Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 30 *XXX*
Number 4

Article 2

2020

Down the Rabbit Hole: Applying a Right to Be Forgotten to Personal Images Uploaded on Social Networks

Eugenia Georgiades
Bond University, egeorgia@bond.edu.au

Down the Rabbit Hole: Applying a Right to Be Forgotten to Personal Images Uploaded on Social Networks

Cover Page Footnote

Dr. Eugenia Georgiades, Assistant Professor Faculty of Law, Bond University. The author would like to thank Professor Brad Sherman, Associate Professor Leanne Wiseman, Associate Professor Jay Sanderson, and Dr. Allan Ardil for their feedback.

Down the Rabbit Hole: Applying a Right to Be Forgotten to Personal Images Uploaded on Social Networks

Eugenia Georgiades*

The right to be forgotten has been the subject of extensive scrutiny in the broad context of data protection. However, little consideration has been given to the misuse of personal images that are uploaded on social networks. Given the prevalent use of online and digital spaces, social networks process and use various forms of data, including personal images that are uploaded by individuals. The potential for misuse of images is particularly acute when users upload images of third parties. In light of the European Union's enshrinement of the "right to be forgotten" amid provisions of the General Data Protection Regulation that tighten protections for Internet users' privacy, this Article examines whether the European "right to be forgotten" is a model that could be adopted, specifically in Australia, and perhaps elsewhere, as a mechanism to protect against the misuse of people's images within social networks.

* Dr. Eugenia Georgiades, Assistant Professor Faculty of Law, Bond University. The author would like to thank Professor Brad Sherman, Associate Professor Leanne Wiseman, Associate Professor Jay Sanderson, and Dr. Allan Ardil for their feedback.

"The Internet doesn't forget."[1]

INTRODUCTION

Social networks facilitate communication and interaction online. When people communicate and interact online, their private lives often become public. Social networks such as Facebook, Instagram, and Twitter have sparked new trends in the way people exchange and communicate information, particularly personal images. These platforms actively encourage people to share their lives with their friends, family, and social connections within the digital environment.[2] All too frequently, people's images are captured in photographs and shared on social networks without the person knowing

---

[1] Jef Ausloos, *The 'Right to Be Forgotten'—Worth Remembering?*, 28 COMPUTER L. & SECURITY REV. 143, 143 (2012).

[2] Eugenia Georgiades, *Reusing Images Uploaded Online: How Social Networks Contracts Facilitate the Misuse of Personal Images*, 40 EUR. INTELL. PROP. J. 435, 441 (2018). Part of Facebook's Data Policy states that:

> [Facebook is] able to deliver our Services, personalise content, and make suggestions for you by using this information to understand how you use and interact with our Services and the people or things you're connected to and interested in on and off our Services. We also use information we have to provide shortcuts and suggestions to you. *For example, we are able to suggest that your friend tag you in a picture by comparing your friend's pictures to information we've put together from your profile pictures and the other photos in which you've been tagged.* If this feature is enabled for you, you can control whether we suggest that another user tag you in a photo using the 'Timeline and Tagging' settings. When we have location information, we use it to tailor our Services for you and others, like helping you to check-in and find local events or offers in your area or tell your friends that you are nearby. We conduct surveys and research, test features in development, and analyse the information we have to evaluate and improve products and services, develop new products or features, and conduct audits and troubleshooting activities.

See Data Policy, FACEBOOK, https://www.facebook.com/about/privacy/ [https://perma.cc/792W-W93K] (emphasis added); *see also* BRENDAN VAN ALSENOY ET AL., BELGIAN PRIVACY COMMISSION, FROM SOCIAL MEDIA SERVICE TO ADVERTISING NETWORK: A CRITICAL ANALYSIS OF FACEBOOK'S REVISED POLICIES AND TERMS (Mar. 31, 2015), http://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf [https://perma.cc/U4RF-DJCA].

that their images have been taken and shared online.[3] In the process of sharing images on social networks, people often relinquish control over the use of their images, which allows the images to be exploited by third parties and social networks.[4] The use of digital and communication technologies creates a need to protect personal images and the information captured in those images from misuse.[5]

This Article examines whether the European Union ("EU")'s "right to be forgotten" provides a possible solution to the problem of personal images being misused on social networks in Australia. Specifically, it considers whether the EU's right to be forgotten is a model that could be adopted in Australia as a mechanism to protect against the misuse of people's images within social networks.

---

[3] Notable examples include the infamous photograph of a naked Prince Harry partying in Las Vegas. *See Prince Harry Naked During Vegas Rager*, TMZ (Aug. 22, 2012), http://www.tmz.com/2012/08/21/prince-harry-naked-photos-nude-vegas-hotel-party [https://perma.cc/J48L-E5N2]. The problem with this is captured in Katy Perry's tweet against Australian Media where she said: "Australian PRESS: you should be ashamed of your paparazzi & tabloid culture. Your paparazzi have no respect, no integrity, no character. NO HUMANITY." Perry also wrote: "I was stalked by many grown men today as I tried to take a quiet walk to the beach. These men would not stop as I pleaded over & over to let me have my space. Many other people stopped to try to help but the paps continued to laugh at me & hold their barrels up and shoot." And further: "This is PERVERTED & disgusting behaviour that should NEVER be tolerated, especially by people who do NOT want this." Katy Perry (@katyperry), TWITTER (Nov. 21, 2014, 6:39 PM), https://twitter.com/katyperry/status/535985788983721984/photo/1 [https://perma.cc/683Q-FB7F].

[4] *See generally* VICTOR MAYER-SCHONBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGES 1–2 (2011); Franz Werro, *The Right to Inform v. the Right to Be Forgotten: A Transatlantic Clash, in* HAFTUNGSRECHT IM DRITTEN MILLENNIUM = LIABILITY IN THE THIRD MILLENNIUM (Aurelia Colombi Ciacchi et al. eds., 2009); Ausloos, *supra* note 1; Paul A. Bernal, *A Right to Delete?*, 2 EUR. J.L. & TECH. (2011); Muge Fazlioglu, *Forget Me Not: The Clash of the Right to Be Forgotten and Freedom of Expression on the Internet*, 3 INT'L DATA PRIVACY L. 149, 151 (2013); Andra Giurgiu, *Challenges of Regulating a Right to Be Forgotten with Particular Reference to Facebook*, 7 MASARYK U. J.L. & TECH. 361, 362 (2013); Alessandro Mantelero, *The EU Proposal for a General Data Protection Regulation and the Roots of the 'Right to Be Forgotten'*, 29 COMPUTER L. & SECURITY REV. 229, 230 (2013); Marie-Andrée Weiss, *First Amendment Trumps Couple's Right of Publicity; Copyright Claim to Proceed*, 9 J. INTELL. PROP. L. & PRAC. 797, 798 (2014).

[5] *See* Bert-Jaap Koops, *Forgetting Footprints, Shunning Shadows: A Critical Analysis of the "Right to Be Forgotten" in Big Data Practice*, 8 SCRIPTED 229, 230 (2011); *see also* Viviane Reding, *The Upcoming Data Protection Reform for the European Union*, 1 INT'L DATA PRIVACY L. 3, 3 (2011).

I. ORIGINS AND DEVELOPMENT OF THE RIGHT TO BE FORGOTTEN

The right to be forgotten originated from a growing concern about the impact of digital technologies in general on personal privacy. As Viviane Reding observed, "If an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system."[6] The early 1990s saw the use of digital technologies increase, which created a need to protect people from potential abuse.[7] As communication technologies sparked new trends in the way people exchanged and communicated personal information, the EU recognized that new data protection laws were necessary to protect individual privacy and private life.[8] To this end, European regulators developed the Data Directive[9] in 1995 to protect an individual's personal data and the processing of such data. European data-protection laws were enacted at a time when technology was less advanced and the exchange of personal information was significantly lower than it is at present,[10] in part because the use of social networks was not as prevalent twenty-five years ago as it is today.

One of the challenges that arises with most new forms of technology is that the technology often evolves faster than the law.[11] The position with social networks is no different. As Andra Giurgiu argues, "The main problem relies in the fact that the rapidly changing societal model has not allowed for legal norms to catch up."[12] Concerned about the threat to individual privacy created by the

---

6 Press Release, Viviane Reding, Vice-President of the Eur. Comm'n, EU Justice Comm'r, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age (Jan. 22, 2012), http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm [https://perma.cc/JPU6-VYZ7].

7 *See* Koops, *supra* note 5, at 230; *see also* Reding, *supra* note 5, at 3.

8 *See* Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, *opened for signature* Nov. 4, 1950, E.T.S No. 5, Art 8.

9 Directive 95/46/EC, of the European Parliament and of the Council of 20 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter Data Directive].

10 *See* Giurgiu, *supra* note 4, at 362–64.

11 *Id.* at 362–65; Koops, *supra* note 5; Ausloos, *supra* note 1, at 148.

12 Giurgiu, *supra* note 4, at 362–65.

widespread use of data storage and data mining, European regulators recognized that the rights to privacy and data protection in the Data Directive had become outdated.[13]

The problems with the law under the 1995 Data Directive were highlighted in the landmark 2014 Court of Justice decision of *Google Spain v. Gonzalez.*[14] The case arose when Mr. Gonzalez lodged a complaint against *La Vanguardia Ediciones SL* (a daily Spanish newspaper with a wide circulation), Google Spain, and Google Inc.[15] The basis of the complaint was that whenever an internet user searched for Mr. Gonzalez's name using the Google search engine, the results would link to two pages from the *La Vanguardia* newspaper, which mentioned Mr. Gonzalez's name in connection with proceedings for social security debts.[16]

Mr. Gonzalez requested two things. The first was that the newspaper remove or alter the pages so that "the personal data relating to him no longer appeared or to use certain tools made available by search engines in order to protect the data."[17] The second request was that Google Spain and Google Inc. be required to remove or conceal the personal data relating to him so that that data would not be included in the search results.[18] The grounds for Mr. Gonzalez's claims were that the proceedings for the social security debts mentioned in the newspaper links had been resolved for a number of years. Consequently, that information and any references to that information was no longer relevant to answering a search of his name conducted at the present time or in the future.[19]

---

13 *See* discussion *infra* Part I.

14 Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317 (May 13, 2014).

15 *Id.* at ¶¶ 14–15.

16 *Id*.

17 *Id*.

18 *Id*.

19 *Id*.

