Laws on Erasure of Online Information

Canada • France • European Union • Germany • Israel
Japan • New Zealand • Norway • Portugal
Russia • Spain • United Kingdom

November 2017

The Law Library of Congress, Global Legal Research Center
(202) 707-6462 (phone) • (866) 550-0442 (fax) • law@loc.gov • http://www.law.gov

Contents

Comparative Summary

Luis Acosta
Chief, Foreign, Comparative, and International Law Division II

This report describes the laws of twelve jurisdictions that have some form of remedy available enabling the removal of online data based on harm to individuals' privacy or reputational interests, including but not limited to defamation. Six of the countries surveyed are within the European Union (EU) or the European Economic Area, and therefore have implemented EU law. Five non-EU jurisdictions are also surveyed.

Comparative analysis across jurisdictions presents terminological challenges, because legal language across jurisdictions seems at times to conflate concepts that could be considered analytically distinct. EU law, for example, uses the phrases "right to erasure" and the "right to be forgotten" synonymously, eliding the difference between the right to remedy incorrect or incomplete data in source documents and the right to have search results delisted irrespective of whether the underlying source material is altered or removed.

As described in detail in the EU survey, the EU's law in this area emerged from a 1995 Data Protection Directive that gave individuals the right to erasure of erroneous or incomplete data. A 2014 decision of the European Court of Justice expanded on this right to provide for the right to remove search results to personal information even without deletion of that information from the original publication, where the individuals' privacy interests outweigh the public interest in maintaining the information. A 2016 Regulation that will apply in all EU Member States by May 25, 2018, will codify the 2014 decision.

Most of the surveyed EU countries, in addition to EU law, have parallel domestic law governing harmful online content. The UK, which is slated to leave the EU, nonetheless has pending legislation to update its data protection legislation that will address how certain provisions of the 2016 EU Regulation will apply.

The surveyed countries outside the EU have a range of approaches to these issues:

- Russia has criminal penalties for "invasion of personal privacy" for the illegal spreading of private information about a person, which has been used to prosecute revenge pornography. Its Civil Code provides for the right to demand removal of images improperly distributed on the internet, and under its Law on Information it recognizes the right to be forgotten—the right of applicants to request search engine operators to remove illegal, inaccurate, or outdated search results.
- New Zealand has robust statutory remedies for resolving harmful online content.
- Canadian law provides not only for the processing of complaints regarding privacy and reputational issues through the Office of the Privacy Commissioner, but also for court remedies that include injunctive relief against search engines to delist websites.

- Japanese law allows internet hosting providers to delete defamatory content, provides a safe harbor from liability for such providers, has a mechanism for victims to request the removal of infringing information, and has an easier and faster mechanism for the blocking of revenge porn. It also provides a means by which victims can obtain the identification of offenders from the service provider.
- Israel's Defamation Law has been applied by a court against Google for failing to change a technical code that resulted in defamatory information in online searches.

Jurisdictional Surveys
European Union and European Countries

European Union

Jenny Gesley
Foreign Law Specialist

SUMMARY The right to erasure (right to be forgotten) forms part of the right to personal data protection, which is a fundamental right in the European Union. It is codified in article 17 of the General Data Protection Regulation, which intends to update and clarify the right to erasure for the digital age. A data subject may demand erasure of personal data from a controller of such data if certain conditions are met. Action on a request must be taken without undue delay. If the controller has made the personal data public, he or she has to take reasonable steps to inform other controllers of the request. The controller is also generally obligated to periodically review personal data and to take every reasonable step to ensure that third parties erase inaccurate personal data that was made public. The right to the protection of personal data is not an absolute right and must be balanced against other fundamental rights, such as the freedom of expression and information.

I. Introduction

The protection of personal data and the respect for private life are fundamental rights in the European Union (EU).[1] Personal data is defined as "any information relating to an identified or identifiable natural person (data subject)."[2] The right to erasure (right to be forgotten) forms part of the right to personal data protection. It is codified in article 17 of the General Data Protection Regulation (GDPR).[3] The GDPR entered into force on May 24, 2016, and will apply directly in the EU Member States starting May 25, 2018, with generally no domestic implementing legislation needed.[4] It replaced and updated the 1995 Data Protection Directive,[5] with the goals

[1] Charter of Fundamental Rights of the European Union (EU Charter) arts. 7, 8, 2012 O.J. (C 326) 391, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=EN, *archived at* https://perma.cc/PJN3-A8MZ; Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) art. 16, para. 1, 2012 O.J. (C 326) 47, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN, *archived at* https://perma.cc/K69X-SDQ9.

[2] 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 (General Data Protection Regulation) art. 4(1), 2016 O.J. (L 119) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, *archived at* http://perma.cc/UWW3-KFMH.

[3] *Id*.

[4] *Id*. art. 99; TFEU, *supra* note 1, art. 288, para. 2. Certain national derogations are allowed. *See* GDPR, recitals 10, 19, 52.

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (1995 Data Protection Directive), 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN, *archived at* http://perma.cc/DW3S-KL29.

of strengthening online privacy rights, boosting Europe's digital economy, and streamlining the implementation of data protection rules in EU Member States.[6]

II. The Right to Erasure (Right to Be Forgotten)

A. Background

Article 17 of the GDPR codifies an explicit right to erasure of personal data when certain conditions are met. The provision draws from a decision from the European Court of Justice (ECJ) dated May 13, 2014.[7] The ECJ based its ruling on the 1995 Data Protection Directive and found that the right to be forgotten on the internet as a general principle can be inferred from the 1995 Directive and from the EU Charter.[8] It held that a data subject has the right under certain conditions to ask search engines to remove links with personal data when the data are inaccurate, inadequate, irrelevant, no longer relevant, or excessive for the purposes of the processing; are not kept up to date; or are kept for longer than is necessary.[9] The Court stated that the requests to delete the data must be assessed on a case-by-case basis, taking into account the type of information, the sensitivity of the information for the data subject's private life, and the data subject's role in public life.[10] Deleting the search engine results linked to the data subject's name does not mean that the content is deleted from its original publication location.

Google, the search engine in the ECJ case, complied with the judgment by making available a search removal form on its website.[11] Data subjects must indicate their personal data, identify the links that they wish to be removed, and provide a justification for the request. According to Google's latest transparency report, it assessed 1,925,436 requests between May 29, 2014, and October 2017 and removed 43.2% of the links.[12]

---

[6] European Commission Press Release IP/12/46, Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses (Jan. 25, 2012), http://europa.eu/rapid/press-release_IP-12-46_en.pdf, *archived at* http://perma.cc/BXE7-682P.

[7] Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, ECLI:EU:C:2014:317, http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0131&lang1=en&type=TXT&ancre, *archived at* http://perma.cc/TX38-MV8T. For a summary of the case, see Theresa Papademetriou, *Court of Justice of the European Union: Decision Upholds Right to Have Personal Data Erased*, GLOBAL LEGAL MONITOR (May 21, 2014), http://www.loc.gov/law/foreign-news/article/court-of-justice-of-the-european-union-decision-upholds-right-to-have-personal-data-erased/, *archived at* https://perma.cc/Q36W-JCB9.

[8] Case C-131/12, para. 99; 1995 Data Protection Directive, *supra* note 5, arts. 12, 14; EU Charter, *supra* note 1, arts. 7, 8.

[9] Case C-131/12, paras. 92, 93.

[10] *Id.* paras. 98, 99.

[11] *Transparency Report: Search Removals under European Privacy Law*, GOOGLE, https://transparencyreport.google.com/eu-privacy/overview (last visited Oct. 27, 2017), *archived at* http://perma.cc/92VM-8BYU.

[12] *Legal Help: Removing Content From Google*, GOOGLE, https://support.google.com/legal/troubleshooter/1114905#ts=1115655 (last visited Oct. 27, 2017), *archived at* http://perma.cc/X9CJ-FBBZ.

B. Material Scope

As pointed out by the ECJ in its decision, a general right to erasure of incomplete or inaccurate personal data could already be found in the 1995 Directive. The inclusion of a right to erasure of personal data in the GDPR intends to update and clarify this right for the digital age and provide legal certainty.[13] Article 17 of the GDPR uses the terms "right to erasure" and "right to be forgotten" synonymously. The right to erasure provides data subjects with the right to require controllers to erase personal data when certain conditions are met. "Controller" is broadly defined as any "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data."[14] The ECJ in its judgment held that a search engine is a controller of personal data as defined in the 1995 Data Protection Directive.[15] The Article 29 Working Party, which was set up under article 29 of the 1995 Data Protection Directive as an independent European advisory body on data protection and privacy, concluded in an opinion that social networking services also fall under the definition of personal data controller.[16]

A data subject may demand erasure of personal data from a controller if

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws the consent on which the processing is based and there is no other legal ground for the processing;
- the data subject objects to the processing on the basis of legitimate interests and there are no overriding legitimate grounds for the processing;[17]
- the personal data have been unlawfully processed in breach of the GDPR;
- the personal data must be erased to comply with an EU or Member State legal obligation to which the controller is subject; or
- the personal data have been collected in relation to the offer of information society services[18] directly to a child[19] and consent was given by the child, but he or she was not fully aware of

[13] European Commission, Factsheet on the "Right to Be Forgotten" Ruling (C-131/12), at 2, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, *archived at* http://perma.cc/C9XK-ST2Y.

[14] GDPR, *supra* note 2, art. 4(7).

[15] Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, ECLI:EU:C:2014:317, para. 33.

[16] Article 29 Working Party, *Opinion 5/2009 on Online Social Networking*, WP163 (June 12, 2009), at 5, para. 3.1, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf, *archived at* http://perma.cc/Q3K4-7WBC.

[17] GDPR, *supra* note 2, art. 21.

[18] "Information society services" are defined as services normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services. *See* Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 Laying Down a Procedure for the Provision of Information in the Field of Technical Regulations and of Rules on Information Society Services art. 1, para. 1(b), 2015 O.J. (L 241) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L1535&from=EN,

> the risks involved by the processing at the time, and later wants to remove such personal data.[20]

In addition, even without a request from a data subject, a controller is under a continuous obligation to take every reasonable step to ensure that inaccurate personal data are erased or rectified.[21] This requires periodic reviews of personal data.[22]

C. Consequences

After a data subject makes a request based on his or her right to erasure, the controller must generally take action without undue delay and, in any event, within one month of receipt of the request.[23] If no action is taken, the controller must inform the data subject without undue delay and at the latest within one month of the reasons for not doing so. In addition, he or she needs to inform the data subject of the possibility to lodge a complaint with a national supervisory authority or to enforce the request in court.[24] The controller may generally not charge a fee for the erasure of personal data except for cases in which the request is manifestly unfounded or excessive.[25]

If one of the grounds for erasure applies and the controller has made the personal data public, he or she has to take reasonable steps to inform other controllers who are processing the data that the data subject has requested erasure of any links to, or copy or replication of, those personal data.[26] "Reasonable steps" means "taking into account available technology and the means available to the controller, including technical measures."[27] Article 70 obligates the European Data Protection Board, which is established as an independent body by the GDPR, to issue guidelines, recommendations, and best practices on procedures for the erasure of links, copies, or replications of personal data from publicly available communications services.[28]

In cases in which the personal data has not been made public but has been disclosed in some other form to other recipients, the controller is obligated to communicate the erasure of personal data to these recipients, unless this is impossible or involves a disproportionate effort.[29]

---

archived at http://perma.cc/HS39-U8Z3. Annex I provides an indicative list of services that are not covered by the term.

