enforcing its provisions. Instead, the provisions of the Directive encouraged EU Member States to adopt "suitable measures" to enforce the provisions of Directive 95/46.[58] These special measures included the power to confer *locus standi* on consumer protection centres such as the *Verbraucherzentrale NRW e.V*.[59]

Having found that the Directive does confer locus standi on consumer protection centres, the CJEU turned to examine the manner in which the GDPR dealt with the issue of locus standi and especially the locus standi of consumer protection centres. Article 80(2) of the GDPR expressly permits consumer protection centres to actively enforce data subjects' rights and

---

53 Such as *Verbraucherzentrale NRW e.V.,* i.e. the North Rhine Westphalia's consumer protection centre.

54 Articles 22-24 of Directive 95/46.

55 *Fashion ID* para 43. The relevant provision in the national German legislation is § 3(1) of the *Gesetz gegen den unlauteren Wettbewerb* (Law against Unfair Competition) (hereafter the UWG) which provides: "Unfair commercial practices shall be prohibited." The UWG further provides that unfair commercial practices will include any statutory provisions which "regulate market behaviour and the interests of market participants [i.e. in this instance data subjects]", including where a breach infringes or adversely impacts "on the interests of consumers [i.e. data subjects], or other market competitors" (see § 3a). § 8(1) of the UWG provides that an order to desist or cease or completely prohibit such practices may be granted. § 8(3) provides that applications for the § 8(1) orders may be lodged by the relevant authorities as listed in the specified German and EU legislative instruments.

56 *Fashion ID* paras 56-60.

57 *Fashion ID* para 57.

58 *Fashion ID* paras 58-59.

59 *Fashion ID* para 59; see also *Lindqvist* (C-101/01) EU:C:2003:596 para 97.

freedoms. It followed, therefore, that these centres could approach the courts where this was necessary in the interests of data subjects (i.e. consumers).[60] These provisions, the CJEU held, supported its interpretation of Directive 95/46 and thus reinforced its finding that Directive 95/46 did not preclude consumer protection centres from approaching the courts to protect the rights of consumers (i.e. data subjects).[61] In the light of these findings, the CJEU concluded that consumer protection centres were not precluded by Directive 95/46 from approaching the courts to enforce its provisions.[62]

3.2 Joint controllers

The second issue that the CJEU had to address was whether Fashion ID was a joint controller with Facebook in respect of the social plugin. Insofar as this issue was concerned, it is important to keep in mind that at the same time that the internet user's IP address was retrieving the relevant content information from Fashion ID's servers, the social plugin was storing the browsing habits of that internet user and transferring this data to Facebook's[63] servers automatically.

In terms of Article 2(d) of Directive 95/46, a "controller" was defined as:

> the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or [EU] laws or regulations, the controller or the specific criteria for his nomination may be designated by national or [EU] law.

A careful examination of this wide definition shows that two or more persons may be classified as controllers when they have jointly determined that personal data should be processed, albeit at differing stages.[64] It is important to determine who the controller(s) is (or are) in order to decide who is (or are) responsible for any breach or infringement of the provisions of Directive 95/46 (or even the GDPR).[65]

---

60 See also recital 19 of the GDPR.

61 *Fashion ID* para 62.

62 *Fashion ID* para 63. Compare with the decision in *Facebook Ireland Ltd v Gegevensbeschermingsautoriteit* (C-645/19) EU:C:2021:483, where the court held that for the effective protection of privacy during the processing of personal data a non-leading authority may approach the courts in order to enforce the provisions of the GDPR.

63 Facebook Ireland Ltd is the European representative of the main company Facebook Inc situated in the United States of America – see *Schrems v Data Protection Commissioner* (C-362/14) EU:C:2015:650; *Data Protection Commission v Facebook Ireland and Maximillian Schrems* (C-311/18) EU:C:2020:559.

64 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (C-210/16) EU:C:2018:388; *Fashion ID* para 73. Also see Art 26 of the GDPR.

65 Globocnik 2019 *IIC* 1036.

In its previous judgment in *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH,*[66] the CJEU had held that both the administrator of a fan page hosted on a social network site and the host (i.e. Facebook) were the joint controllers of the content of that fan page.[67] Based on the authority of this judgment and the very wide definition of a "controller" in Article 2(d) of Directive 95/46, the CJEU held in *Fashion ID* that both Fashion ID and Facebook were jointly responsible for the social plugin.[68]

Even though they were jointly responsible for the social plugin, the CJEU held further, Fashion ID's responsibility was limited only to those processing operations that were jointly determined with Facebook. By embedding the social plugin, Fashion ID had made the decision to process (i.e. collect and store) personal data, and had played a role in transmitting personal data to Facebook.[69] However, Fashion ID could be held responsible only for the processing of personal data that took place on its servers.[70] It could not be held responsible for the processing of personal data that took place on Facebook's servers.[71]

The reasons for the abovementioned finding of the CJEU are the following. First, processing refers to a number of operations, whether automatic or not, and includes collecting, storing, and transmitting personal data, to name just a few operations.[72] Second, both Fashion ID and Facebook profited economically through the placement of the embedded social plugin, through free advertising, i.e. internet users "liking" content on Fashion ID's website and thereby promoting the same on their Facebook personal feeds, but also through the easy and free collection of personal data which may be used (processed) for commercial purposes such as paid advertisements without the consent of the data subject (i.e. the internet user).[73] Put differently, the data subject has not consented to the collection and use of his/her personal data for the commercial interests of either Fashion ID or Facebook.[74]

---

66 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* (C-210/16) EU:C:2018:388 (hereafter *Wirtshaftsakademie*).