The court ordered Google Spain to remove Gonzalez's personal data[20] from the internet.[21] The court held that data controllers should remove data where the data was "*inadequate, irrelevant or no longer relevant, or excessive in relation to [the] purposes [for which they were originally collected or processed]* [emphasis added] *and in the light of the time that has elapsed*."[22] The Court of Justice ruled that people could request the removal of their data published by operators of search engines.[23]

The *Google Spain v. Gonzalez*[24] decision not only highlighted some of the inadequacies with the 1995 Data Directive, but it also provided a possible solution. After some debate,[25] on December 15, 2015[26] the European Parliament passed the General Data Protection Regulation ("GDPR"),[27] which received approval from the European Council on April 8, 2016 and became effective on May 28, 2018.[28] One of the key aspects of the GDPR is that it supersedes the

---

[20] Data Directive, *supra* note 9, at art. 2(a), which defines data broadly as:

> '[P]]ersonal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, 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.

[21] *Google Spain SL*, 2014 E.C.R. 317 at ¶ 93.

[22] *Id.* The ruling is based on the Data Directive, *supra* note 9.

[23] *Id.* at ¶ 98.

[24] *Google Spain SL*, 2014 E.C.R. 317 at ¶ 97–98.

[25] *See* W. Gregory Voss, *Looking at the European Union Data Protection Law Reform Through a Different Prism: The Proposed EU General Data Protection Regulation Two Years Later*, 17 J. INTERNET L. 1, 22 (2014); *see also* Peter Blume, *The Myths Pertaining to the Proposed General Data Protection Regulation*, 4 INT'L DATA PRIVACY L. 269, 269–73 (2014).

[26] *See* European Commission Press Release IP/12/46, Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market (Dec. 15, 2015), *available at* http://europa.eu/rapid/press-release_IP-15-6321_en.htm> [https://perma.cc/25XL-ETPP].

[27] Regulation 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 O.J. (L 119) 1 [hereinafter General Data Protection Regulation].

[28] *See Reform of EU Data Protection Rules*, EUR. COMMISSION, https://ec.europa.eu/info/law/law-topic/data-protection/reform_en [https://perma.cc/KT8L-FJ9K].

Data Directive and strengthens individual rights, through the incorporation of a right to be forgotten.[29]

The 2016 GDPR provides that where a data controller has made data public, the controller must take "reasonable steps, including technical measures[in relation to data for the publication of which the controller is responsible], to inform [third parties] which are processing the data that a data subject [requests them to erase] any links to, or copy or replication of [that] personal data."[30] The GDPR provides that a data subject shall have "the right to obtain from the controller the erasure of personal data" relating to them and the abstention from further dissemination of such data especially in relation to personal data which are made available by the subject data while he or she was a child.[31] Article 17 also gives data subjects the right to be forgotten and to erase data relating to them.[32] It provides that users have the right to have information deleted in four situations. This is where:

---

[29] The proposed amendments to the Data Directive included the rights of users to request that their personal data is "no longer processed and deleted when they are no longer needed for legitimate purposes." *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union*, COM (2010) 609 final, at sec. 2.1.3 (Apr. 11, 2010) [hereinafter *A Comprehensive Approach*]; *see also* General Data Protection Regulation, *supra* note 27, at art. 17.

[30] *Id.* at art. 17(2).

[31] *Id.*; *see also id*. at art. 17(1) (referencing back to articles 6(1) and 8(1) of the regulation).

[32] *Id.* at art. 17; *see generally* Ausloos, *supra* note 1; Steven C. Bennett, *The Right to Be Forgotten: Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L L. 161 (2012); Karen Eltis, *Breaking Through the Tower of Babel: A Right to be Forgotten and How Trans-Systemic Thinking Can Help Re-Conceptualize Privacy Harm in the Age of Analytics*, 22 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 69 (2011); Koops, *supra* note 5; Barbara McDonald, *Privacy, Princesses, and Paparazzi*, 50 N.Y. L. SCH. L. REV. 205 (2005); Dominic McGoldbrick, *Developments in the Right to Be Forgotten*, 13 HUM. RTS. L. REV. 761 (2013); Reding, *supra* note 5; Jeffrey Rosen, *The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google*, 80 FORDHAM L. REV. 1525 (2012); Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2011–12); Jeffrey Rosen, *Free Speech, Privacy, and the Web That Never Forgets*, 9 J. TELECOMM. & HIGH TECH. L. 345 (2011); Stijn Smet, *Freedom of Expression and the Right to Reputation: Human Rights in Conflict*, 26 AM. U. INT'L L. REV. 183 (2010); Rolph H. Weber, *The Right to Be Forgotten: More Than Pandora's Box?*, 2 J. INTELL. PROP., INFO. TECH. & E-LAW 120 (2011); *see also generally A Comprehensive Approach*, *supra* note 29; Werro, *supra* note 4.

a) the personal data are no longer necessary in relation to the purposes for which it was collected or otherwise processed;
b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); and
d) the personal data have been unlawfully processed.[33]

When applying the right to be forgotten to personal images shared online, there are a number of criteria that must be satisfied, as explained further in Part II below. Broadly, these are that:

1. the requirements for protection are met;
2. the use of the images falls within the scope of the right; and
3. the use of the images falls outside of the exceptions to the right to be forgotten.

The following section examines these elements in more detail.

II. REQUIREMENTS FOR PROTECTION

There are a number of criteria that must be satisfied in order for the right to be forgotten to apply. The first is that the images must fall within the meaning of "data" as provided in the GDPR.[34] The second is that the person must be a "data subject."[35] The third factor that needs to be satisfied for the right to apply is that the images

---

[33] General Data Protection Regulation, *supra* note 27, at art. 1 7(1); Giurgiu, *supra* note 4, at 366; Mantelero, *supra* note 4, at 233; McGoldbrick, *supra* note 32, at 763.

[34] *See infra* Section II.A.

[35] *See infra* Section II.B.

must be controlled by a third party who is a "data controller."[36] The following sub-sections examine each in turn.

A. Data

In Europe, the term "data" is defined broadly to include any information that relates to a "data subject."[37] Any information that relates to a person or identifies a person in an online environment will be considered "personal data."[38] Photographs depicting people's likenesses are a way of identifying individuals and thus satisfy the definition of data in the Data Directive.[39]

People who join social networks and engage in the digital world exchange and share various types of information. This information forms the data that is processed, collected, and stored in websites' information systems. As social networks allow people to share images with multiple users simultaneously, a number of issues arise in relation to the control of those images. One issue with the control of uploaded images occurs when a person uploads images and those images are consequently reshared by third parties. The reshared images will be stored, collected and processed on their respective profile pages (as well as the network's information systems). Thus, a person whose images are reshared loses control over these images when they are reshared. Another issue that arises is that, under European law, capturing and sharing another person's image on a social network by posting photographs of them online may be considered "processing and collecting" data. Given that people not only share and exchange their own images but also third-party images on social networks, such images that are shared form the "data" of the subject (i.e., the person whose image is being used or shared). Consequently, a person loses control over their image when their image is captured in a photograph by a third party.

---

36 *See infra* Section II.C.

37 *See* Data Directive, *supra* note 9, at art. 2(a) ("'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, 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").

38 *Id*.

39 *Id*.; *see also generally* Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445 (1995).

B. Data Subject

The second criterion that needs to be satisfied for the right to apply is that the person must be a "data subject." European data protection laws apply to data subjects who are located in Europe. People who live in countries that are part of the EU, are entitled to rely on a right to be forgotten when their data are processed, collected, or transferred to countries outside of the EU.[40]

According to Article 4(1) of the GDPR, a data subject is a "natural person,"[41] construed broadly as a person who can be "identified directly or indirectly, in particular reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[42] People who are users of social networks and social media will fall within the definition of a "data subject." Accordingly, any photographs that contain a person's image would also fall within the definition of "personal data," as discussed above.

C. Data Controller

The third factor that needs to be satisfied for the right to apply is that the images must be controlled by a third party who is a "data controller." Article 4(7) of the GDPR defines a "data controller" as follows:

> '[C]ontroller' means 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 Union or Member State law, the controller or the

---

40 *See* Case C-362/14, Schrems v. Data Protection Comm'r, 56 I.L.M. 245 (2015) (EU) (Schrems objected to the transfer of his personal data from Facebook Ireland to servers in the United States).

41 *See* General Data Protection Regulation, *supra* note 27, at art. 4(1); *see also* Opinion 5/2009 on Online Social Networking adopted on 12 June 2009, The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, art. 29, 1995 O.J. (L 281/31) (EC) [hereinafter Working Party Opinion].

42 *Id*.

> specific criteria for its nomination may be provided for by Union or Member State law.[43]

Google Spain v. Gonzalez confirms that search engines are data controllers and as such are liable under the GDPR.[44] To fall within the definition of data controllers, the social network must determine the purpose and means of processing personal data. Social networks clearly fall within the definition of data controllers, because virtually every social network determines the purpose and means of processing personal data. The processing of personal data occurs when people subscribe to a social network service because they provide personal information such as name, email, and often a profile picture, which are stored, collected, and processed on the social network's information systems. For example, when people use Facebook, personal data processing occurs as an integral part of the company's mission: "bringing people together."[45] In pursuit of this purpose, Facebook determines how people's photographs will be processed and collected, including that the network will collect those images when people share images of third parties.[46] Thus, Facebook is a data controller because the network processes, stores, transfers and collects people's personal data.[47] Similarly, Instagram's purpose is for people to share their photographs with other users, and it is for this purpose that they collect and process people's information and specifically their photographs.[48] Twitter also shares

---

[43] General Data Protection Regulation, *supra* note 27, at art. 4(7); *see also* Data Directive, *supra* note 9, at art. 2; Rebecca Wong, *Social Networking: Anybody Is a Data Controller*, NOTTINGHAM L. SCH. (Sept. 21, 2008), http://ssrn.com/abstract=1271668 [https://perma.cc/8CED-L4AD] [hereinafter Wong, *Anybody Is a Data Controller*].

[44] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317, ¶ 33 (May 13, 2014).

[45] Adam Mosseri, *Bringing People Closer Together*, FACEBOOK (Jan. 11, 2018), https://about.fb.com/news/2018/01/news-feed-fyi-bringing-people-closer-together/ [https://perma.cc/4R4V-RMCA].

[46] *See* General Data Protection Regulation, *supra* note 27, at art. 7 (providing that a person can withdraw their consent).

[47] *See, e.g.*, Rebecca Wong, *Social Networking: A Conceptual Analysis of a Data Controller*, 14 COMM. L. 142, 142 (2009) [hereinafter Wong, *A Conceptual Analysis*]; Working Party Opinion, *supra* note 41.

[48] *See Features*, INSTAGRAM, https://about.instagram.com/features [perma.cc/PN2R-7XQD]; *see also* Wong, *supra* note 47; Working Party Opinion, *supra* note 41.

the same purpose as Facebook and Instagram, which satisfies the definition of a data controller of the Data Directive and the GDPR.