[19] GDPR, *supra* note 2, art. 8.

[20] *Id.* art. 17, para. 1 & recital 65.

[21] *Id*. art. 5, para. 1d, para. 2, recital 39.

[22] *Id*. recital 39.

[23] *Id*. art. 12, para. 3.

[24] *Id*. art. 12, para. 4.

[25] *Id* art. 12, para. 5.

[26] *Id.* art. 17, para. 2 & recital 66.

[27] *Id*.

[28] *Id.* art. 70, para. 1d.

[29] *Id*. art. 19.

D. Exceptions to the Right to Erasure

The right to the protection of personal data is not an absolute right; it must be balanced against other fundamental rights in accordance with the principle of proportionality.[30] The data subject has no right to demand erasure, and the controller is not obligated to erase personal data, if the processing is necessary to the exercise of the right to freedom of expression and information.[31] Article 85 of the GDPR obligates EU Member States to pass national legislation that balances the right to personal data protection with the right to freedom of expression and information. It should be noted that, according to the EU Commission, indexation of personal data by a search engine does not fall under freedom of expression.[32]

An exception from the right to have personal data erased and the obligation to erase it also applies if the processing is necessary for the controller to comply with a legal obligation, for the performance of a task carried out in the public interest, or for the exercise of official authority vested in the controller; for reasons of public interest in the area of public health;[33] for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes; and for the establishment, exercise, or defense of legal claims.[34]

E. Restrictions on the Scope of the Right to Erasure

The scope of the right to erasure may be restricted by EU law or by Member State law if the measure respects the essence of fundamental rights and freedoms, and is necessary and proportionate in a democratic society to safeguard important objectives of general public interest, such as national security.[35]

F. Fines

If article 17 is violated, the national supervisory authority may impose an administrative fine of up to €20 million (around US$23.3 million) or, in the case of an undertaking, of up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[36]

---

[30] *Id*. recital 4.

[31] *Id.* art. 17, para. 3.

[32] Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) – Preparation for a General Approach: – Chapter III*, Doc. No. 7978/1/15 REV 1 (Apr. 27, 2015), at 35, n.160, http://data.consilium.europa.eu/doc/document/ST-7978-2015-REV-1/en/pdf, *archived at* http://perma.cc/SX4D-CH3G.

[33] GDPR, *supra* note 2, art. 9, paras. 2h, 2i, 3.

[34] *Id*. art. 17, para. 3.

[35] *Id.* art. 23.

[36] *Id*. art. 83, para. 5b.

France

Nicolas Boring
Foreign Law Specialist

SUMMARY The right to erasure in France can be divided into two components: the right to object, which is the right to have personal information removed from a website or database, and the right to delisting, which is the right to have a search engine remove search results related to one's name. The right to object is based on French domestic legislation, while the right to delisting is principally based on European law.

The main enforcers of the right to erasure are the court system, and an independent government agency called the CNIL. The CNIL has the authority to order website owners to remove information, and may impose monetary sanctions to force compliance. The French Penal Code also provides that criminal sanctions, including fines and/or jail time, may be imposed by courts on those who illegally process or publish others' personal information online.

I. Introduction

In France, the right to erasure (often referred to as "the right to be forgotten") can be divided into to two components. One is a right to object (*droit d'opposition*), which refers to a one's right to have personal information removed from a website or database, and is based on French legislation.[1] The other component is a right to delisting (*droit au déréférencement*), which refers to one's right to have a search engine remove search results related to one's name. This right is principally based upon European Union legal norms, particularly on a May 13, 2014, decision of the European Court of Justice,[2] which itself was based on the EU's 1995 Data Protection Directive.[3]

The main enforcers of the right to erasure are the court system and the Commission Nationale de l'Informatique et des Libertés (National Commission on Computer Technology and Civil

[1] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law No. 78-17 of 6 January 1978 Regarding Computer Technology, Data Files and Civil Liberties] art. 38, https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460, *archived at* https://perma.cc/3GZG-7V8R.

[2] Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, ECLI:EU:C:2014:317, http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0131&lang1=en&type=TXT&ancre, *archived at* http://perma.cc/TX38-MV8T.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (1995 Data Protection Directive), 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN, *archived at* http://perma.cc/DW3S-KL29; now replaced by 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 (General Data Protection Regulation) art. 4 (1), 2016 O.J. (L 119) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, *archived at* http://perma.cc/UWW3-KFMH.

Liberties) (CNIL). The CNIL is an independent government agency that was created in 1978 to regulate the use of personal data in the digital world.[4]

II. Right to Object

French law provides that "any physical person has the right to object, for legitimate reasons, to the processing of information of a personal nature."[5] According to the CNIL, the right to object includes (though is not limited to) the right to have comments or photos removed from websites or networks, and the right to have personal data removed from commercial databases.[6]

A person who wishes to have personal information removed from a website or database must first send a written request to the organization in charge of the website or database.[7] This organization then has two months to reply to the request. In the case of refusal, the requester may either appeal to the CNIL or sue the organization in court.[8]

III. Right to Delisting

As noted above, delisting (*déréférencement*) refers to the removal from a search engine of search results related to a person's name—a right principally based upon the May 13, 2014, *Google Spain* decision of the European Court of Justice.

Just a few months after the ECJ's *Google Spain* decision, a Paris court referred to it as precedent to apply the right to be forgotten in France.[9] In this case, a couple that had been the victims of defamation had asked that Google deindex webpages containing the defamatory information so that someone searching for their names would no longer see these webpages appear in the search results. The Paris Tribunal de grande instance (Trial Court) ruled that the couple's request was justified and that Google needed to take the actions necessary to comply.[10]

In addition to suing in court, any resident of France may appeal to the CNIL if he/she has unsuccessfully asked a search engine to remove certain search results linked to the requester's

---

[4] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés art. 11; *La CNIL en France* [*The CNIL in France*], CNIL, https://www.cnil.fr/fr/la-cnil-en-france (last visited Nov. 7, 2017), *archived at* https://perma.cc/GR7N-VF8K.

[5] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés art. 38 (all translations by author).

[6] *Le droit d'opposition* [*The Right to Object*], CNIL, https://www.cnil.fr/fr/le-droit-dopposition (last visited Nov. 7, 2017), *archived at* https://perma.cc/NFY3-GJED.

[7] *Id.*

[8] *Id.*

[9] M. et Mme. X et M. Y / Google France [Mr. & Mrs. X and Mr. Y vs. Google France], TGI Paris, réf. [Paris Trial Court, single judge formation], Sept. 16, 2014, https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-du-16-septembre-2014/, *archived at* https://perma.cc/BC8C-2TSY; Hubert Bitan, DROIT ET EXPERTISE DU NUMÉRIQUE [DIGITAL LAW AND EXPERTISE] 321 (2015), *bibliographical record at* https://lccn.loc.gov/2015484480.

[10] *Id.*

name.[11] Website owners who are sanctioned by the CNIL may appeal to the Conseil d'Etat (Council of State), France's highest court for administrative matters.[12] The Conseil d'Etat has recognized the applicability of the right to delisting based on the *Google Spain* decision, but has recently asked the European Court of Justice for clarification on the proper limits of this right in two pending cases.[13]

IV. Sanctions

The CNIL has the authority to order a website owner to remove information, and may impose a monetary sanction to force the website owner to comply.[14] The monetary sanction must be proportional to the seriousness of the website owner's offense, or to the benefit that the website owner derived from the offense.[15]

Furthermore, a number of criminal sanctions may be imposed by courts on those who illegally process or publish others' personal information online.[16] In particular, the use of someone's personal information despite that person's legitimate opposition is punishable by up to five years of imprisonment and/or a fine of €300,000 (approximately US$348,000).[17]

[11] *Le droit au déréférencement* [*The Right to Deindexing*], CNIL, https://www.cnil.fr/fr/le-droit-au-dereferencement (lasted visited Nov. 7, 2017), *archived at* https://perma.cc/NA6H-9Z5P.

[12] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés art. 46.

[13] *Google Inc.*, CE [Council of State], July 19, 2017, No. 399922, http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC, *archived at* https://perma.cc/Q28Y-258J; *Mme. C, M. F, M. H, M. D* [*Mrs. C, Mr. F, Mr. H, Mr. D*], CE, Feb. 24, 2017, Nos. 391000, 393769, 399999, 401258, http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-24-fevrier-2017-Mme-C-M.-F-M.-H-M.-D, *archived at* https://perma.cc/BC8G-FZVA.

[14] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés art. 45.

[15] *Id.* art. 47.

[16] CODE PENAL [PENAL CODE] arts. 226-16 to 226-24, https://www.legifrance.gouv.fr/affichCode.do;jsessionid=FCA913D4A8A77F0B112765B62F0FE1A0.tplgfr24s_1?idSectionTA=LEGISCTA000006165313&cidTexte=LEGITEXT000006070719&dateTexte=20171108, *archived at* https://perma.cc/54JF-6MYY.

[17] *Id.* art. 226-18-1.

Germany

Jenny Gesley
Foreign Law Specialist

SUMMARY The right to erasure of personal data in Germany used to be codified in various places in the German Federal Data Protection Act, in sector-specific legislation, and in state law. Starting on May 25, 2018, it will be replaced by article 17 of the European Union General Data Protection Regulation, which is directly applicable in Germany. A violation of the data subject's right to erasure is an administrative offense punishable with a fine of up to €20 million or up to 4% of the total worldwide annual turnover in the case of an undertaking.

I. Introduction

The right to erasure (right to be forgotten) forms part of the right to personal data protection. It used to be codified in former sections 20 and 35 of the German Federal Data Protection Act.[1] Other sector-specific legislation as well as state law also contained provisions on a right to erasure of personal data. Starting on May 25, 2018, these provisions will be replaced by article 17 of the European Union (EU) General Data Protection Regulation (GDPR).[2] The GDPR entered into force on May 24, 2016, and will apply directly in the EU Member States from May 25, 2018, with generally no domestic implementing legislation needed.[3] However, the GDPR also contains "opening clauses" that permit diverging national legislation, thereby allowing the Member States to enact more restrictive legislation in certain areas, for example for the processing of special categories of personal data or in the context of employment.[4] It also specifically allows Member States to incorporate elements of the GDPR into their national law as far as necessary for coherence and making it comprehensible.[5]

---

[1] Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Jan. 14, 2003, § 20, para. 2, § 35, para. 2, BUNDESGESETZBLATT [BGBL.] [FEDERAL LAW GAZETTE] I at 66, as amended, http://www.gesetze-im-internet.de/bdsg_1990/BDSG.pdf, *archived at* http://perma.cc/9A7M-JDK9, unofficial English translation *available at* http://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf, *archived at* http://perma.cc/4MLZ-NJFT (English version updated through Aug. 14, 2009).

[2] 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 (General Data Protection Regulation) (GDPR) art. 4 (1), 2016 O.J. (L 119) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, *archived at* http://perma.cc/UWW3-KFMH.

[3] *Id*. art. 99; Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) art. 288, para. 2, 2012 O.J. (C 326) 47, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN, *archived at* https://perma.cc/K69X-SDQ9. Some provisions nonetheless require for their implementation the adoption of application measures by the Member States—for example, the appointment of a national regulator and administrative sanctions for a violation of the GDPR.

[4] GDPR, *supra* note 2, recitals 10, 19, 52; art. 9, para. 4; art. 88.

[5] *Id.* recital 8.