67 See generally Lindroos-Hovinheimo 2019 *Info & Comm Tech L* 229-234, Globocnik 2019 *IIC* 1036.

68 *Fashion ID* paras 68-70; *Wirtschaftsakademie* para 38; *Meta Platforms Ireland Ltd v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.* (Case C- 319/20) EU:C:2022:322. Note Veale and Zuiderveen Borgesius 2022 *German Law Journal* 246.

69 Globocnik 2019 *IIC* 1307.

70 *Fashion ID* paras 75, 78.

71 *Fashion ID* para 82.

72 *Fashion ID* paras 71-72; Art 2(b) of Directive 95/46.

73 *Fashion ID* para 80.

74 Zalnieriute and Churches 2020 *MLR* 862-863, Globocnik 2019 *IIC* 1039-1040.

In summary, the CJEU held that both Fashion ID and Facebook were the joint controllers of the social plugin. However, Fashion ID was responsible only for the data that was collected and disclosed from its visitors, and not for the further processing thereafter, which included those persons who did not have a Facebook account.[75]

3.3 Processing in terms of the legitimate interests of the website operator

The third issue the CJEU had to deal with was whether Fashion ID's decision to embed the social plugin on its website served its legitimate interests[76] in terms of Article 7(f) of Directive 95/46, read with the relevant provisions of Directive 2002/58.[77] Article 7(f) of Directive 95/46 read as follows:

> processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).

Before turning to consider the provisions of Article 7(f), the CJEU noted that in terms of Article 5(3) of Directive 2002/58[78] a party who wishes to store or access stored personal data kept in the terminal equipment of a subscriber (i.e. the data subject)[79] may do so only after obtaining the consent of that subscriber and that the subscriber must be provided with "clear and comprehensive information" before giving such consent. For the purposes of this case, however, the CJEU held, it was not necessary for it to decide

---

75 *Fashion ID* para 85. Specifically regarding joint controllers and a comparison between Directive 95/46 and the GDPR, see Zalnieriute and Churches 2020 *MLR* 869-875.

76 In terms of Directive 95/46, there are two reasons which may be provided for the processing of personal data, namely (1) a legitimate interest, or (2) the consent of the data subject. Where controllers are unable to prove that they have a legitimate interest in the processing of the personal data, i.e. a legal or economic interest, they will need to rely on having received the consent of the data subject. In terms of data processing, it is far easier to prove a legitimate interest than the consent of the data subject, as consent amounts to "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed" (Art 2(h) of Directive 95/46). See Globocnik 2019 *IIC* 1040.

77 *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector* (2002) (*Directive on Privacy and Electronic Communications*) (hereafter Directive 2002/58).

78 *Fashion ID* para 89. Directive 2002/58 (also referred to as the e-Privacy Directive) relates to cookies and deals with the storing of data on terminal devices such as mobile phones and computers. The data is stored in the form of cookies. It also deals with how consent should be obtained herein for the accessing and use of these cookies. See Globocnik 2019 *IIC* 1039.

79 Terminal equipment refers to information stored on a computer, mobile phone, etc. See Globocnik 2019 *IIC* 1039.

whether the data subjects (i.e. the internet users who visited Fashion ID's website) had in fact been given clear and comprehensive information and thus validly consented to their personal data being processed. Instead, that question would have to be answered by the referring court.[80]

Having found that it was not necessary to consider whether the provisions of Article 5(3) of Directive 2002/58 had been satisfied, the CJEU turned to focus on Article 7(f) of Directive 95/46. In this respect the CJEU began by confirming that, subject to the exceptions in Article 13, the processing of personal data must take place in accordance with the provisions of Chapter II of Directive 95/46, which is titled "General rules on the lawfulness of the processing of personal data".[81] Article 7(f) provides in this respect: first, that personal data may be lawfully processed by the controller when such processing serves the legitimate interests of the controller and it does not infringe on the fundamental rights and freedoms of the data subject, and especially the fundamental right to the protection of personal data. Secondly, that personal data may be lawfully processed by a third party (or parties) where that data has been divulged to them and such processing does not infringe on the fundamental rights and freedoms of the data subject, and especially the fundamental right to the protection of personal data.[82]

After setting out these principles, the CJEU held that in a case such as this one, where a social plugin embedded on Fashion ID's website by its operators not only requests content from Facebook's servers but automatically collects and transmits a visitor's personal data to Facebook's servers, both Fashion ID and Facebook as joint controllers must have a legitimate interest that justifies the collection of such data.[83]

3.4 The need to obtain consent to process the personal data

Regarding the need to obtain consent, the fourth and final issue before the CJEU had two aspects. The first aspect dealt with consent and the second with notification. Insofar as the first aspect was concerned, the CJEU had to decide, in the light of Articles 2(h) and 7(a) of Directive 95/46, who was responsible for obtaining the consent of a visitor to Fashion ID's website. Was it Fashion ID, as the operator of the website, or Facebook, as the provider of the social plugin? Insofar as the second aspect was concerned,

---

80 *Fashion ID* para 89; Globocnik 2019 *IIC* 1039; Zalnieriute and Churches 2020 *MLR* 868.

81 *Fashion ID* para 93; see also *Google Spain SL, Google LLC v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* (C-131/12) EU:C:2014:317 para 71.