One question that arises is whether individuals who share other people's images fall under the definition of data controller. Given the scope of Web 2.0 and the participative culture that it created, individuals who share other people's images may also be treated as "data controllers."[49] This is because people share and exchange personal images within their profiles on social networks and thus facilitate the "processing" of personal data. A person may be a "data controller" when they capture an image and upload it on their social network profile page. When a person captures their own image (i.e., a selfie) and uploads that image on their profile, they are in effect collecting and processing their own data. This data in turn is stored on the social network information system. In situations where a person captures an image of a third party, the information captured in the photograph forms part of a record which is collected and processed when it is uploaded online. As a result, a person may also collect and process a third party's data, and thus each person who has a social network page has the ability to collect and process other people's data. Consequently, it is arguable that people who take photographs of third parties and upload and exchange the images on social networks would facilitate the "processing of personal data" and as such arguably fall within the definition of "data controller."

III. USE IS WITHIN THE SCOPE OF THE RIGHT TO BE FORGOTTEN

The right to be forgotten provides that the "fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data" should be protected.[50] The right to be forgotten strengthens the rights of data subjects when their data is used or misused, by giving them the right to control the use of their image when the image is shared by third parties.[51] The right to be forgotten is not a mechanism that will actually prevent the misuse of personal images. Rather, it provides

---

[49] *See, e.g.*, Wong, *A Conceptual Analysis*, *supra* note 47; Working Party Opinion, *supra* note 41.

[50] Data Directive, *supra* note 9, at art. 1; *see also* General Data Protection Regulation, *supra* note 27, at art. 17.

[51] *See supra* Section II.C.

a remedy for people who have had their personal images misused. For example, the right enables a person whose data has been misused to request the removal of the data; it does not prevent or provide protection against the misuse of the data. This right extends to data such as personal images that are uploaded and shared on social networks or appear in search results.[52] Thus, a person would not be able to rely on the right to be forgotten to prevent the misuse of their image, but would be able to request that the data controller remove the misused image from the network's system.

The right to be forgotten operates in a number of different situations. The first is where the data is no longer relevant or if it is outdated (as in *Google Spain v. Gonzalez*).[53] The second is when a person withdraws the consent on which the processing of the data is based.[54] Under the GDPR, the withdrawal must be unambiguous. When people sign up to a social network, they agree to the social network's terms of use. By agreeing to the terms, they are providing their consent to the network to use, collect, process, and store their images. By entering into a social network contract, people give their consent to the network to capture their photographs legitimately. However, people often do not understand what the consent entails.[55] Social network contracts allow personal images to be passed to third-party affiliates for use in advertising or marketing purposes. Consequently, once a person has consented to the network's terms of use, their photographs and personal images—as well as the ways in which their images may be used—are out of their control.[56]

Under the GDPR, users may withdraw their consent allowing social networks to process, store, and collect their data.[57] Such withdrawal of consent has particularly acute ramifications when a user

---

52 *See id*.

53 *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317, ¶ 49 (May 13, 2014).

54 *See* General Data Protection Regulation, *supra* note 27, at art. 7 (providing that a person can withdraw their consent).

55 *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1884 (2013).

56 *See generally* Bernal, *supra* note 4; *see also* Ausloos, *supra* note 1, at 146; Fazlioglu, *supra* note 1, at 151; Mantelero, *supra* note 4, at 230.

57 *See* General Data Protection Regulation, *supra* note 27, at art. 7(3) (providing that "[t]he data subject shall have the right to withdraw his or her consent at any time").

decides to terminate their social media account.[58] When a user terminates their social network contract, the network is still able to use any images of the (former) user that have been reshared on the network—even if the user removes all of their content on their profile page from the network by deleting their account. This is due to the fact that users agree to the social network's terms of use which include the non-exclusive licensing of their content.[59] The non-exclusive license clause provides that a social network may continue to use the images after the contract is terminated. This means that a network may be in breach of the GDPR if it continues to use people's images after the contract ends. Accordingly, when this occurs, a person would be able to use the right to be forgotten to request that the network remove their images from the network.

The third situation where the right to be forgotten might apply is when a person objects to the *processing* of their data.[60] A situation of this kind might occur, for example, when a person takes a photograph of a third party who does not want their image to be shared online. The GDPR defines "processing" broadly as:

> any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as *collection*, recording, organisation, structuring, *storage*, *adaptation or alteration*, retrieval, consultation, *use*, *disclosure by transmission*, *dissemination or otherwise*

---

[58] Particularly significant are Facebook's Terms of Service. In relation to the right to be forgotten, any requests from its users to erase the data would have to be erased from all of Facebook's data-storage systems, not just its platform. This contravenes Facebook's new Terms of Service, which also state that the network can access archived copies of users' shared data despite the user deleting or deactivating their account. *See, e.g.*, *Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/update [perma.cc/4JCT-M2KB]; *Terms of Service*, FACEBOOK, https://www.facebook.com/legal/terms/ [perma.ccU7PY-NNHQ].

[59] *See, e.g.*, Georgiades, *supra* note 2, at 436–38; VAN ALSENOY ET AL., *supra* note 2; *Statement of Rights and Responsibilities*, FACEBOOK (Jan. 30, 2015), https://www.facebook.com/legal/terms/previous [perma.cc/9BH6-ECXH]; *Terms of Service*, TWITTER (Jan. 1, 2020), https://twitter.com/en/tos [perma.cc/TEX8-24WU]; *Terms of Use*, INSTAGRAM (Apr. 19, 2018), https://help.instagram.com/478745558852511 [perma.cc/LY97-4SG3].

[60] An objection to the processing of a data subject's data may be aimed at a data controller such as a search engine like Google, or a social network site like Facebook.

> *making available*, *alignment or combination*, restriction, erasure or destruction.[61]

When a person takes their own photograph or a photograph of a third party, they are potentially "processing" data in so far as they are collecting and recording the image. Similarly, the uploading of an image on a social network page may fall within "use, disclosure, dissemination or otherwise making available."[62]

A fourth situation where the right to be forgotten may apply is where a data subject's information is transferred for processing to a country outside of Europe that does not protect data to the standard required by European law.[63] Specifically, the right to be forgotten allows data subjects to object if their data has been transferred to third countries that do not safeguard or protect the fundamental right to respect for private life and freedom of that right that the European Union law guarantees.[64] *Schrems v. Data Protection Commissioner* stands for this proposition, as the Court of Justice held that the existing safe harbor provisions which provided that a data subject's data may be transferred to a third country were invalid.[65]

---

61 General Data Protection Regulation, *supra* note 27, at art. 4(2) (emphasis added).

62 *Id.*

63 Case C-362/14, Schrems v. Data Protection Comm'r, 56 I.L.M. 245, ¶ 71 (2015) (EU). The Court of Justice stated that:

> [A]s is apparent from the very wording of Article 25(6) of Directive 95/46, that provision requires that a third country 'ensures' an adequate level of protection by reason of its domestic law or its international commitments. Secondly, according to the same provision, the adequacy of the protection ensured by the third country is assessed 'for the protection of the private lives and basic freedoms and rights of individuals.'

Id.

64 *Id.* at ¶¶ 90–91 (citing C-293/12 and C-594/12, Digital Rights Ireland and Others, 2014 E.C.R 238, ¶¶ 52–55); *see also* EUROPEAN COURT OF HUMAN RIGHTS COUNCIL OF EUROPE, EUROPEAN CONVENTION ON HUMAN RIGHTS, art. 8 (June 1, 2010), www.echr.coe.int/Documents/Convention_ENG.pdf [https://perma.cc/5MRF-FUFJ] ("Everyone has the right to respect for his private and family life, his home and his correspondence.").

65 *Schrems*, 56 I.L.M. 245, at ¶ 107. In a press release outlining the decision, the Court of Justice noted that the Irish High Court had to examine:

> [Schrem's] complaint with all due diligence and, at the conclusion of its investigation, . . . decide whether, pursuant to the directive, transfer

Furthermore, the Court of Justice held that a data subject may object to the transfer or processing of their data to a third country if it can be shown that the third country does not protect personal data in accordance with European law.[66] As the Court of Justice said:

> [T]he Commission found that the United States authorities were able to access the *personal data transferred from* the *Member States to the United States* and *process it in a way incompatible*, in particular, with the purposes for which it was *transferred, beyond* what was strictly necessary and proportionate to the protection of national security.[67]

The Court of Justice also noted that when transferring a data subject's data to a third country, the data subject would need to have "administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, *rectified or erased*."[68] Consequently, the right to be forgotten allows data subjects to object if their data have been transferred to third countries which do not safeguard or protect the fundamental right to private life and freedoms that are guaranteed within the EU.[69]

IV. EXCEPTIONS TO THE RIGHT TO BE FORGOTTEN

There are a number of exceptions to Article 17 ('the right to be forgotten') in the GDPR. One of the most important exceptions is found in Article 80 of the GDPR*,* which provides an exception for journalists and artists for the processing of personal data and freedom of expression.[70] This requires that a data subject's request to

---

> of the data of Facebook's European subscribers to the United States should be suspended on the ground that that country does not afford an adequate level of protection of personal data.

European Commission Press Release 117/15, The Court of Justice Declares that the Commission's US Safe Harbour Decision Is Invalid (Oct. 6, 2015).

66 *Schrems*, 56 I.L.M. 245, at ¶ 107.

67 *Id.* at ¶ 90 (emphasis added).

68 *Id.* (emphasis added).

69 *Id*. ¶ 91.

70 *Compare* General Data Protection Regulation, *supra* note 27, at art. 80, *with* Data Directive, *supra* note 9, at art. 9 (previous exception for "processing of personal data

remove data must be balanced against freedom of speech or expression but also the public's interest in having access to the information.[71] For example, as noted above, the Court in *Google Spain v. Gonzalez* held that outdated information lies beyond the scope of the public's interest.[72]

The balancing of freedom of expression and the right to be forgotten is critical when people share and exchange personal images on social networks. The GDPR recognizes that when people upload and share images within a social network, there are competing interests between the users who upload images, the users that access images, and the subjects of the images. When deciding how the balance between these interests is to be drawn, the court may take a variety of factors into account. In *Google Spain v. Gonzalez*, the court considered "the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life."[73] In the case of public figures, the courts seem willing to give more weight to the public's right to know than their ability to keep matters private, because "the interference with [a famous person's] fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question."[74]

One of the important consequences of the right to be forgotten is that it enables people to regain control over their data. One of the main arguments against the right to be forgotten is that it threatens freedom of speech. It appears that if people did regain control, this

---

carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression"). *See also, e.g.*, Fazlioglu, *supra* note 4, at 154; Anne Flanagan, *Defining "Journalism" in the Age of Evolving Social Media: A Questionable EU Legal Test*, 21 INT'L J. L. & INFO. TECH. 1, 1 (2012); Mantelero, *supra* note 4, at 234; Giovanni Sartor, *The Right to Be Forgotten: Balancing Interests in the Flux of Time*, 24 INT'L J. L. & INFO. TECH. 72, 72 (2015).