Germany published the amendment of its Data Protection Act, which aligns it with the requirements of the GDPR and the EU Law Enforcement Directive (EU) 2016/680, in July 2017—the first EU Member State to do so.[6] With regard to the right to erasure as codified in the GDPR, the Member States are obligated to pass national legislation that balances the right to personal data protection with the right to freedom of expression and information and provide for exemptions or derogations if the processing is carried out for journalistic purposes or for academic, artistic, or literary expression.[7] Member States must notify the EU Commission of laws enacted in this regard or any amendments to them.[8]

Furthermore, the scope of the right to erasure may be restricted by EU law or by Member-State law if the measure respects the essence of fundamental rights and freedoms and is necessary and proportionate in a democratic society to safeguard important objectives of general public interest, such as national security.[9]

II. The Right to Erasure

The German Data Protection Act has a wider scope than the GDPR; it applies to the processing of personal data by federal and state public authorities and bodies as well as by private bodies.[10] Article 17 of the GDPR replaces and harmonizes the various rights to erasure that were codified in former section 20, paragraph 2 and section 35, paragraph 2 of the German Federal Data Protection Act, as well as sector-specific rules and rights to erasure contained in state law.

As mentioned, article 17 of the GDPR is directly applicable in Germany. Section 35 of the amended German Federal Data Protection Act modifies the data subject's right to erasure and the controller's corresponding duty to erase.[11] If in a case of nonautomated data processing erasure is impossible or only possible with a disproportionate effort due to the specific mode of storage, and if the data subject's interest in erasure is minimal, the right to erasure is replaced with a right to restriction of processing as codified in article 18 of the GDPR. This modification is not applicable if the processing was unlawful. Furthermore, the right to restriction applies instead of the right to erasure if erasure would conflict with a legal duty of the controller to retain the data for a specific time period.[12] However, it is unclear whether the modifications of the right to

[6] Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU - DSAnpUG-EU) [Act to Adapt the Data Protection Law to Regulation (EU) 2016/679 and to Implement Directive (EU) 2016/680 (Data Protection Adaption and Implementation Act EU)], June 30, 2017, BGBL. I at 2097, http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s2097.pdf, *archived at* http://perma.cc/DL3C-LKGD, English translation *available at* https://www.bmi.bund.de/SharedDocs/downloads/EN/gesetztestexte/datenschutzanpassungsumsetzungsgesetz.pdf?__blob=publicationFile&v=1, *archived at* http://perma.cc/K79T-PMUW.

[7] GDPR, *supra* note **Error! Bookmark not defined.**, art. 85, paras. 2, 3.

[8] *Id.* art. 85, para. 3.

[9] *Id.* art. 23.

[10] Data Protection Adaption and Implementation Act EU, *supra* note 6, § 1; GDPR, *supra* note 2, recital 19.

[11] GDPR, *supra* note 2, art. 23.

[12] Data Protection Adaption and Implementation Act EU, *supra* note 6, § 35, para. 3; GDPR, *supra* note 2, art. 17, para. 3b.

erasure, in particular the modification because of a disproportionate effort, are compatible with article 23 of the GDPR or if they are too far-reaching.[13] The German legislator justifies the modification with the need to protect the rights and freedoms of others without any further explanation.[14]

Germany has not yet enacted legislation to implement the obligation contained in article 85 of the GDPR.

III. Processing that Falls Outside of the Scope of the GDPR

The GDPR is not applicable to processing of personal data that does not form part of a filing system. A filing system is defined as "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis."[15] If a data subject wants erasure of personal data in such a case, he or she may demand erasure based on general civil law provisions or based on the general public law right to remedial action.[16] Other cases that are outside the scope of the GDPR can also be pursued by relying on these general provisions. However, if the GDPR is applicable, the GDPR right to erasure will take precedence as the more specific right (*lex specialis*).

IV. Sanctions

A violation of the data subject's right to erasure is an administrative offense punishable with a fine of up to €20 million (about US$23.5 million), or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher.[17]

---

[13] Tobias Herbst, *Art. 17 Recht auf Löschung („Recht auf Vergessenwerden")* [*Art. 17 Right to Erasure ("Right to be Forgotten")*], *in* DS-GVO. DATENSCHUTZ-GRUNDVERORDNUNG: KOMMENTAR [GDPR. GENERAL DATA PROTECTION REGULATION: COMMENTARY] 430 (Jürgen Kühling & Benedikt Buchner eds., 2017); Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder [Datenschutzkonferenz] [DSK] [Conference of the Independent Data Protection Authorities of the German Federation and the German States] [German Data Protection Conference], Kurzpapier Nr. 11. Recht auf Löschung /„Recht auf Vergessenwerden" [Short Paper No. 11: Right to Erasure/"Right to be Forgotten"], Aug. 29, 2017, p. 3, https://www.tlfdi.de/mam/tlfdi/gesetze/dsk_kpnr_11_recht_auf_vergessenwerden.pdf, *archived at* http://perma.cc/FQV2-879P.

[14] DEUTSCHER BUNDESTAG: DRUCKSACHEN UND PROTOKOLLE [BT-DRS.] 18/11325, p. 105, http://dipbt.bundestag.de/doc/btd/18/113/1811325.pdf, *archived at* http://perma.cc/CC83-XURM.

[15] GDPR, *supra* note 2, art. 4(6).

[16] Bürgerliches Gesetzbuch (BGB) [Civil Code], Jan. 2, 2002, §§ 823, 824, 1004, para. 1, BGBL. I at 42, 2909; corrected in BGBL. 2003 I at 738, as amended, http://www.gesetze-im-internet.de/bgb/BGB.pdf, *archived at* http://perma.cc/D4U5-AX88, unofficial English translation *available at* http://www.gesetze-im-internet.de/englisch_bgb/englisch_bgb.pdf, *archived at* http://perma.cc/DZ3H-XZGG; Verwaltungsgerichtsordnung [VwGO] [Code of Administrative Court Procedure], Mar. 19, 1991, § 113, BGBL. I at 686, as amended, http://www.gesetze-im-internet.de/vwgo/VwGO.pdf, *archived at* http://perma.cc/8J6U-X5DG, unofficial English translation *available at* http://www.gesetze-im-internet.de/englisch_vwgo/englisch_vwgo.pdf, *archived at* http://perma.cc/98XV-RMFF.

[17] GDPR, *supra* note 2, art. 83, para. 5; Data Protection Adaption and Implementation Act EU, *supra* note 6, § 41; Gesetz über Ordnungswidrigkeiten [OwiG] [Act on Administrative Offenses], Feb. 19, 1987, BGBL. I at 602, as amended, http://www.gesetze-im-internet.de/owig_1968/OWiG.pdf, *archived at* http://perma.cc/NLL2-TRBA, unofficial English translation *available at* http://www.gesetze-im-internet.de/englisch_owig/englisch_owig.pdf, *archived at* http://perma.cc/2BL2-W7VF.

Authorities and other public bodies are not subject to administrative fines, unless they take part in competition as enterprises governed by public law.[18]

[18] Data Protection Adaption and Implementation Act EU, *supra* note 6, § 43, para. 3; § 2, para. 5.

Norway

Elin Hofverberg
Foreign Law Research Consultant

SUMMARY Norway, a European Economic Area member, has implemented the 1995 European Union Data Protection Directive on personal data but has not yet implemented the EU General Data Protection Regulation (GDPR). The enforcement authority for private data protection legislation is Datatilsynet (the Norwegian Data Protection Authority). Datatilsynet has aided Norwegians in removing search results online.

As of 2015, defamation is no longer a specific crime under Norwegian law, but crimes against personal life are still recognized. In addition, victims may be entitled to monetary compensation (damages) for defamation even if the act in question does not rise to the level of a crime.

I. Introduction

Norway is not a member of the European Union, but instead is a member of the European Economic Area (EEA). As an EEA member it is nevertheless bound by the EU Data Protection Directive 95/46/EF,[1] which was incorporated into the EEA agreements in 1999,[2] and is thus bound by the 2014 decision of the European Court of Justice (ECJ) on the right to be forgotten. Norway is also bound by privacy protections found in the European Convention on Human Rights (EHCR).[3]

The EU General Data Protection Regulation (GDPR), discussed in more detail in the survey of European Union law, is set to become directly enforceable in EU Member States in May 2018. As of yet, the Regulation has not been incorporated into the EEA Treaty.[4] However, as with the previous EU Data Protection Directive 95/46/EF, the Norwegian government is planning to

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (1995 Data Protection Directive), 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, *archived at* https://perma.cc/WXE2-SETM.

[2] Decision of the EEA Joint Committee No 83/1999 of 25 June 1999 Amending Protocol 37 and Annex XI (Telecommunication Services) to the EEA Agreement, 2000 O.J. (L 296) 41, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:22000D1123(08), *archived at* https://perma.cc/TN6L-4HPB.

[3] §2 LOV OM STYRKING AV MENNESKERETTIGHETENES STILLING I NORSK RETT (MENNESKERETTSLOVEN) [ACT ON HUMAN RIGHTS POSITION IN NORWEGIAN LAW], LOV-1999-05-21-30, https://lovdata.no/dokument/NL/lov/1999-05-21-30, *archived at* https://perma.cc/Q5YZ-L6HL.

[4] *Nye personvernregler i EU*, REGJERINGEN.NO (Apr. 27, 2017), https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/nye-personvernregler-i-eu/id2340094/, *archived at* https://perma.cc/66AK-EMCP. The three EEA European Free Trade Association states of Iceland, Liechtenstein, and Norway are currently evaluating the Regulation for incorporation into the EEA Agreement. *32016R0679*, EUROPEAN FREE TRADE ASSOCIATION, http://www.efta.int/eea-lex/32016R0679 (last visited Nov. 14, 2017), *archived at* https://perma.cc/74WG-4YCJ.

incorporate the new provisions into Norwegian law.[5] Thus, the article 17 right to be forgotten is likely to become Norwegian law in 2018.[6] This report, however, is based on the laws currently in force as of November 2017.

II. Domestic Legislation

A. Data Protections

Norway has adopted the following two regulations on privacy: (1) the Personal Data Act[7] relating to the processing of personal data, and (2) the Personal Data Regulation.[8] These both include provisions from the 1995 EU Data Protection Directive.

Section 27 of the Personal Data Act provides a right to erasure of erroneous content when "weighty considerations relating to protection of privacy so warrant."[9] As noted above, this right to be forgotten is derived from the ECJ's 2014 decision involving Google.[10] Section 9 of the Norwegian Personal Data Act provides how and when processing of data may be carried out.[11] Under the Personal Data Act it is the Data Protection Authority, also known as the Data Inspectorate (Datatilsynet), that oversees compliance with the Act.[12] Decisions by Datatilsynet can be appealed to the Personal Data Protection Board (Personvernsnemnda).[13]

B. Defamation

As of January 1, 2015, defamation is no longer specifically criminalized in the Norwegian Criminal Code (Straffeloven).[14] Crimes against a person's personal life are, however, still

[5] *Nye personvernregler i EU*, *supra* note 5.

[6] *Id.*

[7] LOV OM BEHANDLING AV PERSONOPPLYSNINGER (PERSONOPPLYSNINGSLOVEN) [PERSONAL DATA ACT], LOV 2000-04-14-31, https://lovdata.no/dokument/NL/lov/2000-04-14-31?q=LOV-200004-14-31, *archived at* https://perma.cc/NTH3-XG72; PERSONAL DATA ACT, Act of 14 April 2000 No. 31 (unofficial English translation), https://www.datatilsynet.no/en/regulations-and-tools/regulations-and-decisions/norwegian-privacy-law/personal-data-act, *archived at* https://perma.cc/AW4A-XNU4.