82 *Valsts Policijas Rīgas Reģiona Pārvaldes Kārtības Policijas Pārvalde v Rīgas Pašvaldības SIA 'Rīgas Satiksme'* (Case C-13/16) EU:C:2017:336 para 28; *Fashion ID* para 95. The CJEU did not provide much detail in respect hereof.

83 *Fashion ID* paras 96-97.

the CJEU had to decide, in terms of Article 10 of Directive 95/46,[84] who was responsible for notifying visitors of the fact that their data were being collected by a third party and what form that notification had to take.

Insofar as the first aspect was concerned, Article 2(h) defined the concept of a "data subject's consent" as

> any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 7(a), in turn, provided that personal data may be processed only where "the data subject has unambiguously given his consent". In the light of these provisions, the CJEU held that even though Fashion ID's responsibility was limited, it was nevertheless obliged not only to notify its website visitors of the fact that their data was being collected by a third party, but also to provide them with a means of withholding their consent to their data being processed via an embedded social plugin.[85]

The CJEU based its decision on the grounds that by agreeing to embed the social plugin on its website, Fashion ID could be classified as a joint controller together with Facebook of that plugin. As such, Fashion ID was required not only to obtain the consent of its visitors but also to notify them that their personal data were being collected and transmitted to a third party.[86] In addition, the CJEU held, Fashion ID was obliged to obtain this consent before the personal data of its visitors were collected and transferred to Facebook.[87] Despite the fact that it was a joint controller together with Facebook, the CJEU held further, that the obligation to obtain consent and notify visitors rested on Fashion ID and not Facebook. This is because the process of collecting a visitor's data began when that visitor opened Fashion ID's website and not Facebook's.[88]

In summary, the CJEU confirmed that Fashion ID was obliged to obtain consent from and notify visitors to its website that their personal data would be collected and transferred to a third party because the process was triggered automatically whenever a visitor opened the website. The CJEU emphasised, however, that these obligations were limited to those processes for which Fashion ID was responsible.[89]

---

84 Article 10 of Directive 95/46 is titled: "Information in cases of collection of data from the data subject".

85 *Fashion ID* para 100.

86 *Fashion ID* para 101.

87 *Fashion ID* para 102.

88 *Fashion ID* paras 102 and 105. Also see *Institut Professionnel des Agents Immobiliers (IPI) v Geoffrey Englebert* (C-473/12) EU:C:2009:293 para 23.

89 Note, Facebook was only an intervening party to the proceedings. In other words, they were not directly involved in the issues of dispute between the parties, but

4 South African law: POPI

POPI came into full operation in 2021.[90] The drafters of POPI had the advantage of consulting both Directive 95/46, as this previously had been the most widely used legislative instrument in terms of data protection, as well as the GDPR.[91] It is consequently not surprising that POPI and Directive 95/46 overlap in many respects, although there are some important differences. Given the extent to which they overlap, Directive 95/46 and the manner in which it has been interpreted and applied by the CJEU serves as a useful comparator when it comes to the interpretation and application of POPI, taking into account how the courts have interpreted various concepts in South Africa.

The overall aim of POPI is set out in section 2 of the Act, which provides that effect must be given to the right to privacy guaranteed in section 14 of the Constitution, especially where a responsible party processes the personal information of a data subject.[92] This is subject to the principle that the right to privacy may be limited by other rights and freedoms, particularly the right to access to information protected in section 32 of the Constitution,[93] which includes not only the free flow of information in South Africa but also the cross-border transfer of information, including personal information.[94] In order to achieve its overall aim, POPI regulates the manner in which personal information may be lawfully processed by providing minimum thresholds that are "in harmony with international standards".[95] POPI also provides for remedies where there is a breach during the processing of personal information and for an Office of the Information Regulator, whose purpose is to enforce and promote the implementation of POPI.[96]

As the brief discussion above illustrates, one important area in which POPI overlaps with Directive 95/46 and the GDPR is that all three statutes are based on human rights instruments and have as their key goal the

Facebook did file papers to provide the court with further arguments to consider on the various points of law raised.

90 Proc 21 in GG 43461 of 22 June 2020 provided that POPI will commence fully by 30 June 2021.

91 SALRC *Discussion Paper 109*. Although the EU was busy with the drafting of the GDPR, throughout its discussion on the provisions of POPI the SALRC referred mainly to Directive 95/46. Hence the similarities among the various provisions throughout the two pieces of legislation. The differences will be set out below in the application of *Fashion ID* in terms of POPI.

92 See the preamble to POPI.

93 Note generally the *Promotion of Access to Information Act* 2 of 2000, which gives effect to this right.

94 Section 2(1) of POPI.

95 Section 2(2) of POPI.

96 Sections 2(3) and (4) of POPI.

protection of privacy and the lawful processing of personal data or personal information, subject to reasonable limitations where this is in the interests of the responsible party. Like Directive 95/46 and the GDPR, POPI also encourages the unhindered flow of data, not only in South Africa but also across international borders.[97]