71 *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317, ¶ 81.

72 *Id.* ¶ 98.

73 *Id.* ¶ 81.

74 *Id.* ¶ 97.

would be detrimental to a person's freedom of expression or speech. The detriment potentially is attributed to overriding need to maintain control of the information that is uploaded by users. This is because every person has the right to express themselves and may do so by uploading images of third parties. More often, it means that people whose images are captured and uploaded lose their ability to control the use of their image because it is captured by another person who is the creator of the image. Thus, when images are captured and uploaded the use of the images is subject to the social network's terms of use which means that the network controls the use of the images. While these concerns are valid, they often disregard the key issue redressed by the right to be forgotten, which is that large internet firms such as Google, Facebook, and Microsoft have turned the sharing of images online into a source of advertising revenue and thus have developed a business model that depends on the collection and storage of vast quantities of personal images online.[75] For example, in *Fraley v. Facebook*, the court found that Facebook's Sponsored stories misappropriated users' profile images because users did not explicitly agree to have their image used in connection to the Sponsored Stories feature.[76]

Another exception that potentially restricts the operation of the right to be forgotten is the "personal or household purposes" exception. According to Article 2 of the GDPR,[77] where the processing of personal data is by a "natural person in the course of a purely personal or household activity," it will fall outside the scope

---

75 *See* Bernal, *supra* note 4.

76 Fraley v. Facebook, Inc., 830 F. Supp. 2d 785, 803–06 (N.D. Cal. 2011). Judge Koh dismissed Facebook's claim that users had consented to the use of their profile images to be used because the plaintiffs were "likely to be deceived likely to be deceived into believing [they] had full control to prevent [their] appearances in Sponsored Story advertisements while otherwise engaging with Facebook's various features, such as clicking on a 'Like' button, when in fact members lack such control." *Id.* at 814–15. *See* Jesse Koehler, Note, Fraley v. Facebook*: The Right of Publicity in Online Social Networks*, 28 BERKELEY TECH. L.J. 963, 964 (2013); *see also generally* Francesca Grea, *To Like or Not to Like:* Fraley v. Facebook*'s Impact on California's Right of Publicity Statute in the Age of the Internet*, 47 LOY. L.A. L. REV. 865, 869 (2014).

77 General Data Protection Regulation, *supra* note 27, at art. 2.

of the Regulation.[78] One example where the purely personal or household exception may not apply to personal data that is processed in the course of purely personal or household activity is highlighted in *Bodil Lindqvist v. Åklagarkammaren i Jönköping*.[79] The court in this case held that the personal or household activity exception did not apply to referring to people's names on an internet page that identified them by name or by other means because the information related to charitable and religious activities.[80] However, the personal and household exception covers most of the activities that people engage in online, including uploading and sharing a personal image on a personal profile page.[81]

The household exception predates the GDPR, as it had been incorporated into the 1995 European Data Directive 95/46/EC. In 1995, the internet was in its infancy, and most people's access to information was limited to written records or held on a computer that did not have internet.[82] Given that the exception effectively excludes individuals from the right to be forgotten, it has very important consequences for how useful the right to be forgotten may be in protecting against online misuse of personal images.[83]

---

[78] *Id.* at art. 2(2)(c). *See also* Zuzanna Warso, *There's More to It Than Data Protection-Fundamental Rights, Privacy and the Personal/Household Exemption in the Digital Age*, 29 COMPUTER L. & SECURITY REV. 491, 491–92, 495 (2013); Wong, *A Conceptual Analysis*, *supra* note 47, at 147; *see generally* Wong, *Anybody Is a Data Controller*, *supra* note 43.

[79] Case C-101/01, Bodil Lindqvist v. Åklagarkammaren i Jönköping, 2003 E.C.R. I-12992, ¶ 45.

[80] *Id*.

[81] *See* Article 29 Data Protection Working Party, *Annex 2: Proposals for Amendments Regarding Exemption for Personal or Household Activities*, EUR. COMMISSION (Feb. 27, 2013), https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20130227_statement_dp_annex2_en.pdf [https://perma.cc/7A2U-BQPW] [hereinafter Working Party, *Annex 2*].

[82] *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2013, Opinion of AG Jääskinen, ¶ 27 ("In 1995, generalised access to the internet was a new phenomenon. . . . However, it is clear that the development of the internet into a comprehensive global stock of information which is universally accessible and searchable was not foreseen by the Community legislator."); *see also* Claire Bessant, *The Application of Directive 95/46/EC and the Data Protection Act 1998 When an Individual Posts Photographs of Other Individuals Online*, 6 EUR. J.L. & TECH. 1, 2 (2015).

[83] *See generally* Bessant, *supra* note 82.

V. REDRESSING AND REMEDYING THE MISUSE OF PERSONAL DATA BY COMPANIES

Social networks increasingly intrude on people's privacy because they have a "great data concentration"[84] about their user's online interactions. Companies such as Google, Instagram, Facebook, Microsoft, and Twitter collect, process, and store vast amounts of personal data. These companies retain a significant amount of their users' data which increasingly are used to intrude on people's personal lives online. For example, Facebook tracks their users even if they are not logged into the Facebook platform; as such it acquires data about the user without their knowledge.[85] Social networks historically promoted "the idea that sharing information is a social norm and that privacy or oblivion is an outdated concept."[86] By encouraging people to share their images and personal information, companies like Facebook, Google, and Instagram (to name a few) collect vast amounts of data. This collection of data highlights that "the same companies are progressively collecting an enormous amount of data in order to profile individuals and, above all, to extract predictive information with high economic, social, political and strategic value."[87] As Mantelero argues, "[i]n a world where it is assumed that no value is attributed to privacy and oblivion, the only ones to gain from this abandonment of old rights are the owners of these platforms or services which have an exclusive and comprehensive view of the entire mass of data."[88]

Social networks "represent[] an antimony because they do not share the information taken from the data and, even though they give little value to privacy and affirm the end of oblivion (describing life as a timeline); they extract a high value from this data."[89] Thus, when social networks store and collect people's images, the network

---

84 Mantelero, *supra* note 4, at 234.

85 *See* Jason Murdock, *Facebook Is Tracking You Online, Even If You Don't Have An Account*, NEWSWEEK (Apr. 17, 2018, 6:53 AM EDT), https://www.newsweek.com/facebook-tracking-you-even-if-you-dont-have-account-888699 [https://perma.cc/Q6AE-XAS2].

86 Mantelero, *supra* note 4, at 234.

87 *Id*.

88 *Id*.

89 *Id*.

yields power over their users, because even if the user can delete their photographs on their profile page, they cannot control the use of their personal image on their friend's profile page. As Mantelero suggests, the data collected and stored by social networks represents "not only money, but also power," and this power in turn facilitates the ongoing exploitation and the expropriation of users' data.[90] The right to be forgotten is an "attempt to reduce the amount of data collected" and this reduction would undermine the social network's power.[91] Mantelero states that "[f]or this reason the owners of big data have tried to make it more difficult to change privacy settings, have used technical devices to track users in a persistent way and have thus evoked the end of the privacy era."[92]

One of the consequences of the right to be forgotten is that it enables people to regain control over their data by reshifting the power imbalance that exists between corporations and individuals. The right to be forgotten illuminates the critical issue of users being given the right to delete the data which is controlled by social networks.[93] These companies retain a significant amount of their users' data (images), which increasingly intrudes on people's personal lives and thus diminishes a user's autonomy over their own image. As Bernal argues, this "kind of transfer of power, that kind of re-balancing, could have possibilities to redress the current imbalance over personal data—and to help re-establish at least some control that people both have lost and feel that they have lost."[94]

While the right to be forgotten is not a mechanism that will actually prevent the misuse of personal images, it does provide an ex post facto remedy for people whose personal images have been misused. This is because the right to be forgotten enables people to request that when their images have been misused they are deleted from the network.[95] In this sense, the right to be forgotten would provide a practical solution for social media users as well as any

---

90 *Id*.
91 *Id*.
92 *Id.*
93 *See id.*
94 Bernal, *supra* note 4, at 4.
95 *See* discussion *supra* Part I.

third parties (who may be non-users) that object when their image is captured and is uploaded or shared online.

VI. CRITICISMS OF THE RIGHT TO BE FORGOTTEN

A number of arguments have been made against the right to be forgotten. Insofar as the right allows an individual to have data about them deleted or removed, there is a concern that it will facilitate self-censorship.[96] The fear here is that the right to be forgotten will allow people to rewrite history[97]; i.e., that it will allow people to manage public information in order to ensure that only certain perspectives of them are in the public domain.[98] While there is a chance that the right to be forgotten may be used in this way, such use would require the courts to adopt a very broad reading of the type of situations where the right to be forgotten might be applied. On most readings,[99] such cases of "censorship" would only be allowed in limited and presumably justified situations, for example when the data is out-dated, irrelevant, or when a person withdraws their consent to have the data published.[100]

Another concern with the right to be forgotten is that it will restrict freedom of speech and/or expression.[101] It is clear that the right to be forgotten will remove information from the public domain. In introducing the right to be forgotten the intention of the European legislators was not to restrict freedom of the press or free

---

96 *See* Giurgiu, *supra* note 4, at 367–68; Koops, *supra* note 5, at 232; *see generally* Bennett, *supra* note 32; Pere Simón Castellano, *The Right to Be Forgotten Under European Law: A Constitutional Debate*, 16 LEX ELECTRONICA 1 (2012); Omer Tene & Jules Polonetsky, *Privacy In the Age of Big Data: A Time for Big Decisions*, 64 STAN. L. REV. ONLINE 63 (2012); Smet, *supra* note 32; Weber, *supra* note 32.

97 *See generally* Bennett, *supra* note 32; Smet, *supra* note 32; Tene & Polonetsky, *supra* note 96; Weber, *supra* note 32.

98 Some scholars argue that the right to be forgotten needs to be framed in a different language, such as "the right to delete." *See, e.g.*, Bernal, *supra* note 4; *see generally* Bennett, *supra* note 32; Smet, *supra* note 32; Tene & Polonetsky, *supra* note 96; Weber, *supra* note 32.

99 *See generally* Julia Powles, *The Case That Won't Be Forgotten*, 47 LOY. U. CHI. L.J. 583, 586–90, 606–10 (2015); Lawrence Siry, *Forget Me, Forget Me Not: Reconciling Two Different Paradigms of the Right to Be Forgotten*, 103 KY. L.J. 311, 328–31 (2015).

100 *See generally* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317; Bennett, *supra* note 32; Bernal, *supra* note 4; Smet, *supra* note 32; Tene & Polonetsky, *supra* note 96; Weber, *supra* note 32.