[8] Personal Data Regulation (unofficial English translation), https://www.datatilsynet.no/en/regulations-and-tools/regulations-and-decisions/norwegian-privacy-law/personal-data-regulations2/, *archived at* https://perma.cc/F3MG-DXZ7.

[9] § 27 PERSONAL DATA ACT.

[10] Case C‑131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, ECLI:EU:C:2014:317, http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0131&lang1=en&type=TXT&ancre, *archived at* http://perma.cc/TX38-MV8T.

[11] § 9 PERSONAL DATA ACT.

[12] § 42 PERSONAL DATA ACT.

[13] *See*, *e.g.*, Personverdsnemda decision of Dec. 8, 2015, PVN-2015-06 Google, http://www.personvernnemnda.no/vedtak/2015_06.htm, *archived at* https://perma.cc/PW6A-4FG6.

[14] Compare the revoked Norwegian Criminal Code of 1902: §§ 246 & 247 ALMINDELIG BORGERLIG STRAFFELOV (STRAFFELOVEN) [CRIMINAL CODE 1902], https://lovdata.no/dokument/NLO/lov/1902-05-22-10/KAPITTEL_2-16#§246, *archived at* https://perma.cc/LC5T-EK66.

criminalized, and defamation acts may fall under this provision.[15] Acts against a person's personal life are penalized with either a fine or up to one year of imprisonment.[16] Persons who are defamed have a specific right to damages, even when the defamation does not meet the threshold of being a crime against personal life.[17]

III. Datatilsynet and Google

Already in 2014 Datatilsynet supported several Norwegians' removal requests against Google.[18] By 2015 Datatilsynet had acted on behalf of thirteen Norwegians, aiding them in their efforts to remove online content from Google's search results.[19] According to information from Google's webpage, it has received a total of forty-seven requests from Norwegians, requesting removal of some 2,003 items.[20]

In addition to removing search results, the Datatilsynet has determined that, in accordance with the 2014 ECJ decision discussed above, Norwegians may also demand that Google remove automatic search suggestions that pop up after one's name, such as "John Doe alzheimers" or "John Doe criminal" ("Ola Nordmann Alzheimer" eller "Ola Nordmann kriminell").[21] By June 2015 only two such requests had been handled by the Norwegian Data Protection Authority.[22]

[15] § 267 LOV OM STRAFF (STRAFFELOVEN) [CRIMINAL CODE], LOV 2005-05-20-28, https://lovdata.no/dokument/NL/lov/2005-05-20-28, *archived at* https://perma.cc/K268-97JR.

[16] *Id*.

[17] §§ 3-6a & 3-6 SKADESERSTATNINGSLOVEN [DAMAGES ACT], LOV-1969-06-13-26, https://lovdata.no/dokument/NL/lov/1969-06-13-26, *archived at* https://perma.cc/98UM-E8QV.

[18] *Én har fått medhold i Google-sletting*, DATATILSYNET (Oct. 28, 2014), https://www.datatilsynet.no/regelverk-og-skjema/lover-og-regler/avgjorelser-fra-datatilsynet/andre-avgjorelser-og-vedtak/eldre-vedtak/En-har-fatt-medhold-i-fjerning-av-Google-treff/, *archived at* https://perma.cc/MMJ9-BZRU.

[19] *Kan få fjernet Googles forslag til søk*, DATATILSYNET (June 16, 2015), https://www.datatilsynet.no/aktuelt/2015/Kan-fa-fjernet-Googles-automatiske-forslag-til-sok/, *archived at* https://perma.cc/NFK4-5A6E.

[20] *Transparency Report*, GOOGLE, https://transparencyreport.google.com/government-removals/overview?authority_search=country:NO&lu=authority_search (last visited Nov. 7, 2017), *archived at* https://perma.cc/Z62Q-DAYM.

[21] *Kan få fjernet Googles forslag til søk*, DATATILSYNET (June 16, 2015), https://www.datatilsynet.no/aktuelt/2015/Kan-fa-fjernet-Googles-automatiske-forslag-til-sok/, *archived at* https://perma.cc/RS4Q-MPKF.

[22] *Id*.

Portugal

Eduardo Soares
Senior Foreign Law Specialist

SUMMARY Personal data in Portugal is protected by Law No. 67 of October 26, 1998, which transposed European Directive 95/46/EC into its domestic legal system. On April 26, 2016, the European Union issued Regulation (EU) 2016/679 updating the protection of personal data and revoking Directive 95/46/EC effective May 25, 2018. Portugal has yet to enact domestic legislation in response to Regulation (EU) 2016/679.

In 1995 the European Union issued Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (the Data Protection Directive).[1] Portugal then enacted a new law on the protection of personal data, Law No. 67 of October 26, 1998, which transposed Directive No. 95/46/EC into its domestic legislation.[2]

According to Law No. 67, a data subject has the right to obtain from the controller,[3] freely and without constraint, at reasonable intervals and without excessive delay or expense, the correction, erasure, or blocking of data whose processing does not comply with the provisions of Law No. 67/98, in particular because of the incomplete or inaccurate nature of the data.[4] Article 12 of Law No. 67/98 defines the situations where the data subject has the right to object to the processing of data relating to him or her.

Pursuant to article 12 of Law No. 67, the data subject has the right

> (a) except where otherwise provided by law, and at least in the cases referred to in articles 6(d) and 6(e) of Law No. 67/98, to object at any time, on compelling legitimate grounds relating to his particular situation, to the processing of data relating to him, and where there is a justified objection, the processing of data performed by the controller may no longer involve those data;

[1] Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (1995 Data Protection Directive), 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, *archived at* https://perma.cc/P5FP-2RR8.

[2] Lei No. 67/98, de 26 de Outubro, Lei da Protecção de Dados Pessoais [Personal Data Protection Law], http://www.pgdlisboa.pt/pgdl/leis/lei_mostra_articulado.php?nid=156&tabela=leis&ficha=1&pagina=1, *archived at* https://perma.cc/SQF7-YXAS.

[3] According to article 3(d) of Law No. 67/98, "controller" [*responsável pelo tratamento*] is defined as "the natural or legal person, public authority, agency, or any other body that 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 laws or regulations, the controller must be designated in the Act establishing its organization and functioning, or in the statutes of the legal or statutory body competent to process the personal data concerned." *Id.* art. 3(d) (translation by author).

[4] *Id.* art. 11(1)(d).

> (b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing or any other form of research, or to be informed before personal data are disclosed for the first time to third parties for the purposes of direct marketing or for use on behalf of third parties, and to be expressly offered the right to object, free of charge, to such disclosure or uses.[5]

The National Commission of Data Protection (Comissão Nacional de Protecção de Dados, CNPD) is the agency in charge of controlling and inspecting the enforcement of laws and regulations on the protection of personal data.[6]

Without prejudice to the right to submit a complaint to the CNPD, any person may resort to administrative or judicial measures to ensure compliance with the legal provisions on protection of personal data.[7] Any person who has suffered damage as a result of the unlawful processing of data or of any other acts incompatible with legal provisions in the area of personal data protection is entitled to receive compensation from the controller for the damage suffered.[8]

On April 26, 2016, the European Union issued Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC effective May 25, 2018.[9] Portugal has yet to enact domestic legislation in response to Regulation (EU) 2016/679.

Google offers its users in Portugal an option to remove content indexed in its search engine based on the EU Data Protection Directive.[10]

---

[5] *Id.* art. 12 (translation by author).

[6] *O que é a CNPD*, COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS, http://www.cnpd.pt/bin/cnpd/acnpd.htm (last visited Nov. 14, 2017). Article 22(1) of Law No. 67/98 determines that CNPD is the national authority charged with the power to supervise and monitor compliance with the laws and regulations in the area of personal data protection, with strict respect for the human rights and the fundamental freedoms and guarantees provided by the Constitution and the law.

[7] *Id.* art. 33.

[8] *Id.* art. 34(1).

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) art. 94, 2016 O.J. (L 119) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&qid=1509458857466&from=EN, *archived at* https://perma.cc/4HPB-DXKW.

[10] *Remoção de Privacidade da UE*, GOOGLE, https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=0-636422845330448542-1068676439&hl=pt&rd=1 (last visited Oct. 30, 2017), *archived at* https://perma.cc/TK8F-4DRC.

Spain

Graciela Rodriguez-Ferrand
Senior Foreign Law Specialist

SUMMARY Under the Law on Data Protection, individuals have the right to access, rectify, cancel, and oppose personal data in search engine indexes and digital archives, under certain circumstances. A claim by a Spanish national against Google based on these rights ended up before the European Court of Justice, which in its 2014 landmark decision favored privacy rights by recognizing the right of individuals to request that search engines remove links to their personal data when the linked information does not meet the standards of appropriateness and relevance, is outdated, has become irrelevant, or lacks any public interest.

I. Domestic Law

In Spain the right to protection of personal data has been recognized under the Law on Data Protection (LOPD)[1] and Royal Decree 1720/2007, which regulates application of the Law (RDLOPD).[2] The Agencia Española de Protección de Datos (AEPD) (Spanish Data Protection Agency) is the enforcement authority on data protection.[3]

Under this legal regime, individuals have the right to access, rectify, cancel, and oppose personal data in search engine indexes and digital archives, under certain circumstances.[4] These rights are known as the "ARCO" rights (for *acceso*, *rectificacióon*, *cancelación y oposición* [access, rectification, cancellation, and opposition]). They include the right to know what personal data is contained in a file, the right to amend incorrect or incomplete data in a file, the right to suppress and block incorrect data in a file, and the right to object to the processing of personal data within a file.[5] These are personal rights and may only be exercised by the affected person or

[1] Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal [Law on Personal Data Protection (LOPD)], BOLETÍN OFICIAL DEL ESTADO [B.O.E.] Dec. 14, 1999, http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Ley_Organica_15-1999_de_13_de_diciembre_de_Proteccion_de_Datos_Consolidado.pdf, *archived at* https://perma.cc/N3MM-XMLE.

[2] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal [Royal Decree 1720/2007, . . . Approving the Regulation of the Law on Data Protection (RDLOPD)], B.O.E. Jan. 19, 2008, http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Real_Decreto_1720-2007_de_21_de_diciembre_por_el_que_se_aprueba_Reglamento_de_desarrollo_Ley_Organica_15-1999_Consolidado.pdf, *archived at* https://perma.cc/BGV3-FKN3.

[3] LOPD art. 35.

[4] JUAN PABLO APARICIO VAQUERO & ALFREDO BATUECAS CALETRIO, EN TORNO A LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS EN LA SOCIEDAD DE LA INFORMACIÓN 2 (Granada, 2015).

[5] *Id.* at 73.

his or her legal representative. File managers may not charge fees in order to process claims involving the exercise of these rights.[6]

II. Right of Cancellation

The right of cancellation gives individuals the right to cancel inappropriate or excessive personal data that is held in an entity's file.[7] The exercise of this right may only be carried out by the person concerned, who should address the firm or public entity holding the data, identifying the specifics of the data in question and the justification for its removal.[8]

The entity responsible for the file must render a decision on the cancellation petition within ten days after receipt of the request. If a decision is not rendered by the deadline or is unsatisfactory, the petitioner may seek protection before the AEPD.[9]

If granted, the cancellation order will mandate the removal of the data, which will still be retained by public administrations, judges, and courts when required by law or contractual obligations.[10]

III. Right of Opposition

Individuals may exercise the right to oppose the use of personal data when the interested party's consent for its processing is not required and the request is based on a legitimate and well-founded reason related to the personal situation of the affected individual, unless the law requires otherwise; when the files are aimed at advertising or commercial purposes; or when the use of personal data aims at adopting a decision involving the affected individual based solely on an automated treatment of the personal data.[11]

The right of opposition may only be exercised by the affected individual through a request directed to the entity or person responsible for the data treatment, stating the legitimate grounds justifying the opposition.[12] The entity responsible for the file's management must reach a decision within ten days after receipt of the request, and either exclude the personal data as requested or deny the petition on reasoned grounds.[13] If the petition is not decided within the deadline or if the entity holding the file that contains the personal data denies the right to

[6] *Id.*

[7] LOPD art. 16; RDLOPD arts. 31–33.