An important difference to note at this stage is that Directive 95/46 speaks of "personal data" while POPI refers to "personal information". POPI also defines the concept of "personal information" in much greater detail than Directive 95/46 defines the concept of "personal data". Instead of defining the concept of "personal information" in general terms, POPI divides the concept into eight broad categories (listed in paragraphs (a) to (h)), some of which encompass several types of personal information. While there are clear differences among the eight categories, there are also some overlaps. For example, paragraph (a) includes identifiers that relate to who the person is, such as the person's race, gender, marital status, sexual orientation, political, religious or philosophical beliefs or affiliations, to name but a few characteristics. At the same time, paragraph (h) states that where the name of the person appears with other identifiable information that reveals who the person is, then in those circumstances the name will be personal information. For example, where a person's name and race or gender appears in the same sentence, then the name will be considered to be personal information. Paragraph (e) refers to "personal opinions, views and preferences", while paragraph (f) notes that a person may be identified through the person's correspondence, which must be seen as private information, irrespective of whether the information is confidential or not. Paragraphs (b), (d), and (g) do not overlap with any of the others, but it is still important to note what they contain. Paragraph (b) refers to a standard of living such as educational background, criminal or employment history, financial status, and medical information. Paragraph (d) refers to biometric information. Paragraph (g) refers to the views or opinions of the data subject that are held by others.

Paragraph (c) is particularly important for the purposes of this article. This is because it expressly includes certain numerical or technological identifiers in the concept of personal information, one of which is an "online identifier". As we have already seen in *Fashion ID*, the CJEU confirmed that an IP address – which is a well-known example of an online identifier – taken together with the browsing habits of a data subject, has the potential of revealing who a data subject is[98] and thus falls into the definition of

97 *Smuts v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism* (1199/2021) [2022] ZAECMKHC 42 (26 July 2022) para 18.

98 Larson 2017 *NC J L & Tech* 317-321.

"personal information" for the purposes of Directive 95/46.[99] Given first that an IP address is a well-known example of an online identifier; second, the reasoning of the CJEU; and third, that the term "online identifier" has been included in the definition of "personal information", it follows that the approach adopted in *Fashion ID* will in all likelihood also be followed in South Africa.

One of the most important differences between POPI and Directive 95/46 is that POPI applies to both natural and juristic persons, whereas Directive 95/46 applies only to natural persons. The reason for this is that the Constitution provides that juristic persons have as far as possible the same rights as natural persons. Hence, the right to privacy is guaranteed for juristic persons as well and consequently they have similar rights in terms of legislation of national application.[100]

In the light of the points set out above, we may now turn to consider how the four issues that arose in *Fashion ID* are addressed in POPI.

5 Application of POPI to the facts of *Fashion ID*

In this part of the article each of the four issues that arose in *Fashion ID* will be examined through the lens of POPI, namely locus standi, joint responsibility, legitimate interest and consent. A hypothetical South African version of Fashion ID will be referred to throughout this part of the article.

5.1 Locus standi

Apart from the internet users who visit a website that uses social plugins, the first issue that arises is whether third parties, and especially consumer protection groups, have locus standi to enforce the provisions of POPI against the business that owns the website. While POPI does not refer to consumer protection groups, it provides that the Office of the Information Regulator may assist data subjects where they have a civil claim against a business that owns a website.

The Office of the Information Regulator[101] has been designated *inter alia* to monitor and enforce the provisions of POPI.[102] In terms of section 99(1) of POPI the legislature has made provision for the Information Regulator to assist data subjects with their civil claims, as follows:

---

99 *Breyer* paras 15-16.

100 See s 8(4) of the *Constitution of the Republic of South Africa*, 1996 (hereafter the Constitution).

101 Section 39 of POPI establishes the independent, juristic state entity known as the information regulator, which amongst other responsibilities must monitor and ensure compliance with the provisions of POPI (see s 40). The current chairperson of the information regulator's office is Adv Pansy Tlakula.

102 Section 40(1)(b) of POPI.

> A data subject or, at the request of the data subject, the Regulator, may institute a civil action for damages in a court having jurisdiction against a responsible party for breach of any provision of this Act as referred to in section 73, whether or not there is intent or negligence on the part of the responsible party.[103]

In other words, and based on the facts of *Fashion ID*, the Information Regulator would assist the data subject (or internet user), if requested, where a responsible party has not adhered to the relevant data processing provisions set out in Chapter 3 of POPI,[104] thereby infringing on the data subject's rights. Unlike Articles 22 to 24 of Directive 95/46, POPI is explicit, as is the GDPR, by specifying that the Information Regulator is the authority responsible for assisting data subjects in their court matters.

5.2 Joint responsible parties

The second issue is whether a business that uses social plugins on its website (e.g., a hypothetical South African version of Fashion ID) may be regarded as a joint controller together with another party that is using the same website to collect and process personal data (e.g., Facebook South Africa would be the equivalent of Facebook Ireland Ltd).[105] Unlike Directive 95/46 POPI provides for a "responsible party" instead of a "controller", but the definitions are similar. A "responsible party" is defined as

> a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.

Both the definitions of "controller" and "responsible party" provide that multiple persons (whether public or private persons) may in concurrence with each other determine the reasons for the processing of the personal information, which in terms of section 13(1) of POPI must be lawful and specifically prescribed by the data subject and must be connected to the interests of the responsible party.

In terms of POPI, the processing of personal information is defined to include collection, recording, storage and collation, "dissemination by

---

103 Section 73 of POPI is titled "Interference with protection of personal information of data subject" and states that instances of interference with a data subject's personal information will include (a) the breach of any of the conditions for the lawful processing of personal data, set out in Chapter 3 (thereby including special personal information and the personal information of children); (b) non-compliance with certain sections, which includes the notification that a data subject's information is being processed, in terms of direct marketing, confidentiality breaches, etc.; and (c) where there is a breach in terms of the code of conduct as provided for in s 60 of POPI.