101 *See* Koops, *supra* note 5, at 238–39.

speech; rather it was to protect an equally important right: personal privacy. Given that the GDPR includes an exception for free speech, it seems that many of the complaints about free speech are about the balancing of the rights and where the line is to be drawn. Any risk to free speech or freedom of the press has been incorporated into the GDPR and any requests must be balanced against freedom of expression and the public interests.[102]

A number of other problems exist with the right to be forgotten; one of which is that there are many aspects of the new regulation and its application that are uncertain. The right to be forgotten itself is not problematic, but the application of the right may potentially give rise to problems. For example, when personal images are misused online, it is unclear whether the social network or the individual would be responsible for removing the image.[103] This is important because the data subject may not be the owner of the image and would need to seek permission from the copyright owner or social network to remove the photograph on their behalf. For example, when a person captures an image of a third party in a photograph, the creation of the image gives rise to copyright protection. As such

---

[102] This is because there are a number of exceptions to the right to be forgotten as stated in General Data Protection Regulation, art. 17(3), which provides:

> Paragraphs 1 and 2 will not apply to the extent of the processing is necessary:
>
> 1) for exercising the right of freedom of expression and information;
> 2) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
> 3) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
> 4) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
> 5) for the establishment, exercise or defence of legal claims.

General Data Protection Regulation, *supra* note 27, at art. 17(3).

[103] *Id.* at art. 17(1).

it is the creator of the image and not the subject that owns the copyright.[104] This means that the subject in the image may not have a right to remove their image from a third-party profile page.[105] As a result, it may be unclear whether the data subject has a claim on the copyright owner to remove their image from their personal profile page. It is also uncertain whether the data subject has a claim on the social network provider to remove their image from the network.[106] The distribution of responsibilities in the removal of data is "not particularly clear, since both the SNS provider and the user/uploader are being designated as data controllers in the standard interpretation of the Directive."[107]

Another problem with the right to be forgotten relates to the scope of the personal or household purpose exception.[108] The problem with Article 2 of the GDPR is that it is unclear "whether an individual posting personal data openly for a worldwide, unrestricted audience can still be considered to be processing the data for personal or household purposes."[109] This is because a person who disseminates an image on a social network may still fall within a personal or household purpose.[110]

Another uncertainty that may arise with the right to be forgotten is the way in which the right will apply in relation to photographs, as distinct from written information. Although photographs clearly will fall within the definition of "data," it is less clear to predict whether a photograph will trigger the right to be removed. For example, it is not clear what will need to change for a photograph to be declared "irrelevant," "inadequate," or "excessive."[111] Most of

---

104 *See generally* Eugenia Georgiades, *The Limitations of Copyright: Sharing Personal Images on Social Networks*, 40 EUR. INTELL. PROP. REV. 230 (2018).

105 *See id*.

106 *See* Koops, *supra* note 5, at 239.

107 *Id.* at 238 (citing Article 29 Data Protection Working Party, *Opinion 1/2010 on the Concepts of "Controller" and "Processor"* (2010), at 21).

108 *See* General Data Protection Regulation, *supra* note 27, at art. 2(c).

109 Working Party, *Annex 2*, *supra* note 81, at 3.

110 *See* Norberto Nuno Gomes de Andrade, *Oblivion: The Right to Be Different . . . From Oneself: Reproposing The Right to Be Forgotten*, 13 REVISTA DE LOS ESTUDIOS DE DERECHO Y CIENCIA POLÍTICA DE LA UOC 122, 128 (Feb. 2012).

111 See *Google Spain v. Gonzalez*:

the examples given where the right to be forgotten applies are in relation to textual data—newspapers stories and the like—not photographs.[112] While this is an issue that needs clarification, it would seem that photographs are capable of triggering the right to be forgotten in certain situations. It will be more difficult to establish the criteria required for applying a right to be forgotten for a photograph than it is with textual data. Although the right to be forgotten may not be exercised in relation to trivial matters such as changes in fashion or a bad haircut, it may apply where a photograph presents factual information that later becomes irrelevant or where the image contains sensitive data.[113] For example, a photograph could contain

---

> It follows from those requirements, laid down in Article 6(1)(c) to (e) of Directive 95/46, that even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed.

Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317, ¶ 93; *see also* General Data Protection Regulation, *supra* note 27, at Recital 65 ("A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. *In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her,* or where the processing of his or her personal data does not otherwise comply with this Regulation.") (emphasis added).

[112] *See* Rhiannon Williams, *Telegraph Stories Affected by the EU 'Right to Be 'Forgotten,'* TELEGRAPH (Sept. 3, 2015), http://www.telegraph.co.uk/technology/google/11036257/Telegraph-stories-affected-by-EU-right-to-be-forgotten.html [https://perma.cc/NT2Y-8X2P] (demonstrating that most of stories in *The Telegraph* affected by the right to be forgotten pertain to articles rather than photographs); *see generally* Philip Delves Broughton, *Four Years for British Convent Girl Who Ran a Ring of 600 Call Girls*, TELEGRAPH (Oct. 24, 2003), https://www.telegraph.co.uk/news/uknews/4190437/Four-years-for-British-convent-girl-who-ran-a-ring-of-600-call-girls.html [https://perma.cc/MS7K-9HRE]; *Italian Job Stunt Lands Mini Driver a Ban*, TELEGRAPH (Nov. 10, 2008, 8:26 PM GMT), https://www.telegraph.co.uk/news/newstopics/howaboutthat/3419280/Italian-Job-stunt-lands-Mini-driver-a-ban.html [https://perma.cc/8YMP-DTQT].

[113] For example, four images had been removed from *The Telegraph*. The images in question relate to Max Mosley's 2008 sex scandal. *See generally* Williams, *supra* note 112.

information concerning a person's political views or revealing information about their health.[114]

The right to be forgotten raises a number of practical issues. One issue is that the removal of images may be difficult to implement.[115] Even though a network may remove an image, it may still be possible to view the image online.[116] This is because it may take some time to remove the image from the cache memory, or the images may be stored on a person's hard drive or in the cloud.[117] As Ausloos says, even if "notice and take down procedures might take content out of the (public) sight," it does not result in the removal of the images from the data user's servers.[118] Even if a person chooses to remove their images from their own profile page, the image may still be available if the image has been shared and reshared. These problems are exacerbated by the global nature of the internet, which may place images in jurisdictions with little or no protection. There is little use in demanding an image be removed in one country if users can simply obtain the image from another country.

VII. SHOULD OTHER COUNTRIES ADOPT THE RIGHT TO BE FORGOTTEN?

A. Imagining an Australian Right to Be Forgotten

If a right to be forgotten were adopted in Australia, it would help to restore the imbalance between people whose images are captured

---

114 *See* General Data Protection Regulation, *supra* note 27, at rec. 10; *see also* Data Directive, *supra* note 9, at art. 2.

115 *See* Cecile de Terwangne, *Internet Privacy and the Right to Be Forgotten/Right to Oblivion*, 13 REVISTA DE INTERNET, DERECHO Y POLÍTICA 109, 117 (2012); *see also generally* Kathryn Smith, *The Right to Be Forgotten: Legislating for Individuals to Regain Control of Their Personal Information on Social Networks*, 7(1) REINVENTION (2014).

116 *See* Terwangne, *supra* note 115, at 117.

117 *See id.*

118 Ausloos, *supra* note 1, at 148. Ausloos states that while European citizens can request Facebook to send them all personal data in Facebook's possession, Facebook still keeps track of your removed data as well. *See* Omer Tene, *Privacy: The New Generations*, 1 INT'L DATA PRIVACY L. 15, 25 (2010); *see also generally* Meg Leta Ambrose & Jef Ausloos, *The Right to Be Forgotten Across the Pond*, 3 J. INFO POL'Y 1 (2013).

and those who control the data.[119] An Australian version of this right would also enable people to regain control over their images on social networks. If introduced it "could give individuals the possibility of more control over their data and hence more autonomy. It could directly reduce the amount of data that is held—hence that is vulnerable—as individuals exercise their right to delete."[120] An Australian right to be forgotten would also address broader privacy concerns with respect to social networks. It would help to respond to the fact that social networks increasingly chip away at personal privacy. Particularly concerning is the way that people's personal images are prone to misuse by those who collect information, as the data can be aggregated and combined with other forms of data, which can then be used for profiling.[121]

It is arguable that the right to be forgotten might also force social networks to justify why they are holding information.[122] As Bernal said:

> It could force those holding data to justify why they're holding it—in such a way that the data subjects understand, for if data subjects cannot understand why the data is wanted, they might simply delete it. If there is a benefit and that benefit is made clear, why would an individual wish to delete that data? Most importantly of all, the fact that data could be deleted at any time could encourage the development of business models that do not rely on the holding of so much personal data.[123]

Insofar that the right to be forgotten "reflects a paradigm shift" in privacy, where the individuals have "power[, they] . . . can and

---

119 *See generally* Paul De Hert & Vagelis Papakonstantinou, *The Proposed Data Protection Regulation Replacing 95/46/EC: A Sound System for the Protection of Individuals*, 28 COMPUTER L. & SECURITY REV. 130 (2012); Jasmine McNealy, *The Emerging Conflict Between Newsworthiness and the Right to Be Forgotten*, 39 N. KY. L. REV. 119 (2012); Robert Kirk Walker, *The Right to Be Forgotten*, 64 HASTINGS L.J. 257 (2012).

120 Bernal, *supra* note 4.

121 *See id.*

122 *See id.*

123 *Id.*

should restrict the actions of those who might oppress, abuse or take advantage of those individuals."[124] This right would help individuals to regain control over how their personal images are used. For too long, in American culture and to some extent Australian culture, privacy interests have been overshadowed by, or come second to, freedom of expression and speech. As it stands, a right to be forgotten would be useful in Australia because it would potentially close some of the gaps in the existing legal protection for personal images. While there is some legal protection, the protection is fragmented and piecemeal under federal and common law. For example, the Australian Privacy Act 1988 (Cth) does not protect personal images that are uploaded by individuals.[125] An aggrieved person would need to seek a remedy under other areas of law such as copyright or tort—for example, the tort of breach of confidence. However, it should be noted that the tort of breach of confidence may only protect personal images, if the misuse of the image relates to matters of an intimate or sexual nature. Presently, Australian law provides specific protection for certain types of images such as those of an intimate (and/or of a sexual) nature. Despite this, there is no recognized image right or a right to one's image, which leaves people vulnerable and unprotected when an image is captured and uploaded by a third party. In particular, a right to be forgotten would enable people to control use of their image, particularly when it is shared by other people on social networks.[126] Incorporating a right to be forgotten in the Australian Privacy Act would provide people with similar

---

124 *Id*.