[8] RDLOPD art. 23.

[9] *Id.*

[10] LOPD art. 16.3.

[11] RDLOPD art. 34.

[12] LOPD art. 16.5.

[13] RDLOPD art. 35.2.

opposition, the petitioner may seek redress before the AEDP upon submitting evidence that the file's holder has denied the opposition petition.[14]

IV. The Right to Be Forgotten

According to the AEDP,

> [t]he so-called "right to be forgotten" is an expression derived from the rights of cancellation and opposition regulated under the LOPD as applied to internet browsers. The right to be forgotten encompasses the right to prevent the dissemination of personal information through the internet when its publication does not meet the standards of appropriateness and relevance, when the information is already outdated or became irrelevant or lacks any public interest, even if the original publication is legitimate and protected by the freedoms of expression and information, such as the information available in official gazettes.[15]

In this regard, the LOPD provides that personal data may be canceled when it has stopped being necessary or pertinent for the purpose for which it was originally collected or recorded. Personal data will not be kept beyond the time period needed to fulfill its purpose. In exceptional circumstances it may be maintained for historical, scientific, or statistical purposes.[16]

V. Google v. Spain

Based on the LOPD rights of cancellation and opposition, Spanish national Mario Costeja González filed a complaint before the AEDP in 2010 against *La Vanguardia*, a Spanish newspaper, and Google Spain for 1998 auction legal notices that cited Costeja González.[17] The legal notices were required by the Ministerio de Trabajo y Asuntos Sociales (Ministry of Labor and Social Matters) in reference to auctions of real estate seized to secure social security contributions owed by Costeja González.[18] Costeja González argued that links to the auction notices were no longer necessary because the seizure proceeding involving his social security debt had been settled more than ten years ago and therefore its mention was entirely irrelevant.[19] He requested that *La Vanguardia* remove the pages or change them so that his personal information was no longer shown.[20] He also requested that Google remove links to the 1998 auction notices in order to remove them from Google Search results.[21]

---

[14] *Id*.

[15] *'Derecho al Olvido'?*, AEDP, http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php (last visited Nov. 15, 2017), *archived at* https://perma.cc/BEF7-NCFA.

[16] LOPD art. 4.5.

[17] Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, ECLI:EU:C:2014:317, http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0131&lang1=en&type=TXT&ancre, *archived at* https://perma.cc/UUQ6-FRXS.

[18] APARICIO VAQUERO & BATUECAS CALETRIO, *supra* note 4, at 78.

[19] *Id.*

[20] *Id.*

[21] *Id.* at 79.

The AEDP dismissed Costeja González's claim against *La Vanguardia*, but granted the claims against Google.[22] Google then filed an appeal before the Audiencia Nacional (Spain's highest court), which in turn referred the case to the European Court of Justice (ECJ).[23]

In a decision rendered on May 13, 2014, the ECJ determined that search engines engage in the processing of data because they navigate the internet in an automatic, continuous, and systematic manner searching for information.[24] The decision further established that since Google, a US-based company, had a Spanish subsidiary, it was subject to EU law because it operated as an establishment in Spain and carried out its commercial transactions there through advertising space accessible in its search engine.[25] Based on EU legislation and specifically EU Directive 95/46 on Data Protection,[26] the ECJ ruled that Google had an obligation to remove links to pages displayed by third parties, in this case *La Vanguardia* newspaper, when they became inadequate, irrelevant, or excessive in relation to the purposes for which they were collected by the mere fact of the passage of time, even if the content published by the third parties was lawful.[27] The ECJ also recognized the right of individuals to request that search engines remove links to personal data. It concluded that there was not a preponderant public interest in access to the links offered by the search engine related to auction notices for a debt that was settled sixteen years before that outweighed Costeja González's privacy interests. Therefore, the court granted the plaintiff the right to demand that the search engine erase all search result links to his name and the 1998 auction legal notices.[28]

The decision also established that the right to be forgotten is not without limitations. The balance between the privacy rights of the individual affected and the legitimate interest of the search engine may depend on the type of information involved, such as the sensitivity for the privacy of the individual in question, the public interest in access the information, and the status of the individual in the public sphere.[29]

VI. Current Status on the Right to Be Forgotten

Since the Costeja González decision, anyone in Spain who wants search results related to personal data removed must make a direct claim to the search engine in question, which must then decide on a case-by-case basis whether there are justified grounds for the request.[30] This is

[22] *Id.*

[23] *Id*.

[24] *Id.* at 81.

[25] *Id*.

[26] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (1995 Data Protection Directive), 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A31995L0046, *archived at* https://perma.cc/MB6S-347M.

[27] APARICIO VAQUERO & BATUECAS CALETRIO at 82.

[28] *Id*. at 83.

[29] *Id*. at 85–86.

[30] *Id*. at 90.

the case if the individual's right of privacy takes precedence over the public interest to access such information.[31] If the petition is denied, the petitioner may seek redress through the courts.[32]

As a consequence of the ECJ decision, search engines such as Google, Yahoo, and others now offer users a special form to request the removal of links according to data protection standards.[33]

[31] *Id.*

[32] *Id.*

[33] *Id*.

United Kingdom

Clare Feikert-Ahalt
Senior Foreign Law Specialist

SUMMARY The Data Protection Act 1998 regulates the processing of personal data in the United Kingdom. That Act does not provide a process through which individuals may request to be forgotten, nor is such a right recognized by other UK laws. However, a bill is currently being considered before Parliament that would repeal and replace the Data Protection Act by incorporating, and expanding upon, the European Union's General Data Protection Regulation, which establishes a right to be forgotten, into the national law of the UK.

While no specific law has yet been enacted, UK citizens do have the right, under a European Court of Justice Ruling, to request the removal of web pages that refer to them from Google's search results. In addition, the Defamation Act 2013 provides a specific process for individuals to request the removal of material that they believe is defamatory. The process uses website operators as an intermediary to facilitate the removal of this type of information.

I. Introduction

The Data Protection Act 1998 governs how personal information is held in the United Kingdom.[1] The Act is broad and applies to obtaining, holding, using, or disclosing personal information. It was enacted and implemented to meet the requirements of the European Union's Data Protection Directive,[2] which has now been updated and replaced by the EU General Data Protection Regulation (GDPR).[3] The Act is overseen by an Information Commissioner, who has stated that the aim of data protection legislation is to "strike a balance between the rights of individuals and the sometimes competing interests of those with legitimate reasons for using personal information."[4]

The Data Protection Act 1998 does not provide a formal legal process to request to be "forgotten." However, the UK is currently part of the European Union, and as a result of a ruling

[1] Data Protection Act 1998, c. 29, https://www.legislation.gov.uk/ukpga/1998/29, *archived at* https://perma.cc/83C7-CRDG.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, *archived at* https://perma.cc/UEF6-BDEZ.

[3] 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 (General Data Protection Regulation) art. 4(1), 2016 O.J. (L 119) 1, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN, *archived at* http://perma.cc/UWW3-KFMH.

[4] *Your Legal Obligations*, NATIONAL ARCHIVES, http://webarchive.nationalarchives.gov.uk/20090609140314/http://www.ico.gov.uk/what_we_cover/data_protection/your_legal_obligations.aspx (last visited Aug. 30, 2017), *archived at* https://perma.cc/XLD3-T7W8.

from the European Court of Justice, individuals have the right to have links to web pages that refer to them removed from Google's search results.[5] The UK's Information Commissioner is the local regulatory authority in the UK responsible for ensuring compliance with this ruling.[6] In addition, the government recently introduced a bill, discussed below, to repeal and replace the Data Protection Act 1998, which includes provisions that would enable an individual to request to be forgotten online, in accordance with the provisions of the GDPR.[7]

Defamation law is currently provided for in the Defamation Act 2013[8] and in the common law. As discussed below, the Defamation Act provides a process through which persons who believe they have been defamed may request the removal of information from the website operator who hosts third party content, as well as the party who has posted the content.

II. Removal of Online Personal Information

On August 1, 2012, the government issued a statement of intent to introduce a new data protection bill to update and strengthen data protection laws.[9] The statement of intent noted that the government wants to provide individuals with more control over their personal data and the right, with certain exceptions, to be forgotten.[10]

On September 13, 2017, the government followed through on the statement of intent and introduced an almost two-hundred-page bill, known as the Data Protection Bill, which would repeal and replace the Data Protection Act 1998 and follow, but expand upon, the European Union's GDPR.[11] The GDPR will apply in the UK beginning in May 2018, and enable individuals to request the deletion of their personal data in certain circumstances. While EU regulations are directly applicable, given the UK's recent decision to leave the European Union,

> [t]he Government has indicated that primary legislation is required to supplement the Directive, until the instrument is brought into UK law in line with provisions in the European Union (Withdrawal) Bill, because there are derogations (exemptions) within

[5] Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, ECLI:EU:C:2014:317, http://curia.europa.eu/juris/celex.jsf?celex=62012CJ0131&lang1=en&type=TXT&ancre, *archived at* http://perma.cc/TX38-MV8T.

[6] House of Commons Library, *The "Right to Be Forgotten,"* Sept. 2011, SN/HA/6983, http://researchbriefings.files.parliament.uk/documents/SN06983/SN06983.pdf, *archived at* https://perma.cc/A8WQ-2LNM.

[7] Data Protection Bill, 2017-18, HL Bill 66, https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/18066.pdf, *archived at* https://perma.cc/P3GQ-9ZFF.

[8] Defamation Act 2013, c. 26, http://www.legislation.gov.uk/ukpga/2013/26, *archived at* https://perma.cc/2X3V-3SGC.

[9] *A New Data Protection Bill: Our Planned Reforms, Statement of Intent*, DEPARTMENT FOR DIGITAL, CULTURE MEDIA & SPORT (Aug. 7, 2017), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/635900/2017-08-07_DP_Bill_-_Statement_of_Intent.pdf, *archived at* https://perma.cc/TE8A-42ZD.

[10] *Id.*

[11] Data Protection Bill, 2017-18, HL Bill 66, https://publications.parliament.uk/pa/bills/lbill/2017-2019/0066/18066.pdf, *archived at* https://perma.cc/P3GQ-9ZFF.