104 Section 99(1) of POPI.

105 Mata Platforms Inc have offices for Facebook South African and Facebook Africa in Johannesburg, South Africa. Formerly Facebook Inc, they are now known in South Africa as Meta Platforms Inc.

means of transmission", as well as linking, irrespective of whether the processing occurs automatically or not.[106]

The following points may be made in the light of the definition set out above. First, in terms of POPI both a hypothetical South African version of Fashion ID and Facebook South Africa would be responsible parties in terms of the processing of personal information by the social plugin. They would have decided in conjunction or in concurrence with one another to embed a social plugin on the hypothetical South African version of Fashion ID's website and to use it to collect the personal information of those visiting the website.

However, as explained above, the CJEU held that Fashion ID's responsibility was limited to those operations for which it might be held responsible and not for the further processing by Facebook Ireland. Fashion ID, therefore, could not be held responsible for those processing operations that were carried out solely by Facebook Ireland. Due to the similarities in the definitions of "controller" and "responsible party", it is likely that a South African court would come to a similar conclusion as that of the CJEU in *Fashion ID*. Put differently, the hypothetical South African version of Fashion ID would be held jointly responsible with Facebook South Africa, but only for those processing operations over which it exercised joint control with Facebook South Africa. It would not be held responsible for those processing operations over which Facebook South Africa exercised sole control.

Second, both the hypothetical South African version of Fashion ID and Facebook South Africa would profit from the free collection of data to further their business interests, either in the form of free advertising on the internet user's Facebook feed (where they have a Facebook account), alternatively from the collection of data to sell advertising space on the social network.[107] The problem would be that the data subject (i.e. the internet user) would not have consented to the collection of their personal data to be used for the commercial interests of both the hypothetical South African version of Fashion ID and Facebook South Africa.[108] Obtaining the consent of the data subject is fully discussed later in this section, but it is important to keep it in mind at this stage because of the implications for privacy.

In summary, both the hypothetical South African version of Fashion ID and Facebook South Africa would be responsible parties with respect to the social plugin. However, the responsibility of the hypothetical South African

106 Section 1 of POPI.
107 *Fashion ID* para 80.
108 Zalnieriute and Churches 2020 *MLR* 862-863; Globocnik 2019 *IIC* 1039-1040.

version of Fashion ID would be limited to those processing operations over which it had joint control with Facebook South Africa.[109]

5.3 Processing in terms of the legitimate interests of the website operator

One of the grounds for the lawful processing of data is that the responsible party must have a legitimate interest in doing so. A legitimate interest has been held to be a legal or economic interest. In *Fashion ID* the CJEU held that both Fashion ID and Facebook, as joint controllers, had to have a legitimate interest in processing the personal data collected by the social plugin. Similarly, both the hypothetical South African version of Fashion ID as well as Facebook South Africa would also need to have a legitimate interest in processing the personal data.

Section 11 of POPI sets out under which circumstances personal information may be processed. Section 11(1) provides in this respect that personal data may be processed *inter alia* where the data subject has consented,[110] where it is necessary to enter or fulfil a contract,[111] or where the processing complies with a legal obligation imposed on the responsible party.[112]

Section 11(1)(f) provides for the lawful processing of personal information where this is necessary for the pursuit of the "legitimate interests" of both the responsible party and a third party "to whom the information is supplied". All processing must, in terms of section 9, be lawful[113] and reasonable in the light of protecting the rights and freedoms of the data subject (or as in this instance the internet user).[114] In other words, a legitimate interest, like consent, is one of the listed justifications for the lawful processing of personal information. Where personal information is processed in terms of the responsible party's legitimate interest, which potentially may limit the data subject's rights and freedoms, the legitimate interests must first be balanced against the data subject's rights and freedoms to determine

---

109 Note the judgment of *Isparta v Richter* 2013 6 SA 529 (GNP) wherein it was held that where A "tags" B into a post which may contain defamatory statements, and B does not remove the "tag" after a reasonable period, then B will be held responsible with A for defamation by association, i.e. both parties are jointly responsible for the post. If joint responsibility in terms of defamation cases is possible based on the initial actions of one individual, then in terms of the facts of *Fashion ID* it is likely that South Africa's courts would hold two separate legal entities jointly responsible in terms of the processing of personal information.

110 Section 11(1)(a) of POPI.

111 Section 11(1)(b) of POPI.

112 Section 11(1)(c) of POPI.

113 Section 9(a) of POPI.

114 Section 9(b) of POPI.

whether the limitation will be considered reasonable.[115] Consent is dealt with below.

Section 11(1)(f) of POPI is similar to Article 7(f) of Directive 95/46. Both paragraphs provide for the processing of personal information to meet the responsible party's (alternatively the controller's) legitimate interests. This includes a third party to whom the personal information is supplied, depending on the facts in each specific circumstance. Neither provision defines "legitimate interests", possibly to allow for as wide a meaning as possible. The CJEU recognised that economic gain is a legitimate interest of a controller (i.e. or joint controllers).[116]

Similar inferences can be drawn in the South African context. In *H v W*[117] the court, quoting with approval from *Largent v Reed and Pena*,[118] explained that where individuals post on Facebook, these posts may be liked, disliked or commented on by other Facebook users. This would include posts or suggestions regarding restaurants, clothing retailers and other businesses, etc.[119] Hence, when a person clicks on the Facebook social plugin to "like" the content of a website, this will appear as a post on their feed or wall to which other Facebook users may post a "like" or a comment.[120]