125 Privacy Act 1988 (Cth).

126 Virginia Da Cunha is an Argentinian singer, dancer, model and actress who had posted various pictures of herself in short shorts, swimsuits, tank tops, and at least one sexually provocative pose on Twitter and Facebook. She sued Yahoo Argentina for linking and showing results of her name and image to websites offering sexual content, pornography, escorts, and other related activities. *See* Juzgado de Primera Instancia [1A INST.] [Court of First Instance], 29/7/2009, "Da Cunha, Virginia c. Yahoo de Argentina s/ Daños y Perjuicos," (Resulta, I, para. 3) (Arg.) [hereinafter Opinion of Judge Simari]. Da Cunha was successful at first instance; however, she lost on appeal in 2010. *See* Cámara Nacional de Apelaciones en lo Civil de la Capital Federal [CNCiv.] [National Court of Civil Appeals of the Federal Capital], sala D, 10/8/2010, "Da Cunha Virginia c/ Yahoo de Argentina SRL y otro s/ Daños y Perjuicios," (Arg.); *see also generally* Edward L. Carter, *Argentina's Right to Be Forgotten,* 27 EMORY INT'L L. REV. 23 (2013).

privacy rights to European citizens who have clearer and stronger data protection.

A right to be forgotten could be adopted in Australia by amending the Australian Privacy Act and the Australian Privacy Principles (APPs) to include "data subject" protection rights similar to the EU's GDPR.[127] Incorporating data subject rights in Australia's Privacy Act would provide more relief for people when their image is misused.

As noted in Part III, *infra*, the GDPR allows a person to object to the transfer of their data to another country when the standard of data protection is not to the European standard.[128] The Australian Privacy Act has a similar provision under the Australian Privacy Principles (APPs) that relates to cross-border disclosure of personal information.[129] However, it is uncertain whether the Australian Privacy Principle 8 would provide adequate protection to prevent an Australian national's data from being disclosed to a third-party country, because the text is silent on whether the disclosure of the information to a third party would constitute a "transfer." Australian Privacy Principle 8 provides that, prior to any disclosure of personal information to an overseas recipient, there must be reasonable steps taken to ensure that the overseas recipient does not breach the Australian Privacy Principles.[130] What is "reasonable" is not defined in the legislation which makes it difficult for determining whether a person in Australia would have the same rights as European citizens. Moreover, where data is processed and stored overseas, it may also be difficult to prove that data is processed, collected, or stored in Australia, or by an Australian corporation. Consequently, provisions similar to Article 21 of the GDPR, i.e., the

---

127 *See* General Data Protection Regulation, *supra* note 27*,* at art. 4(1).

128 *See generally id*.

129 *See Australian Privacy Principles* (Cth) c 8 (July 2019) (Austl.), https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information [https://perma.cc/99CE-NH9M].

130 *Id.* ("[B]efore an APP entity discloses personal information about an individual to an overseas recipient, the entity must take reasonable steps to ensure that the recipient does not breach the APPs in relation to that information. Where an entity discloses personal information to an overseas recipient, it is accountable for an act or practice of the overseas recipient that would breach the APPs (s 16C).").

right to object to the transfer of personal data, should be adopted in Australia.

B. Imagining a Right to be Forgotten in the United States

Over the years, many legal scholars have argued against adopting a right to be forgotten in the United States because it would oppress freedom of expression and speech.[131] Given the serious data breaches that occurred with Facebook's Cambridge Analytica scandal,[132] and at Equifax,[133] there has been a stronger accountability put towards American companies which operate services in Europe. In particular, data breaches that have occurred in Europe have alerted American legislators towards recognizing the need for stronger privacy protection for personal data.[134] Consequently, data breaches that occurred in Europe have impacted the United States by demonstrating the need for stronger data privacy protection.[135] American companies that provide online services to European citizens and operate in Europe must comply with the GDPR. For example, in Europe, Google received over 2.5 million requests for data erasure since the right to be forgotten was introduced in 2014.[136] As a result of *Google Spain v. Gonzalez*,[137] the European

---

131 *See generally* Eltis, *supra* note 32; McGoldbrick, *supra* note 32; Smet, *supra* note 32; Daniel J. Solove, *'Conceptualizing Privac*y, 90 CALIF. L. REV. 1087 (2002); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477, 564 (2006); Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L. J. 967 (2003); Weber, *supra* note 32.

132 *See* Emma Graham-Harrison & Carole Cadwalladr, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, GUARDIAN (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election [https://perma.cc/9R8J-NZVC].

133 *See* Seena Gressin, *The Equifax Data Breach: What to Do*, FED. TRADE COMM'N (Sept. 8, 2017), https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do [https://perma.cc/KJ6S-ZKX6].

134 *See* Hillary C. Webb, Note, *People Don't Forget: The Necessity of Legislating Guidance in Implementing a U.S Right to Be Forgotten*, 85 GEO. WASH. L. REV. 1304, 1331 (2017).

135 *See generally id.*

136 Stuart Lauchlan, *The EU's Right to Be Forgotten Should Stay Within the EU—An Important Legal Opinion in a Fake News World*, DIGINOMICA (Jan. 13, 2019), https://diginomica.com/the-eus-right-to-be-forgotten-should-stay-within-the-eu-an-important-legal-opinion-in-a-fake-news-world [https://perma.cc/T6FK-NZH2].

137 Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317 (May 13, 2014).

Court of Justice introduced the right for people to be able to request that their data be removed. While companies such as Facebook and Google have to comply with the requirements of the GDPR in Europe, non-European citizens are not afforded the same level of data protection.[138]

In the United States, data protection laws remain stagnant because the Federal Trade Commission ("FTC") is the main venue for most privacy policy making.[139] The United States does not have a designated data protection agency similar to those created by the GDPR, and the courts in the United States "mainly rule on the constitutionality of regulations, legislation, and government actions."[140] Despite playing an active role in data protection, the FTC's authority is limited to data breaches that fall within the scope of prohibiting unfair or deceptive practices.[141] Leticia Bode and Leta Jones note that the FTC is "limited to enforcement of unfair or deceptive data practices, generally tied to the terms of service drafted and published by the data collectors and controllers and drafting policy recommendations and reports."[142] This in effect limits the authority of the FTC to particular circumstances of data breaches that arise out of unfair or deceptive practices.[143]

The U.S. Constitution enables the various States to develop and implement privacy protection under their respective law.[144] Each State incorporates the protection of image rights either under statute

---

138 *See* Case C-507/17, Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL), 2019 E.C.R. 772 (Sept. 24, 2019) (limiting the right to be forgotten to only EU countries).

139 *See* Leticia Bode & Meg Leta Jones*, Ready to Forget: American Attitudes Toward the Right to Be Forgotten*, 33 INFO. SOC'Y 76, 77 (2017) (citing Daniel Solove & Woodrow Harzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 600 (2014)).

140 *Id.*

141 *See* Federal Trade Commission Act § 5, 15 U.S.C. §§ 41–58 (2006)*; see also* Bode & Jones, *supra* note 139.

142 *See* Bode & Jones, *supra* note 139, at 77.

143 In *In re Snapchat*, the FTC held that Snapchat's claims that images would disappear were false. Decision & Order, In re Snapchat, Inc., F.T.C. Docket No. C-4501 (Dec. 23, 2014); *see also* F.T.C. v. Wyndham Worldwide Corp., 799 F.3d. 236 (3d Cir. 2015) (hotel chain failed to protect customers' personal information stored on their information systems).

144 *See* U.S. CONST. amend. X.

or through common law.[145] In their seminal work, Warren and Brandeis argued for the protection of people's privacy as photography and photographic equipment evolved.[146] Concerned that the development of photography intruded on people's lives, Warren and Brandeis attempted to protect image rights under the tort of privacy.[147] Building upon Warren and Brandeis' tort of privacy, William Prosser identified four torts for invasions of privacy.[148] These torts are as follows:

> (1) intrusion upon the plaintiff's seclusion or solitude or into his private affairs;
> (2) public disclosure of embarrassing private facts about the plaintiff;
> (3) publicity which places the plaintiff in a false light in the public eye; and
> (4) appropriation for the defendant's advantage, of the plaintiff's name or likeness.[149]

At the state level, a person may draw upon either of the four torts to protect specific invasions of privacy[150] if the state has incorporated them in their common law. The most relevant of the four torts which more closely relates to personal images is the appropriation of a person's likeness, also known as the right of publicity.[151] For example, Californian courts do protect personal images in the way of personality rights; however, the protection is limited and balanced with freedom of speech.[152] The courts provide that "no cause of action will lie for the '[p]ublication of matters in the public interest, which rests on the right of the public to know and the freedom of the

---

145 *See generally* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).

146 *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

147 *Id*. at 195–96 (citing Marion Manola v. Stevens & Myers, *N.Y. Supreme Court*, N.Y. TIMES (June 15, 18, 21, 1890)).

148 *See* Prosser, *supra* note 145, at 389.

149 *Id*.; *see also* Warren & Brandeis*, supra* note 146, at 197.

150 Prosser, *supra* note 145, at 386–87.

151 Fraley v. Facebook Inc., 830 F. Supp. 2d 785, 796–97 (N.D. Cal. 2011).

152 *Id.* at 805 (users were identified as "subjects of public interest among the same audience") (citing Downing v. Abercrombie & Fitch, 265 F.3d 994, 1002 (9th Cir. 2001)); *see also generally* Grea, *supra* note 76.

press to tell it. . . .'"[153] While there is some protection of privacy in relation to privacy of communications,[154] more often it is balanced against the public's interest in knowing when the information relates to matters of public concern.[155] Further, the creation of an image (personal or otherwise) is protected under copyright and thus more readily protected under the First Amendment.[156]

This is not to suggest that the U.S. Constitution provides no privacy protection. Rather, this protection is limited. For example, there is protection for people's privacy against intrusions by government.[157] Even though the U.S. Constitution does not explicitly provide for a right to privacy for breaches of privacy between individuals,[158] the FTC does offer some protection in certain circumstances against breaches of personal information.[159] However, in the context of privacy protection for misuses of personal images, the protection is limited to each individual state's common law or statute. It can be argued that whenever there are competing interests between privacy and a creator's freedom of expression, the courts traditionally favor

---

153 Montana v. San Jose Mercury News, Inc., 34 Cal. App. 4th 790, 793 (Cal. Ct. App. 1995) (quoting Eastwood v. Superior Court, 149 Cal. App. 3d 409, 417 (Cal Ct. App. 1983)); *see also* CAL. CIV. CODE § 3344(a) (West 2012); Amy Morganstern, *In the Spotlight: Social Network Advertising and the Right of Publicity*, 12 INTELL. PROP. L. BULLETIN 181, 191 (2008); Koehler, *supra* note 76, at 984 (2013). Koehler further states that "because California's right of publicity statute prevents a commercial speaker from inappropriately using an individual's name or likeness and thus places a strain on what a speaker can say, the right of publicity can conflict with the First Amendment's free speech and freedom of the press clauses." *Id.* at 974–75.