> the GDPR where the UK wishes to exercise discretion over how certain provisions would apply.[12]

The intent behind the Data Protection Bill is to "update data protection laws for the digital age"[13] and provide clarity for the UK's data protection regime in anticipation of the UK leaving the EU.[14]

III. Removal of Online Defamatory Material

The use of online forums and social media can involve a number of different areas of law, the vast majority of which were drafted prior to the explosion in the use of communications technology.[15] The law relating to defamatory material—that is, published material that causes, or is likely to cause, serious harm to a person's reputation[16]—has recently been updated by the Defamation Act 2013, which was enacted in part to provide a fairer system for addressing materials published online. The update

> reflects the Government's view that disputes should be resolved directly between the complainant and the poster [of the information] where possible. It aims to support freedom of expression by giving the poster an opportunity to express his or her views. It also aims to enable complainants to protect their reputation by resolving matters with the person who is responsible for the defamatory posting where they can be identified, while ensuring that material is removed where the poster cannot be identified or is unwilling to engage in the process. The Government believes that this strikes a fair balance between all the interests involved.[17]

Prior to the enactment of the Defamation Act 2013, website operators generally automatically removed content upon the receipt of a complaint in order to avoid becoming a party to a lawsuit, as they were considered to be the publisher of the statement at common law and could be held liable for the content of these posts.[18] *Godfrey v. Demon Internet Ltd.* was the leading case in

---

[12] House of Lords, *Data Protection Bill [HL] (HL Bill 66 of 2017-19)*, Library Briefing, at 1, http://researchbriefings.files.parliament.uk/documents/LLN-2017-0065/LLN-2017-0065.pdf, *archived at* https://perma.cc/F38N-NQWR.

[13] *Data Protection Bill 2017, Protection Bill 2017*. DEPARTMENT FOR DIGITAL, CULTURE, MEDIA & SPORT (Sept. 14, 2017), https://www.gov.uk/government/collections/data-protection-bill-2017, *archived at* https://perma.cc/2QS2-RGU5.

[14] House of Lords, *supra* note 12, at 1.

[15] HOUSE OF LORDS, SELECT COMMITTEE ON COMMUNICATIONS, FIRST REPORT, 2014-15, HL 37, *available at* https://publications.parliament.uk/pa/ld201415/ldselect/ldcomuni/37/37.pdf, *archived at* https://perma.cc/5P4J-VGGL.

[16] Defamation Act 2013, c. 26, § 1(1), http://www.legislation.gov.uk/ukpga/2013/26, *archived at* https://perma.cc/2X3V-3SGC.

[17] Explanatory Memorandum to the Defamation (Operators of Websites) Regulations 2013, SI 2013/3028, ¶ 7.6, https://www.legislation.gov.uk/uksi/2013/3028/pdfs/uksiem_20133028_en.pdf, *archived at* https://perma.cc/5DT8-HNC3.

[18] Godfrey v. Demon Internet Ltd. [1999] EWHC QB 244, ¶ *available at* http://www.bailii.org/ew/cases/EWHC/QB/1999/244.html, *archived at* https://perma.cc/YBV8-7JLY. This case found that the service provider who transmits or facilitates the transmission of a post is the publisher of the statement at common law and that if,

this area and provided that a service provider who transmitted or facilitated the transmission of a post was considered to be the publisher of the statement at common law, and was thus liable for any defamatory statements. Defenses available to website operators[19] were limited, and these cases were expensive to defend.[20] Additionally, concerns were raised that this cautious approach was limiting free speech, as it meant that some non-defamatory content was being removed and, in cases where it was not removed, individuals were pursuing legal actions against the website operator rather than the individual who authored and posted the content.[21]

Given the vast increase in online users, the government determined that failing to take action in this area of law would result in a chilling effect upon free speech.[22] In 2011 the government held a public consultation on how to address online defamation. Two main options were presented: the first option required a complainant to obtain a court order before an obligation could be imposed on the website provider to remove the allegedly defamatory material. The second sought to place the website operator as a liaison point between the complainant and the individual who posted the allegedly defamatory material.[23] The latter option was the preferred approach and was incorporated by section 5 of the Defamation Act 2013,[24] with the regulatory process contained in the Defamation (Operators of Websites) Regulations 2013.[25] This process is designed to facilitate contact between the aggrieved party and the author of the content.[26] Website operators are not under a duty to follow this procedure, and they may instead choose, independently from the process, whether or not to remove any disputed material, or whether they wish to rely on other defenses to the defamation action.[27]

Section 5 of the Defamation Act 2013 provides website operators that host third-party content with a defense against claims of defamation. In order to use the defense, however, the website

---

upon receiving notice of the defamatory nature of a post, the service provider fails to remove the content, it could not rely upon the defense contained in section 1 of the Defamation Act 1996, because if it did not remove the material upon receiving notice of the material's defamatory nature, the service provider could not satisfy the requirement that it took reasonable care in relation to the publication and could no longer believe that its actions did not cause or contribute to the publication. *Id*. ¶ 50.

[19] Defenses were available at common law and in the Electronic Commerce (EC Directive) Regulations 2002, SI 2002/2012, art. 19, https://www.legislation.gov.uk/uksi/2002/2013/made, *archived at* https://perma.cc/T5JQ-93J3, and the Defamation Act 1996, c. 31, § 1, https://www.legislation.gov.uk/ukpga/1996/31, *archived at* https://perma.cc/U3X4-ZEJM.

[20] MINISTRY OF JUSTICE, DRAFT DEFAMATION BILL, CONSULTATION, 2011, CP3/11, ¶¶ 101–130, https://consult.justice.gov.uk/digital-communications/draft_defamation_bill/supporting_documents/draftdefamationbillconsultation.pdf, *archived at* https://perma.cc/E92F-KVXQ.

[21] Explanatory Memorandum to the Defamation (Operators of Websites) Regulations 2013, *supra* note 17, ¶ 7.2.

[22] *Id*.

[23] DRAFT DEFAMATION BILL, CONSULTATION, *supra* note 20.

[24] Defamation Act 2013, c. 26, http://www.legislation.gov.uk/ukpga/2013/26, *archived at* https://perma.cc/2X3V-3SGC.

[25] Defamation (Operators of Websites) Regulations 2013, SI 2013/3028, https://www.legislation.gov.uk/uksi/2013/3028/contents/made, *archived at* https://perma.cc/W7Y9-49BG.

[26] Defamation Act 2013, c. 26, § 5.

[27] Explanatory Memorandum to the Defamation (Operators of Websites) Regulations 2013, *supra* note 17, ¶ 7.4.

operator must "show that it was not the operator who posted the statement on the website."[28] The defense may be defeated if the claimant can show that

- he or she could not identify the person who posted the allegedly defamatory statement;
- he or she notified the operator of the complaint relating to the statement; and
- the website operator failed to respond to the complaint in accordance with the process contained in the Defamation (Operators of Websites) Regulations 2013.[29]

Section 5(6) of the Act provides that the complainant must include the following information in the complaint: his or her name, the statement as it appears on the website in question, and the reasons why the statement is believed to be defamatory. Regulation 2 of the Defamation (Operators of Websites) Regulations 2013 provides that the complainant must also include the following information contacting the service provider:

> (a) specify the electronic mail address at which the complainant can be contacted;
> (b) set out the meaning which the complainant attributes to the statement referred to in the notice;
> (c) set out the aspects of the statement which the complainant believes are—
> (i) factually inaccurate; or
> (ii) opinions not supported by fact;
> (d) confirm that the complainant does not have sufficient information about the poster to bring proceedings against that person; and
> (e) confirm whether the complainant consents to the operator providing the poster with—
> (i) the complainant's name; and
> (ii) the complainant's electronic mail address.[30]

Even if the notice provided to the website operator does not contain all the information required by both the Act and the Regulations, the Regulations provide that it must be treated as a complaint for the purposes of the Defamation Act 2013.[31]

Within forty-eight hours of receiving a complaint, the website operator must send the poster of the content complained of

- a copy of the complaint, with the complainant's information concealed if he or she has not consented to the sharing of this information; and
- written notice that the content complained of will be removed unless the poster provides a written response by midnight no later than the fifth day after the notification was sent.[32]

[28] Defamation Act 2013, c. 26, § 5(2).

[29] *Id*. § 5.

[30] Defamation (Operators of Websites) Regulations 2013, *supra* note 25, ¶ 2.

[31] *Id*. ¶ 4.

[32] *Id*. Sched. ¶ 2.

The poster must then notify the operator of whether he or she wants the content to be removed from the website specified in the notice. If the poster does not want the content to be removed, the poster must provide his or her full name and postal address, and indicate whether the website operator may provide this personal information to the complainant. If the poster fails to respond to a notice from the website operator, or does respond but fails to include all the required information, the website operator must, within forty-eight hours after the deadline provided to the poster, remove the statement from the websites contained in the notice of complaint and notify the complainant of this. If the poster responds to the website operator that he or she wants the content removed, the website operator has forty-eight hours after notification to remove the information, and must then notify the complainant that the content has been removed.

If the website operator does not have a means of contacting the poster, he or she must remove the statement complained of within forty-eight hours of receiving a written notice from the complainant. The website operator has forty-eight hours after receiving the complaint to send an acknowledgement to the claimant stating that either the poster has been notified, or the post has been removed.[33]

The law also provides an expedited process in cases where an alleged defamatory statement is posted repeatedly. If the same complainant has requested the removal of the same material from the same website operator more than two times, and the information has been removed in accordance with the provisions of the Regulations, the complainant must specify this in the complaint and the website operator must remove the statement within forty-eight hours of receiving the complaint.[34]

If the website operator fails to follow the procedure specified in the Regulations and meet the time limits, the operator can potentially be held liable for the content.[35]

[33] *Id*. Sched. ¶¶ 2–4.

[34] *Id*. Sched. ¶ 9.

[35] House of Commons Library, *The Defamation Act 2013*, Jan. 2014, SN/HA/6801, at 6, http://researchbriefings.files.parliament.uk/documents/SN06801/SN06801.pdf, *archived at* https://perma.cc/2H2Y-JBCF.

Jurisdictional Surveys
Other Countries

Canada

Tariq Ahmad
Foreign Law Specialist

SUMMARY Canada has yet to recognize "a right to be forgotten" or to enact erasure laws. However, injured parties can use the complaint procedure under the Personal Information Protection and Electronic Documents Act. Persons who find personal information on websites without their consent that has an impact on their reputation have turned to the Office of the Privacy Commissioner for assistance to remove the material. In addition, online defamatory material is typically dealt with through a common-law action for libel (defamation). Defamatory content can be removed through interlocutory or permanent injunctions issued by courts, but such remedies appear to be difficult to obtain. Legislation at the federal and provincial levels has been passed to deal with online reputational harms such as revenge porn and cyberbullying.

I. Background

In Canada, the right to privacy is based on number of rights under the Canadian Charter of Rights and Freedoms.[1] The Privacy Commissioner of Canada notes that "[t]he Charter does not specifically mention privacy or the protection of personal information. However, it does afford protection under Section 7 (the right to life, liberty and the security of the person), and Section 8 (the right to be secure against unreasonable search or seizure)."[2]

The removal of personal information that impacts a person's reputation is done largely through the application of Canada's privacy laws. There are a number of laws on the federal and provincial levels in Canada that relate to the protection of personal information. The Personal Information Protection and Electronic Documents Act (PIPEDA) is a federal privacy law that is applicable to the private sector.[3] In addition, injunctive relief can be provided for online defamatory material, as discussed below.

Canada does not yet recognize "a right to be forgotten." However, there has been some debate over whether various decisions, including a recent decision of the Federal Court of Canada, *A.T. v. Globe24h.com*,[4] could open the door to such a right.[5]

---

[1] Canadian Charter of Rights and Freedoms, Constitution Acts, 1867 to 1982, http://laws-lois.justice.gc.ca/eng/Const/page-15.html, *archived at* https://perma.cc/7NPJ-S9P3.

[2] *Your Privacy Rights*, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA (OPC), https://www.priv.gc.ca/en/privacy-topics/your-privacy-rights/ (last modified Sept. 28, 2015), *archived at* https://perma.cc/6P9J-YX4W.