In terms of the facts of *Fashion ID*, this would amount to free advertising on behalf of the hypothetical South African version of Fashion ID, as internet users (who have a Facebook account) visiting their website might click the "like" button, and it would appear as a post on their wall or feed. The post might be seen by their Facebook contacts, and there would be the possibility of these contacts clicking on the link provided in the post to look at the content on Fashion ID's website, after which they might purchase an item. Facebook South Africa would be able to collect personal information to entice companies to advertise on the social network site and these adverts might be targeted at those who have "liked" similar content on Fashion ID's website, to encourage a sale. Facebook South Africa would be selling the

115 Section 36 of the Constitution. Also see De Stadler *et al Over-Thinking the Protection of Personal Information Act* 59-60. Note that the data subject may, in terms of s 11(3)(a) of POPI, object to the processing of his/her personal information where the responsible party relies on a legitimate interest in terms of s 11(1)(f) – De Stadler *et al Over-Thinking the Protection of Personal Information Act* 197.

116 *Fashion ID* para 80.

117 *H v W* 2013 2 SA 530 (GSJ).

118 *Largent v Reed and Pena* (Case No 2009-1823) 39th Judicial District of Pennsylvania, Franklin County (7 November 2011) 3-5.

119 *H v W* 2013 2 SA 530 (GSJ) paras 10-11. See Coetzee 2019 *PELJ* for the far-reaching consequences that these posts have, and Karjiker 2022 *SALJ* regarding how a hyperlink works and the legal consequences thereof – a social plugin functions like a hyperlink.

120 Röttgen "Like or Dislike" 74, 76-78; Karjiker 2022 *SALJ* 184-187.

advertising space; hence they too would be making a profit (i.e. this would be a form of economic interest).

In terms of section 11(f) of POPI, this would amount to processing for the responsible party's interests – being able to make a profit through the use of the social plugin, i.e. for financial or economic gain, through advertising or capitalising on the collection of the personal information.

5.4 The need to obtain consent to process the personal information

The two questions asked above were, first, who must obtain the consent of the data subject and, second, do data subjects need to be notified of the collection of their personal information by a third party? To understand the first question it is best to look at what type of consent is required in terms of POPI. Section 1 defines "consent" in definitive terms as:

> any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

Personal information cannot be collected automatically without the explicit consent of the data subject, subject to certain exemptions as provided for in POPI.[121] As set out above, for the processing of personal data to be lawful one of the justified grounds for the processing of personal information provided for in section 11(1) of POPI must be present. One of those grounds is consent. Section 11(1)(a) of POPI provides that for the lawful processing of personal information, explicit consent from the data subject must be obtained.[122] Consent for the processing of personal information is often a vital requirement for the lawful processing thereof. Section 13(1) provides that personal information may be collected only for a "specific, explicitly defined and lawful purpose relating to a function of the responsible party". In other words, echoing the definition of "consent", the data subject must be informed as to why such personal information is being collected.

Section 13(2) expands on this and specifically requires that the responsible party must take the necessary steps to notify the data subject of the reason for the collection of the personal information, unless certain exceptions are applicable.[123] In other words, section 13(2) requires that data subjects must know what they are consenting to in relation to the processing of their personal information. Applying this to the facts of *Fashion ID*, in respect of the social plugin, since it is on the hypothetical South African version of Fashion ID's website, it would in terms of POPI be most expedient for the hypothetical South African version of Fashion ID to obtain consent for the

---

121 See s 6 of POPI, which lists the exclusions.

122 Note the definition of "consent" in s 1 of POPI which reads as follows: "any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information".

123 Regarding notification, see s 18(1), and for the exceptions, see s 18(4) of POPI.

processing on its own behalf and on that of Facebook South Africa because the hypothetical South African version of Fashion ID placed the social plugin on their website.

To complete this picture and to provide a further reason for the answer to the first question, as well as to answer the second, section 13(2) of POPI must be read with section 18. Section 18(1) requires that reasonably practicable steps must be taken to inform a data subject that their personal information is being collected.[124] Section 18(1) provides, amongst other requirements, that the data subject must be aware of what personal information is being collected, the reason or purpose thereof and whether the personal information will be transferred to a third party.[125]

In other words, applying POPI to *Fashion ID*, visitors to the hypothetical South African version of Fashion ID's website would have to be warned that their personal information will be collected for processing, and told the reason for the collection thereof, to provide the necessary informed consent to allow for the collection and processing of their personal information. As to who must warn, it will again, for expediency and because of the placement of the social plugin on their website, be the responsibility of the hypothetical South African version of Fashion ID.

6 Conclusion

The need for control over the collection of personal information both directly and via third parties by means of internet websites with the use of social plugins and other trackers must be met on a case-by-case basis. It is important that data subjects (or internet users) have control over and protection of their personal information (or data) during all interactions with companies with an active online profile and that trackers are limited to providing only the necessary support needed for the website to function correctly.[126] *Fashion ID* highlights the privacy concerns that social plugins and trackers raise, especially where internet users have not joined the social media website (i.e. Facebook), and they click on websites that automatically collect and store their personal information. One suggestion relative to this

124 This is subject to certain exceptions that are set out in s 18(4) of POPI.

125 Sections 18(1)(a), (c) and (g) of POPI are specifically mentioned here for their relevance to the discussion. S 18(4) provides for the exceptions. The only two that may have a slight bearing on the case, where notification is not required, are (b), where the data subject's interest will not be prejudiced; (e) where compliance is not reasonably practicable in the circumstances; and (g) where the information collected will (first) not be used to identify the data subject and (second) the collection thereof is for "historical, statistical or research purposes". As the facts of *Fashion ID* did not indicate that a possible exception might apply, it will not be necessary to explore these exceptions in this document.