154 *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514 (2001) (broadcaster published a true recording of a conversation albeit embarrassing); Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975) (name of a rape victim was published); Time, Inc. v. Hill, 385 U.S. 374 (1967) (the real names of juvenile offenders were published); Hustler Magazine v. Falwell, 485 U.S. 46 (1988) (same); Smith v. Daily Mail Publ'g Co., 443 U.S. 97 (1979) (same).

155 *See generally Bartnicki*, 532 U.S. 514.

156 *See* Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 60–61 (1884); *see also* Bleistein v. Donaldson Lithographing Co., 188 U.S. 239, 251–52 (1903).

157 *See* U.S. CONST. amend. IV.

158 *See* Siry, *supra* note 99.

159 *See* Federal Trade Commission Act*,* 15 U.S.C. § 45 (2006); *see also* Bode & Jones, *supra* note 139, at 77. *See* Decision & Order, *In re* Snapchat, Inc., F.T.C. Docket No. C-4501 (Dec. 23, 2014); *see also* F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

freedom of expression over privacy as it is a constitutional right under the First Amendment.[160]

Freedom of the press is given precedence in instances when there are competing interests between privacy and freedom of the press to report news.[161] There is a willingness to strike a more balanced approach between the right to privacy and the public's right to know, as highlighted in *Virgil v. Time Inc,*[162] where Judge Merrill stated:

> Does the spirit of the Bill of Rights require that individuals be free to pry into the unnewsworthy private affairs of their fellowmen? In our view it does not. In our view, fairly defined areas of privacy must have the protection of law if the quality of life is to continue to be reasonably acceptable. The public's right to know is, then, subject to reasonable limitations so far as concerns the private facts of its individual members.[163]

---

[160] *See* Siry, *supra* note 99.

[161] *See* Florida Star v. B.J.F., 491 U.S. 524, 541 (1989) (holding that the publication of a rape victim's name by a newspaper was lawfully obtained) ("We do not hold that truthful publication is automatically constitutionally protected, or that there is no zone of personal privacy within which the State may protect the individual from intrusion by the press, or even that a State may never punish publication of the name of a victim of a sexual offense. We hold only that where a newspaper publishes truthful information which it has lawfully obtained, punishment may lawfully be imposed, if at all, only when narrowly tailored to a state interest of the highest order, and that no such interest is satisfactorily served by imposing liability under § 794.03 to appellant under the facts of this case."). However, White, J., dissenting from the majority, stated:

> *Of course, the right to privacy is not absolute.* Even the article widely relied upon in cases vindicating privacy rights, Warren & Brandeis, The Right to Privacy, 4 HARV. L. REV. 193 (1890), *recognized that this right inevitably conflicts with the public's right to know about matters of general concern—and that sometimes, the latter must trump the former. Id.* at 214–15. *Resolving this conflict is a difficult matter, and I fault the Court not for attempting to strike an appropriate balance between the two, but rather, fault it for according too little weight to B. J. F.'s side of equation, and too much on the other.*

Id. at 551 (emphasis added).

[162] Virgil v. Time, Inc., 527 F.2d 1122 (9th Cir. 1975).

[163] *Id.* at 1128; *see also Florida Star*, 491 U.S. at 524.

Despite having rich tort law to draw upon, when a plaintiff's privacy interests conflict with a defendant's freedom of expression, privacy protection is often weakened.[164] As Judge Renwick remarked in *Foster v. Svenson*, there are limitations to New York State's statutory privacy tort because the court is "constrained to find that the invasion of privacy of one's home that took place here is not actionable as a statutory tort of invasion of privacy pursuant to sections 50 and 51 of the Civil Rights Law."[165] New York State Senator Kevin Thomas proposed a Bill known as the New York Privacy Act ("NYPA") to strengthen privacy rights in New York.[166] The NYPA attempts to rebalance the scales between protecting freedom of expression and privacy rights of users where their data have been misused or used when the information is outdated or no longer relevant.[167] However, although the NYPA was introduced in May 2019,[168] the bill did not receive a floor vote and has not progressed beyond the committee stage.[169]

While there is some common ground between the basis for privacy protection in both European and American courts, there are signficant differences in the ways that privacy protection is implemented in these jurisdictions. One such difference is that the European perspective of developing data protection laws is

---

164 Bode & Jones, *supra* note 139, at 77.

165 Foster v. Svenson, 128 A.D.3d 150, 152 (N.Y. App. Div. 2015).

166 S.B. 5642, 242nd Leg., Reg. Sess. (N.Y. 2019) ("An act to amend the general business law, in relation to the management and oversight of personal data . . . . This act may be known and cited as 'New York Privacy Act.'"). Senator Kevin Thomas proposed the Bill; however, the Bill did not successfully pass. *See* Kathryn Lundstrom, *New York's Privacy Bill Failed Last Session*, ADWEEK: DATA & PRIVACY (Feb. 21, 2020), https://www.adweek.com/digital/new-yorks-privacy-bill-failed-last-session-but-it-gives-us-a-look-at-what-future-laws-might-look-like/ [https://perma.cc/WS6R-PJ5X].

167 *See* Louis Nizer, *The Right of Privacy: A Half Century's Developments*, 39 MICH. L. REV. 526, 540 (1941); *see also* Samantha Barbas, *From Privacy to Publicity: The Tort of Appropriation in the Age of Mass Consumption*, 61 BUFF. L. REV. 1119, 1119 (2013); Grea, *supra* note 76; Alison C. Storella, *It's Selfie-Evident: Spectrums of Alienability and Copyrighted Content on Social Media*, 94 B.U. L. REV 2045, 2069 (2014); W. Mack Webner & Leigh Ann Lindquist, *Transformation: The Bright Line Between Commercial Publicity Rights and the First Amendment*, 37 U. AKRON L. REV. 171, 188 (2004); W.A.C., *The Right of Privacy in News Photographs*, 44 VA. L. REV. 1303, 1315 (1958).

168 *See* S.B. 5642.

169 *See* Sen. Kevin Thomas, *Legislation*, N.Y. ST. SENATE, https://www.nysenate.gov/senators/kevin-thomas/legislation [https://perma.cc/FCL2-424G]; *see also* S.B. 5642.

entrenched in various legislation. For example, the European Charter of Human Rights provides that individuals have the right to private life.[170] The GDPR further strengthens this right by protecting a person's right to control their data.[171] Whilst ensuring that privacy rights need to be balanced with freedom of expression, the legislation incorporates freedom of expression as an exception as to when privacy rights can be exercised.[172] In fact, European courts have considered the competing interests between one person's privacy interests and another's freedom of expression.[173]

On the contrary, there is no singular piece of legislation that protects privacy in the United States. Rather, freedom of expression is protected and valued above privacy interests as it is part of the First Amendment of U.S. Constitution.[174] Conseqently, in situations where there are competing intests between a person's privacy and another person's freedom of expression, American courts err in favor of freedom of expression.[175] Therefore, the protection of freedom of expression and freedom of speech has eroded the privacy interests that Warren and Brandeis recognized in tort law.[176]

The expanding mass media, and the widespread use of social networks, have highlighted the imbalance between individual privacy and freedom of expression in American law and American life. Webb argues that "characterizing the emergence of a balancing approach in the U.S constitutional law as erosion misses the

---

170 *See* EUROPEAN CONVENTION ON HUMAN RIGHTS, *supra* note 64.

171 *See* sources cited *supra* note 32.

172 *See supra* notes 70–71 and accompanying text.

173 For example, in *Von Hannover v. Germany*, Princess Caroline of Monaco campaigned to prevent publications of photographs taken without her consent while going about her everyday life: going shopping, going horse riding, eating, holidaying, tripping on the beach. Von Hannover v. Germany (No.1), App No. 59320/00, Eur. Ct. H.R. (June 24, 2004); *see also* N. A. Moreham, *Privacy in Public Places*, 65 CAMBRIDGE L.J. 606, 607, 614 (2006).

174 *See* Richard J. Peltz-Steele, *The New American Privacy*, 44 GEO. J. INT'L L., 365, 384, 409–10 (2013); *see also* Foster v. Svenson, 128 A.D.3d 150, 161 (N.Y. App. Div. 2015); Amy Gajda, *Privacy, Press, and the Right to Be Forgotten in the United States*, 93 WASH. L. REV. 201, 238–43 (2018).

175 *See* Foster v. Svenson, 128 A.D.3d 150, 161 (N.Y. App. Div. 2015).

176 *See* Warren & Brandeis*, supra* note 146, at 197 (tort of intrusion upon seclusion, tort of public disclosure of private fact, false light and appropriation); *see also* Prosser, *supra* note 145, at 389 (Prosser made the subdivision); Mantelero, *supra* note 4, at 229–35, 230.

mark."[177] This is because "[s]hifts in U.S law are necessary to avoid staleness and obsolescence in light of new technologies and changing worldviews."[178] Where information centers on public officials or public figures, an American court is very likely to favor freedom of the press over personal privacy, especially if the matters reported are highly newsworthy and likely to be in the public's interest.[179]

Although personal images may be protected under American tort law to some extent, there are gaps in the existing law when a third party captures a person's image in a photograph. As the New York Appellate Division noted in *Foster v. Svenson*:

> [A]cknowledging that Civil Rights Law sections 50 and 51 reflect a careful balance of a person's right to privacy against the public's right to a free flow of ideas, plaintiffs argue that defendant's work should not be entitled to First Amendment protection because of the manner or context in which it was formed or made. In essence, plaintiffs seem to be arguing that the manner in which the photographs were obtained constitutes the *extreme and outrageous conduct* contemplated by the tort of intentional infliction of emotional distress and serves to overcome the First Amendment protection contemplated by Civil Rights Law sections 50 and 51.[180]

In America, freedom of expression has become paramount to any privacy right, especially when the photograph is artistic or newsworthy.[181] This is particularly the case when people are captured in

---

177 Webb, *supra* note 134, at 1331.

178 *Id*. ("These shifts require the ebb and flow of certain rights and liberties to parallel and reflect the values citizens place on those principles while the spirit of the U.S Constitution remains fixed."); *see also* Mantelero, *supra* note 4, at 238–43.

179 *See* Mantelero, *supra* note 4, at 229–35; *see also* Werner v. Times-Mirror Co., 193 Cal. App. 2d 111, 113 (Cal. Ct. App. 1961) (involving the invasion of privacy of a public person).

180 *Foster*, 128 A.D.3d at 161 (emphasis added).