[3] Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5, http://laws-lois.justice.gc.ca/eng/acts/P-8.6/FullText.html, *archived at* https://perma.cc/474H-3BTQ.

[4] A.T. v. Globe24h.com, 2017 FC 114 (CanLII), https://www.canlii.org/en/ca/fct/doc/2017/2017fc114/2017fc114.pdf, *archived at* https://perma.cc/C8XY-KHVU.

[5] Mark Hayes & Adam Jacobs, *Forget 'Right to Be Forgotten' Until the Right Case Comes*, THE LAWYERS DAILY (Mar. 23, 2017), https://www.thelawyersdaily.ca/articles/3208/forget-right-to-be-forgotten-until-the-right-case-

II. The Right to be Forgotten Debate

In 2015, the Privacy Commissioner of Canada established four strategic privacy priorities "in support of his vision to give Canadians more control over their personal information."[6] One of the priorities was "Reputation and Privacy,"[7] where a stated aim of the Office of the Privacy Commissioner (OPC) is to "help create an online environment where individuals may use the Internet to explore their interests and develop as persons without fear that their digital trace will lead to unfair treatment."[8] As part of this strategy the Policy and Research Group of the OPC drafted a policy position on "recourse mechanisms, such as the right to be forgotten in the Canadian legal context."[9] According to the policy paper, in Canada "no right to be forgotten or erasure laws exist *per se*."[10] The OPC goes on to discuss what would need to be considered before such a right were to be introduced in the Canadian context:

> As for the "right to be forgotten" debate, if such a mechanism were to be considered in Canada, there would need to be a careful balancing with other societal values, such as the right to freedom of expression, which is guaranteed under the Canadian Charter of Rights and Freedoms. While freedom of expression is already restricted in Canada by hate speech, obscenity, libel and defamation laws, freedom of expression remains a corner stone of Canada's democratic system, allowing individuals to express their opinions and ideas without interference or constraint by the government. In the digital realm, many of the measures used to control threats to privacy and reputation can also constrain freedom of expression. Threats to restrict free speech online have a chilling effect on people's willingness and ability to express themselves fully. At the same time, however, there is also a strong public interest in curbing the posting of personal information that is harmful and damaging to people's reputations particularly on a "net that never forgets."[11]

In January 2016, the Office of the Privacy Commissioner of Canada launched a consultation on the issue of online reputation. According to the OPC's website,

---

comes, *archived at* https://perma.cc/9QQQ-5XP6; Fasken Martineau DuMoulin LLP, *The "Right to Be Forgotten" Has a Three-piece Suit Tailor-made in Canada? From Quebec to British Columbia*, LEXOLOGY (Mar. 10, 2017), https://www.lexology.com/library/detail.aspx?g=d428aca4-761f-4990-b4bc-0d9895c09e8d, *archived at* https://perma.cc/MNU8-C85H.

[6] *OPC Strategic Privacy Priorities*, OPC, https://www.priv.gc.ca/en/about-the-opc/opc-strategic-privacy-priorities/(last modified Sept. 9, 2016), *archived at* https://perma.cc/RD22-M8Q8.

[7] *The Strategic Privacy Priorities*, OPC, https://www.priv.gc.ca/en/about-the-opc/opc-strategic-privacy-priorities/the-strategic-privacy-priorities/#reputation (last modified Sept. 9, 2016), *archived at* https://perma.cc/Q422-VKPS.

[8] *Id*.

[9] *Id*.

[10] POLICY AND RESEARCH GROUP OF THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, ONLINE REPUTATION: WHAT ARE THEY SAYING ABOUT ME? (Jan. 2016), https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/or_201601/#heading-0-0-7, *archived at* https://perma.cc/98HH-FBLD.

[11] *Id*.

> [t]hrough this consultation, the OPC is soliciting input about new and innovative ways to protect reputational privacy. The goal is to enrich the public debate and ensure that OPC is in a better position to inform Parliament of a variety of solutions for addressing issues related to online reputation and to develop a policy position on this issue.[12]

Some twenty-eight submissions were made by the stakeholders, including individuals, organizations, universities, defense groups, and others,[13] who participated in the consultation.[14] According to one article, "seventeen briefs expressed a position on the 'right to be forgotten' in Canada. The end result: 10 against, 4 neutral, 3 in favour (including one concerning the specific case of children)."[15]

III. Privacy Complaints Filed with the Office of the Privacy Commissioner

Persons who find personal information on websites without their consent that has an impact on their reputation have turned to the OPC for assistance to remove the material. If a person feels that his or her personal information has been wrongfully collected, used, or disclosed he or she may file a complaint with the OPC.[16]

PIPEDA "sets out the rules private sector organizations must follow when they handle personal information in the course of their commercial activities."[17] The Act applies to all private-sector organizations in Canada except in provinces that have enacted "substantially similar" legislation. OPC oversees compliance with the Act. According to the OPC,

> [g]enerally, organizations cannot collect, use or disclose personal information without consent unless an exception to the requirement for consent applies. The law also gives individuals the right to access and to ask for corrections to personal information an organization may have collected about them.[18]

The exceptions to the consent requirement are stipulated under section 4(2) of the Act and include an organization that "collects, uses or discloses [information] for journalistic, artistic or literary purposes."[19] Section 5(3) of the Act also stipulates that "[a]n organization may collect,

---

[12] *Consultation on Online Reputation*, OPC, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/ (last modified Jan. 1, 2017), *archived at* https://perma.cc/7CR9-75YF.

[13] Fasken Martineau DuMoulin LLP, *supra* note 5.

[14] *Submissions Received for the Consultation on Online Reputation*, OPC, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/submissions-received-for-the-consultation-on-online-reputation/ (last modified Jan. 17, 2017), *archived at* https://perma.cc/ZJ4A-QRAJ.

[15] Fasken Martineau DuMoulin LLP, *supra* note 5.

[16] *File a Formal Privacy Complaint*, OPC, https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/ (last modified Sept. 13, 2016), *archived at* https://perma.cc/9TG5-5CVF.

[17] *File a Complaint about a Business*, OPC, https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/file-a-complaint-about-a-business/ (last modified Sept. 9, 2016), *archived at* https://perma.cc/36EV-HP7W.

[18] POLICY AND RESEARCH GROUP OF THE OPC, *supra* note 10.

[19] PIPEDA § 4(2)(c).

use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances."[20]

If the complaint is "substantiated or well-founded", the OPC issues a Report of Findings that contains the following elements:

- A summary of both sides' positions and what the investigation uncovered;
- The findings and recommendations;
- Any agreement reached by the parties;
- If appropriate, a request that the organization provide, within a specified time, notice of any action taken or proposed to be taken with respect to the recommendations; or reasons why no such action has been or is proposed to be taken; and
- The recourse, if any, that is available to the Federal Court under the Act.[21]

The websites that are typically involved in complaints about reputational issues "include dating sites, sites that re-post court and tribunal decisions, and, overwhelmingly, the so-called revenge and shaming sites."[22] According to the OPC,

> [o]ne of the biggest challenges for the OPC in dealing with issues of online reputation has been asserting jurisdiction over the sites that come to our attention, particularly when they are based outside of Canada. In those circumstances, there may not always be a real and substantial connection to Canada, which is required in order for a foreign-based organization to be subject to PIPEDA. Moreover, in order for PIPEDA to apply, the website needs to be engaged in commercial activity. It is not unusual to find personal information posted without consent on websites set up for strictly personal use with no commercial purpose.[23]

According to section 14 of PIPEDA, after receiving the Commissioner's report or being notified that the investigation of the complaint has been discontinued, a complainant can apply to the Federal Court. Either party may appeal a decision of the Federal Court to the Federal Court of Appeal "if they are unsatisfied with the Court's ruling."[24]

A recent Federal Court case, *A.T. v. Globe24h.com*, disputed the republishing by the Romanian-based website Globe24h of a significant number of public documents, including Canadian court and tribunal decisions that are available on Canadian legal websites such as CanLII.org.[25] The

---

[20] *Id*. § 5(3).

[21] *What Happens When You File a Complaint under PIPEDA*, OPC, https://www.priv.gc.ca/en/report-a-concern/file-a-formal-privacy-complaint/file-a-complaint-about-a-business/guide/ (last modified Dec. 12, 2012), *archived at* https://perma.cc/4C2E-L8NW.

[22] POLICY AND RESEARCH GROUP OF THE OPC, *supra* note 10.

[23] *Id*.

[24] *Federal Court Applications under PIPEDA*, OPC, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/federal-court-applications-under-pipeda/ (last modified Sept. 27, 2017), *archived at* https://perma.cc/J2DB-CQ24.

[25] A.T. v. Globe24h.com, 2017 FC 114 (CanLII), para. 10, https://www.canlii.org/en/ca/fct/doc/2017/2017fc114/2017fc114.pdf, *archived at* https://perma.cc/C8XY-KHVU.

content on these websites is "generally not indexed and a person seeking such information must go directly to each site and conduct a search with the names of the parties."[26] Globe24h.com republished the content and "permitted these to be indexed and located by search engines such as Google. Such indexing meant that highly sensitive personal information ranging from divorce and immigration issues to personal bankruptcies and health particulars could be easily searched by anyone using a basic search engine."[27] The Federal Court ordered removal of all Canadian decisions containing "personal information from Globe24h.com and any further copying and republishing of such Canadian decisions, along with damages of [Can]$5000."[28] The significance of the case is that it confirmed that PIPEDA "applies to foreign based organizations where there is a 'real and substantial connection' and that Canadian privacy rights will be enforced by the courts across borders."[29] Though the Court does not directly recognize a "right to be forgotten," some commentators believe that it might be a step in that direction and is consonant with "right to be forgotten" rulings by "other [European] courts that have ordered online service providers to remove or disable access to personal information made available over the Internet."[30]

Another recent Supreme Court case that often comes up in the context of the discussion over the "right to be forgotten" in Canada is *Google Inc. v. Equustek*.[31] Though not directly related to privacy or the "right to be forgotten," it does deal with the power of the Court to issue a worldwide injunction ordering the search engine Google to delist certain websites. The Supreme Court of Canada upheld the grant of a "preliminary injunction by the Court of Appeals of British Columbia ordering Google to de-index on a global basis websites of a party accused of passing off the plaintiff's goods and misusing its trade secrets."[32]

IV. Defamation Actions and Similar Remedies

Online defamatory material is typically dealt with through a common-law action for libel (defamation). Defamatory content can be removed through interlocutory or permanent

[26] *Id*. para. 11.

[27] Practical Law Canada Commercial Transactions, *The Extra-Territorial Reach of PIPEDA: T. (A.) v. Globe24h.com*, THOMSON REUTERS PRACTICAL LAW (Feb. 22, 2017), https://ca.practicallaw.thomsonreuters.com/w-005-9407?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1, *archived at* https://perma.cc/7VLN-QA37.

[28] *Id*.

[29] *Id*.

[30] McCarthy Tétrault LLP, *PIPEDA's Global Extra-territorial Jurisdiction: A.T. v. Globe24h.com*, LEXOLOGY (Feb. 3 2017), https://www.lexology.com/library/detail.aspx?g=d74585f3-8961-4387-a2ac-9c5fc2a02b48, *archived at* https://perma.cc/R875-MKUM.

[31] Google Inc. v. Equustek Solutions Inc., 2017 SCC 34, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do, *archived at* https://perma.cc/2K45-AGYU.