126 See generally Strauß and Nentwich 2013 *Science and Public Policy* 727; Larson 2017 *NC J L & Tech* 317-321; Röttgen "Like or Dislike" 73-80.

automatic collection of personal information, especially from internet users that have not subscribed to Facebook, is to provide them an option to either opt out or to allow for the collection.[127] Furthermore, websites such as Fashion ID's must make it clear that there are third parties that collect the personal information of any user that visits the website.[128] This is something that has become the norm in Europe but is lacking in South Africa. Hence, there is a need for websites that host third-party social plugins to be more transparent by warning internet users who open and visit their webpages that there are third parties that are collecting their personal information.[129] The transparency must extend to situations where two or more jointly responsible parties are collecting an internet user's personal information in the light of their own economic interests,[130] as discussed above.[131] A warning that there are third parties that use websites to host social plugins, in the light of POPI, which includes internet users with the option to opt out of the collection of their personal information, even by third parties, in terms of the facts in *Fashion ID*, would go a long way towards providing internet users with suitable protection of their right to data protection.

Bibliography

Literature

Aladeokin, Zavarsky and Memon "Analysis and Compliance"
Aladeokin A, Zavarsky P and Memon N "Analysis and Compliance Evaluation of Cookies-Setting Websites with Privacy Protection Laws" in *Twelfth International Conference on Digital Information Management* (ICDIM) (12-14 September 2017 Fukuoka) 121-126

Coetzee 2019 *PELJ*
Coetzee SA "A Legal Perspective on Social Media Use and Employment: Lessons for South African Educators" 2019 *PELJ* 1-36 http://dx.doi.org/10.17159/1727-3781/2019/v22i0a5778

127 Truyens 2016 *EDPL* 140.

128 *Fashion ID* paras 98-103; *Bundesverband der Verbraucherzentralen und Verbraucherverbände - VerbraucherzentraleBundesverband eV v Planet* 49 (C-673/17) EU:C:2019:801 paras 65 and 81. Also see De Conca 2020 *SCRIPTed* 264-265; Wiedemann 2020 *IIC* 545-549.

129 Aladeokin, Zavarsky and Memon "Analysis and Compliance" 125-126.

130 This includes capitalising on the collection and processing of the free personal information, as well as the free advertising that may (or may not) lead to an increased sale of the joint responsible parties' products. See Wiedemann 2020 *IIC* 545-549.

131 *Fashion ID* para 80.

De Conca 2020 *SCRIPTed*
De Conca S "Between a Rock and a Hard Place: Owners of Smart Speakers and Joint Control" 2020 *SCRIPTed: Journal of Law, Technology and Society* 238-268

De Stadler *et al Over-Thinking the Protection of Personal Information Act*
De Stadler E *et al Over-Thinking the Protection of Personal Information Act: The Last POPIA Book You Will Ever Need* (Juta Cape Town 2021)

Docksey and Hijmans 2019 *EDPL*
Docksey C and Hijmans H "The Court of Justice as a Key Player in Privacy and Data Protection: An Overview of Recent Trends in Case Law at the Start of a New Era of Data Protection Law" 2019 *EDPL* 300-316

Duina 1997 *Int'l J Soc L*
Duina F "Explaining Legal Implementation in the European Union" 1997 *Int'l J Soc L* 155-179

Ermakova *et al* "Web Tracking"
Ermakova T *et al* "Web Tracking: A Literature Review on the State of Research" in *Proceedings of the 51st Hawaii International Conference on System Sciences* (3-6 January 2018 Waikoloa Village) 4732-4741

Gerlitz and Helmond 2013 *New Media and Society*
Gerlitz C and Helmond A "The Like Economy: Social Buttons and the Data-Intensive Web" 2013 *New Media and Society* 1348-1365

Globocnik 2019 *IIC*
Globocnik J "On Joint Controllership for Social Plugins and Other Third-Party Content: A Case Note on the CJEU Decision in *Fashion ID*" 2019 *IIC* 1033-1044

Karjiker 2022 *SALJ*
Karjiker S "Hyperlinking and Copyright" 2022 *SALJ* 181-204

Larson 2017 *NC J L & Tech*
Larson E "Tracking Criminals with Internet Protocol Addresses: Is Law Enforcement Correctly Identifying Perpetrators?" 2017 *NC J L & Tech* 316-358

Lindroos-Hovinheimo 2019 *Info & Comm Tech L*
Lindroos-Hovinheimo S "Who Controls our Data? The Legal Reasoning of the European Court of Justice in *Wirtschaftsakademie Schlewig-Holstein* and *Tietosuojavaltuutettu v Jehovan todistajat*" 2019 *Info & Comm Tech L* 225-238

Röttgen "Like or Dislike"
Röttgen C "Like or Dislike—Web Tracking" in Hoeren T and Kolany-Raiser B (eds) *Big Data in Context: Legal, Social and Technological Insights* (Springer Cham 2018) 73-80

SALRC *Discussion Paper 109*
South African Law Reform Commission *Discussion Paper 109 (Project 124): Privacy and Data Protection* (SALRC Pretoria 2005)