181 *See* Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 60–61 (1884); Bleistein v. Donaldson Lithographing Co., 188 U.S. 239, 251–52 (1903); *see also* Storella, *supra* note 167, at 2051–52; Gajda, *supra* note 174, at 238–43.

photographs by third parties, as was the case in *Foster v. Svenson.*[182] In that case, Svenson was a photographer who used a high-powered lens to capture different photographs of his neighbours (the Fosters) and their children playing, sleeping, and undressing in their home.[183] The Fosters' claims for invasion of privacy were unsuccesful because the images were protected as artistic works.[184]

While it makes plaintiffs cringe to think their private lives and images of their small children can find their way into the public forum of an art exhibition, there is no redress under the current laws of the State of New York. "Simply, an individual's right to privacy under the New York Civil Rights Law sections 50 and 51 yield [sic] to an artist's protections under the First Amendment under the circumstances presented here."[185]

However, the appellate court highlighted the gaps in the way that tort law protected personal images in the United States:

> New technologies can track thought, movement, and intimacies, and expose them to the general public, often in an instant. This public apprehension over new technologies invading one's privacy became a reality for the plaintiffs and their neighbors when a photographer, using a high powered camera lens inside his own apartment, took photographs through the window into the interior of apartments in a neighboring building. The people who were being photographed had no idea this was happening. This case highlights the *limitations of New York's statutory privacy tort as a means of redressing harm that may be caused by this type of technological home invasion and exposure of private life*. *We are constrained to find that the invasion of privacy of one's home that took place here is not actionable as a statutory tort of invasion of privacy pursuant to*

---

182 *See* Foster v. Svenson, No. 651826/2013, 2013 WL 3989038, at *1 (N.Y. Sup. Ct. Aug. 5, 2013).

183 *See id.*; *see also Foster*, 128 A.D.3d at 152–53.

184 *See Foster*, 128 A.D.3d at 163.

185 *Foster*, 2013 WL 3989038, at *1.

> *sections 50 and 51 of the Civil Rights Law, because defendant's use of the images in question constituted art work* and, thus is not deemed "use for advertising or trade purposes," within the meaning of the statute.[186]

The court further acknowledged that U.S. law did not address situations where people are photographed in the privacy of their own homes:

> Undoubtedly, like plaintiffs, many people would be rightfully offended by the intrusive manner in which the photographs were taken in this case. However, such complaints are best addressed to the Legislature—the body empowered to remedy such inequities. Needless to say, as illustrated by the troubling facts here, in these times of heightened threats to privacy posed by new and ever more invasive technologies, we call upon the Legislature to revisit this important issue, as we are constrained to apply the law as it exists.[187]

There are some similarities between Australian and American privacy protection, which is due to a fragmented approach of protecting privacy interests. As commonly known, there are inconsistencies of privacy protection among the various States in America.[188] These inconsistencies may be viewed as a double-edged sword, where the inconsistency may serve as a vehicle for potential state law reform, but people in other states are left without the same rights. It is also uncertain whether other states would follow and adopt into their state legislation another state's law reform. A lack of uniformity means that state laws vary and may not adequately protect people's privacy.

One difference between Australia and the United States is that despite having a fragmented approach to the protection of personal images, Australia has legislation at the federal level which, despite

---

186 *Foster*, 128 A.D.3d at 152 (emphasis added).

187 *Id.* at 163 (citations omitted).

188 *See generally* Melville B. Nimmer, *The Right of Publicity*, 19 L. & CONTEMP. PROBS. 203 (1954).

having gaps, may make it easier to propose law reform to align with the GDPR. Notably, since the emergence of the right to be forgotten, the State of New York has introduced a bill for a Privacy Act,[189] which could potentially align with Europe's GDPR. The proposed Privacy Act would empower New Yorkers to sue companies directly over privacy violations.[190]

In particular, the proposed New York Privacy Act could pave the way for privacy reform in other states. For example, there are serious claims against Facebook for privacy breaches in other states like Illinois.[191] Following numerous data breaches, companies such as Facebook have been fraught with privacy claims. Similar situations have occurred in European countries such as France, where Facebook and Google have been fined by privacy regulatory bodies because of their failure to protect their users' privacy.[192]

CONCLUSION

The right to be forgotten has the potential to re-shift the power imbalance that social networks hold over their users' images by enabling the users to regain some control. As Bernal argues, "That kind of transfer of power, that kind of re-balancing, could have possibilities to redress the current imbalance over personal data—and to help re-establish at least some control that people have lost and feel that they have lost."[193] An alternative view is that the the right to be forgotten does not in fact restrict freedom of speech, but that

> [The] concept of the right to be forgotten is based on the fundamental need of an individual to determine the development of his life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in

---

189 *See* S.B. 5642, 242nd Leg., Reg. Sess. (N.Y. 2019).

190 *See* Karl Bode, *New York State's Privacy Law Would Be Among the Toughest in the US*, TECHDIRT (June 6, 2019), https://www.techdirt.com/articles/20190605/07035842338/new-york-states-privacy-law-would-be-among-toughest-us.shtml [https://perma.cc/76KJ-5QKE].

191 *See, e.g.*, Patel v. Facebook, Inc., 932 F.3d 1264, 1267 (9th Cir. 2019).

192 *See* Alex Hern, *Google Fined Record £44m by French Data Protection Watchdog*, GUARDIAN (Jan. 21, 2019), https://www.theguardian.com/technology/2019/jan/21/google-fined-record-44m-by-french-data-protection-watchdog [https://perma.cc/4Z3T-66HD].

193 Bernal, *supra* note 4.

> the past, especially when these events occurred many years ago and do not have any relationship with the contemporary context.[194]

This is particularly the case where the right to be forgotten is balanced against freedom of the press.[195] As noted by the European Court of Justice,

> [The] balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.[196]

When people are photographed, their images are captured and their ability to control the use of their image is restricted. This restriction is particularly acute when the image is captured by a third party. The difficulty that arises is that the creator of the image has the right to control the use of the photograph. Consequently, the person who is the subject of that image is unable to control how the image and the information captured in the image are used. The lack of user's control over their image was also highlighted above in the New York case *Foster v. Svenson*, where the Fosters were unable to control the use of their images that had been captured by Svenson because the image fell within an artistic work.[197] When personal images are uploaded on social networks such as Facebook, those images are effectively controlled by the social network and may be accessed or stored even if a user has withdrawn their consent.[198] The New York Privacy Act, if enacted, and successful, potentially provides privacy protection that is more robust as it would be in

---

194 Mantelero, *supra* note 4, at 230.

195 *See* General Data Protection Regulation, *supra* note 27, at art. 80; *see also* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317, ¶ 20.

196 Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317, ¶ 81.

197 *See* Foster v. Svenson, 128 A.D.3d 150, 158–59 (N.Y. App. Div. 2015).

198 *See* Georgiades, *supra* note 2, at 435–45.

addition to the existing protection that is afforded under the current legal framework.

The European right to be forgotten would provide people in Australia or the United States with greater control over their images if both countries adopted the right. However, to improve further, a number of changes should be considered in the European model itself. The European law could be improved, for example, by clarifying who has the responsibility to remove images, particularly where there are multiple parties involved. It would also be helpful to clarify the situations where an image may be required to be removed or deleted.

Clarification is also needed about when consent may be withdrawn. To minimize the adverse effects of the exception it might also be useful to consider limiting its use to reasonable withdrawal.[199] Consideration should also be given to amending the personal and household exemption,[200] because if a personal and

---

[199] *See, e.g.*, General Data Protection Regulation, *supra* note 27, at art. 7; *see also id.* at rec. 32:

> Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

[200] Oliver Butler, *The Expanding Scope of the Data Protection Directive: The Exception for a 'Purely Personal or Household Activity,'* 3–4, 8 (Univ. of Cambridge Faculty of Law, Working Paper No. 54, 2015), https://ssrn.com/abstract=2660916 [https://perma.cc/DN9P-G8GV] (referring to the problem of using spatial logic in the interpretation of the exception of purely personal or household activity which applies to the Data Protection Directive 95/46/EC). In particular, the author refers to Ryneš v. Úrad pro ochranu osobních údaju, C-212/13, ECR 0 (2014), where he quotes the Advocate General:

house purpose was included in Australian law it would leave many images unprotected and vulnerable to misuse. However, any such modification of the European model in this respect would have to be done in a manner that carefully balanced the right of individuals to protect their personal images with the ability for individuals to express themselves by uploading images (which was the motivation behind the exception). This is not to suggest that the exception should be abolished so much that it should be modified to take account of the new realities of new technologies.[201]

Overall, it is clear that the EU GDPR provides better protection for people whose images are shared and exchanged on social networks. This Article has argued that the EU's right to be forgotten is a useful mechanism that enables people to regain control over the use of their images within a social network context. The European right to be forgotten is intended to rebalance the scales between freedom of expression and privacy, especially when the information is outdated or no longer relevant.[202] This Article has shown that there are exceptions as to the operation of the right to be forgotten which could serve to limit the right, such as freedom of expression and the press.

The Article has shown that while American courts have traditionally favored freedom of expression over privacy interests, there

---

> In my view, "personal" activities under the second indent of Article 3(2) of Directive 95/46 are activities which are closely and objectively linked to the private life of an individual and which do not significantly impinge upon the personal sphere of others. These activities may, however, take place outside the home. "Household" activities are linked to family life and normally take place at a person's home or in other places shared with family members, such as second homes, hotel rooms or private cars. All such activities have a link with the protection of private life as provided for under Article 7 of the Charter.

Id. at 3–4.

[201] The Article 29 Data Protection Working Party "urge[d] the legislature to use the process of introducing new data protection law as an opportunity to reduce as far as possible the legal uncertainty that currently surrounds various aspects of individuals' personal or household use of the internet." Working Party, *Annex 2*, *supra* note 81, at 3.

[202] *See generally* Nizer, *supra* note 167; *see also* Barbas, *supra*, note 167; Grea, *supra* note 76; Storella, *supra* note 167; W.A.C., *supra* note 167; Webner & Lindquist, *supra* note 167.

is an increasing push to strengthen privacy protection. Despite not having a unified single legislative instrument for the protection of privacy, some states like New York have considered and proposed privacy law reform by incorporating a right to be forgotten in their statutory legislation. If passed, New York courts could serve as a potential model for other states to follow suit. It is worth noting that even if the United States incorporated a right to be forgotten, it may not restrict freedom of expression as the American courts are likely to rule in favor of First Amendment claims. Currently the law in Australia values freedom of expression over privacy. While this may have made sense in a pre-internet world, technological changes that have radically changed the way that images are used and controlled have challenged the now-outdated arrangements. The right to be forgotten would help to reset the scales between privacy and freedom of expression. It is time that Australian law provided people with the right to be forgotten as a way of preventing the misuse of their images. In so doing it would give them the right to control the use of their personal images online.