Srinivasan 2019 *Berkeley Bus LJ*
Srinivasan D "The Antitrust Case against Facebook: A Monopolist's Journey towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy" 2019 *Berkeley Bus LJ* 39-101

Strauß and Nentwich 2013 *Science and Public Policy*
Strauß S and Nentwich M "Social Network Sites, Privacy and the Blurring Boundary between Public and Private Spaces" 2013 *Science and Public Policy* 724-732

Truyens 2016 *EDPL*
Truyens M "No more Cookies for Unregistered Facebook Users in Belgium: Belgian Data Protection Legislation Applies to Facebook" 2016 *EDPL* 135-140

Veale and Zuiderveen Borgesius 2022 *German Law Journal*
Veale M and Zuiderveen Borgesius F "Adtech and Real-Time Bidding under European Data Protection Law" 2022 *German Law Journal* 226-256

Wiedemann 2020 *IIC*
Wiedemann K "The ECJ's Decision in '*Planet49*' (Case C-673/17): A Cookie Monster or Much Ado about Nothing?" 2020 *IIC* 543-553

Zalnieriute and Churches 2020 *MLR*
Zalnieriute M and Churches G "When a 'Like' is not a 'Like': A New Fragmented Approach to Data Controllership" 2020 *MLR* 861-876

Case law

European Union

Breyer v Bundesrepublik Deutschland (C-582/14) EU:C:2016:779

Bundesverband der Verbraucherzentralen und Verbraucherverbände - VerbraucherzentraleBundesverband eV v Planet 49 (C-673/17) EU:C:2019:801

Data Protection Commission v Facebook Ireland and Maximillian Schrems (C-311/18) EU:C:2020:559

Facebook Ireland Ltd v Gegevensbeschermingsautoriteit (C-645/19) EU:C:2021:483

Fashion ID GmbH and Co KG v Verbraucherzentrale NRW e.V. (C-40/17) EU:C:2019:629

Google Spain SL, Google LLC v Agencia Española de Protección de Datos (AEPD), Mario Costeja González (C-131/12) EU:C:2014:317

Institut Professionnel des Agents Immobiliers (IPI) v Geoffrey Englebert (C-473/12) EU:C:2009:293

Lindqvist (C-101/01) EU:C:2003:596

Meta Platforms Ireland Ltd v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. (Case C-319/20) EU:C:2022:322

Rechnungshof v Österreichischer Rundfunk and Christa Neukomm and Joseph Lauermann v Österreichischer Rundfunk (C-465/00, C-138/01 & C-139/01) EU:C:2003:294

Schrems v Data Protection Commissioner (C-362/14) EU:C:2015:650

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH (C-210/16) EU:C:2018:388

Valsts Policijas Rīgas Reģiona Pārvaldes Kārtības Policijas Pārvalde v Rīgas Pašvaldības SIA 'Rīgas Satiksme' (Case C-13/16) EU:C:2017:336

South Africa

H v W 2013 2 SA 530 (GSJ)

Isparta v Richter 2013 6 SA 529 (GNP)

Smuts v Member of the Executive Council: Eastern Cape Department of Economic Development Environmental Affairs and Tourism (1199/2021) [2022] ZAECMKHC 42 (26 July 2022)

United States of America

Largent v Reed and Pena (Case No 2009-1823) 39th Judicial District of Pennsylvania, Franklin County (7 November 2011)

Legislation

Germany

Gesetz gegen den Unlauteren Wettbewerb (1909) (Law against Unfair Competition)

South Africa

Constitution of the Republic of South Africa, 1996

Promotion of Access to Information Act 2 of 2000

Protection of Personal Information Act 4 of 2013

Government publications

Proc 21 in GG 43461 of 22 June 2020

International instruments

Charter of Fundamental Rights of the European Union (2000)

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)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (2002) (*Directive on Privacy and Electronic Communications*)

European Convention for the Protection of Human Rights and Fundamental Freedoms (1950) (as amended by Protocol Nos 11 and 14, and Supplemented by Protocols Nos 1, 4, 6, 7, 12, 13 and 16)

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 (2016) (*General Data Protection Regulation*)

Internet sources

Acar *et al* 2015 https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf

Acar G *et al* 2015 *Facebook Tracking through Social Plug-ins: Technical Report Prepared for the Belgian Privacy Commission* https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf accessed 10 October 2022

Kelly 2019 https://blog.mozilla.org/en/internet-culture/mozilla-explains/what-is-a-web-tracker/
Kelly MJ 2019 *What is a Web Tracker? Mozilla Explains* https://blog.mozilla.org/en/internet-culture/mozilla-explains/what-is-a-web-tracker/ accessed 16 November 2022

List of Abbreviations

Berkeley Bus LJ	Berkeley Business Law Journal
CJEU	Court of Justice of the European Union
EDPL	European Data Protection Law Review
EU	European Union
GDPR	General Data Protection Regulation
IIC	International Review of Intellectual Property and Competition Law
Info & Comm Tech L	Information and Communications Technology Law
Int'l J Soc L	International Journal of Sociology of Law
MLR	Modern Law Review
NC J L & Tech	North Carolina Journal of Law and Technology
PELJ	Potchefstroom Electronic Law Journal
POPI	Protection of Personal Information Act 4 of 2013
SALJ	South African Law Journal
SALRC	South Africa Law Reform Commission
UWG	Gesetz gegen den Unlauteren Wettbewerb (Law against Unfair Competition)