[32] John Richards, *Google Inc. v. Equustek & the Supreme Court of Canada*, LEXOLOGY (Sept. 12 2017), https://www.lexology.com/library/detail.aspx?g=430b17b9-e4cd-4313-accd-0484e56edbec, *archived at* https://perma.cc/6C2N-586U.

injunctions issued by courts, but such remedies are difficult to obtain.[33] Elements that typically apply to defamation also apply to online defamation. However, in respect to online material, the Canadian courts have been dealing with a number of challenges, including "whether words posted on the internet were capable of defamatory meaning,"[34] establishing who is a publisher (including whether or not a hyperlink is considered a publication), whether Google can be considered a publisher, and jurisdictional issues such as forum shopping.[35]

Note that in Canada defamation can in some circumstances constitute a criminal offense under section 298 of the Criminal Code. For example, in the Ontario court case *R. v Simoes*, a "restaurant customer posted negative reviews about an Ottawa restaurant. In retaliation, the restaurant's owner began a harassment campaign that included setting up a false profile of the diner on a dating site and sent lewd e-mails to the customer's employer."[36] The restaurant owner was convicted of defamatory libel by the Ontario Court, and was sentenced to jail time.[37]

In addition, the privacy tort "may provide recourse either by statute or at common law, such as the emerging tort of intrusion upon seclusion in Ontario."[38] The tort of "intrusion upon seclusion" was established by the Ontario Court of Appeal in the 2012 decision of *Jones v. Tsige*.[39] In 2016, the Ontario Superior Court in *Jane Doe 464533 v. ND* also recognized for the first time in Canada the privacy tort of "publication of embarrassing private facts."[40]

V. Protecting Canadians from Online Crime Act and Provincial Legislation

The OPC notes that, "[a]s online reputational harms become more widespread, legislators have been passing laws aimed at supplementing defamation laws and addressing specific online problems."[41] Media attention towards online bullying and the resulting suicides of two young

[33] Karen R. Zimmer, *Canada: Privacy Vs. Free Speech on the Internet: An Update on the Right to Be Forgotten and What Is Happening at Home*, MONDAQ (Aug. 29, 2017), http://www.mondaq.com/canada/x/623970/IT+internet/Privacy+Vs+Free+Speech+On+The+Internet+An+Update+On+The+Right+To+Be+Forgotten+And+What+Is+Happening+At+Home, *archived at* https://perma.cc/U4T9-BP6T.

[34] Elizabeth Segal, *Internet Defamation Law: Update* 9.1.2 (CLE BC Paper 9.1, Torts–2013), https://www.cle.bc.ca/PracticePoints/TECH/14-InternetDefamationLaw.pdf, *archived at* https://perma.cc/3C7H-FEBS; *see also* Bryan G. Baynham, Daniel J. Reid, *The Modern-Day Soapbox: Defamation in the Age of the Internet*, DEFAMATION LAW PAPER 3.1(2010), http://www.cle.bc.ca/practicepoints/lit/11-modernsoapbox.pdf, *archived at* https://perma.cc/7L4T-X5GH.

[35] Segal, *supra* note 34, at 9.1.6.

[36] POLICY AND RESEARCH GROUP OF THE OPC, *supra* note 10.

[37] *Id*.

[38] *Id*.

[39] Jones v. Tsige, 2012 ONCA 32 (CanLII), https://www.canlii.org/en/on/onca/doc/2012/2012onca32/2012onca32.pdf, *archived at* https://perma.cc/2WAV-BSHR.

[40] Jane Doe 464533 v N.D., 2016 ONSC 541 (CanLII), https://www.canlii.org/en/on/onsc/doc/2016/2016onsc541/2016onsc541.pdf, *archived at* https://perma.cc/6FMD-G5TG.

[41] POLICY AND RESEARCH GROUP OF THE OPC, *supra* note 10.

Canadians helped push the passage of the Protecting Canadians from Online Crime Act,[42] which received Royal Assent on December 2014. The Act introduced a hybrid offense aimed at criminalizing the publication of intimate images without consent. The Law also introduced amendments to

> authorize the removal of such images from the Internet and the recovery of expenses incurred to obtain the removal of such images, the forfeiture of property used in the commission of the offence, a recognizance order to be issued to prevent the distribution of such images and the restriction of the use of a computer or the Internet by a convicted offender.

Some provinces, including Manitoba, Alberta,[43] and Nova Scotia,[44] have introduced legislation against cyberbullying and revenge porn. In Manitoba, the Intimate Image Protection Act (IIPA) establishes a civil tort action against the nonconsensual distribution of intimate images. A person who distributes an intimate image of another person that gave rise to a reasonable expectation of privacy, "knowing that the person depicted in the image did not consent to the distribution, or being reckless as to whether or not that person consented to the distribution, commits a tort against that other person." [45] This allows residents to sue perpetrators in civil court for damages or other remedies, such as injunctions.

[42] Protecting Canadians from Online Crime Act, S.C. 2014, c. 31, http://laws-lois.justice.gc.ca/eng/annualstatutes/2014_31/FullText.html, *archived at* https://perma.cc/R9V8-J7SL.

[43] Protecting Victims of Non-consensual Distribution of Intimate Images Act, Statutes of Alberta, 2017 ch. P-26.9, http://www.qp.alberta.ca/documents/Acts/P26p9.pdf, *archived at* https://perma.cc/VZ8N-LQFS.

[44] Intimate Images and Cyber-protection Act, Bill No. 27, 1st Session, 63rd General Assembly Nova Scotia, 66 Elizabeth II, 2017, http://nslegislature.ca/legc/bills/63rd_1st/1st_read/b027.htm, *archived at* https://perma.cc/65AX-7LMG. Nova Scotia previously had cyber-bullying legislation known as the Cyber-safety Act, but it was struck down in 2015 by the Nova Scotia Supreme Court as unconstitutional. Crouch v. Snell, 2015 NSSC 340, https://www.canlii.org/en/ns/nssc/doc/2015/2015nssc340/2015nssc340.pdf, *archived at* https://perma.cc/JBH7-26DG.

[45] Intimate Image Protection Act, Bill 38, 4th Session, 40th Legislature, Manitoba, 64 Elizabeth II, 2015, https://web2.gov.mb.ca/bills/40-4/b038e.php, *archived at* https://perma.cc/H6K3-ZB7Z.

Israel

Ruth Levush
Senior Foreign Law Specialist

SUMMARY As a general rule a "right to be forgotten" is not recognized under Israeli law except in regard to the erasure of information on convictions from the criminal register under conditions enumerated by law. Online defamatory publications may be ordered removed. In addition, website owners and search engine companies who neglect to remove a publication after being informed of its inaccurate and defamatory nature may be liable for payment of compensation.

I. Right to Be Forgotten Not Recognized

Israeli law does not recognize a comprehensive "right to be forgotten" similar in scope to the one recognized under EU law.[1] Four private members' draft bills calling for recognition of such a right have been filed with the Knesset (Israel's parliament) since 2014, with the latest as of February 2017. None have so far been considered.[2]

In a 2015 decision Israel's Supreme Court voided a decision by the Court Administration (CA) to require companies operating commercial databases to commit to not indexing court decisions retrieved from the CA's databank. This requirement would have prevented court decisions published by such companies from being retrieved via internet search engines, including Google and Bing.[3]

The Supreme Court noted that at the time of the decision the right to be forgotten had not been generally recognized under US law. Nor was EU law clear on whether the right extended to officially published court decisions. The Court further commented that Israel's Criminal Registry and Rehabilitation Law, 5741-1981[4] addressed "a specific aspect of the issue" by ordering the erasure of information on convictions from the criminal register ten years after the

[1] *Factsheet on the "Right to be Forgotten" Ruling* (C-131/12), EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (last visited October 23, 2017), *archived at* https://perma.cc/ZG46-2W42.

[2] List of search results on the National Legislation Database (using the search term הזכות להישכח, "the right to be forgotten" in Hebrew): http://main.knesset.gov.il/Activity/Legislation/Laws/Pages/LawSuggestionsSearch.aspx?t=lawsuggestionssearch&st=allsuggestions&wn=%d7%94%d7%96%d7%9b%d7%95%d7%aa%20%d7%9c%d7%94%d7%99%d7%a9%d7%9b%d7%97&ki=-1&sb=LatestSessionDate&so=D, *archived at* https://perma.cc/27LS-3XHY.

[3] HCJ 5870/14 Hashavim v. Court Administration (Nov. 12, 2015), http://elyon1.court.gov.il/files/14/700/058/t17/14058700.t17.pdf (in Hebrew), *archived at* https://perma.cc/S7K2-94MQ; *see also* Ruth Levush, *Israel: Preventing Web Search Retrieval of Court Decisions Held Unlawful*, GLOBAL LEGAL MONITOR (Dec. 7, 2015), http://loc.gov/law/foreign-news/article/israel-preventing-web-search-retrieval-of-court-decisions-held-unlawful/, *archived at* https://perma.cc/DK9B-CJ3G.

[4] Criminal Registry and Rehabilitation Law, 5741-1981, § 16, SEFER HAHUKIM [SH] [BOOK OF LAWS (official gazette)] No. 1031, p. 322.

passage of the applicable statute of limitation, depending on the sentence imposed on the offender.[5] According to drafters of the legislation, the Court stated, the objective of the Law was to support the rehabilitation of offenders and assist them in participating fully in society.[6]

II. Counteracting Online Defamation

The Defamation Law, 5725-1965 defines a defamatory matter as one the publication of which may harm a person's "estimation" by others, bring the person into disrepute because of acts, conduct or qualities attributed to him, because of his/her origin, religion, residence, age, gender, sexual orientation or disability, or harm the person's position, vocation or profession.[7] For the purpose of defamation a "publication" includes by speech, writing, printing, or "any other means."[8]

In a 2015 decision by the Tel Aviv District Court, the Court held that both the owner of a website and Google were liable for defamation under the Defamation Law, 5725-1965. Under the circumstances of the case the court imposed damages on Google for neglecting to change a technical code, the operation of which had resulted in the creation of defamatory information in online searches.[9]

[5] HCJ 5870/14, ¶ 15.

[6] *Id.*

[7] Defamation Law, 5725-1965, § 1, SH No. 464, p. 240, *as amended*.

[8] *Id*. § 2(a).

[9] CA (TA) 44711-11-14, Savir v. Bar Noi & Google Inc. (June 22, 2015), available at the Nevo Legal Database (in Hebrew; by subscription), *archived at* https://perma.cc/P7GM-JTSB.

Japan

Sayuri Umeda
Foreign Law Specialist

SUMMARY The Provider Liability Limitation Act limits the liability of online hosting providers when they block information that infringes on others' rights. The Act also makes it easier for victims to find identifiable information about offenders. Businesses have developed guidelines on the procedures and criteria for determining whether rights have been infringed. The Legal Affairs Bureau of the Ministry of Justice may assist victims.

A specific law deals with so-called revenge porn. The law made it easier for websites to block images.

The right to be forgotten has not been recognized by the Japanese Supreme Court. Requests not to display infringing information in search results generated by search engines are examined under the framework of the right to privacy. Search engine owners have established their own procedures and criteria to determine whether to honor such requests to remove information from search results.

I. Removal of Infringing Information Online

A. Ability to Request Removal of Defamatory Information

A person whose rights have been infringed by a defamatory online posting may submit a request for the deletion of the content to the person who posted it. There is no legal provision that directly establishes a right to demand the deletion of defamatory online content, but it is generally regarded that such a right derives from the "personal right."[1] In addition, a person who posts defamatory information about a person online may be liable for damages to that person[2] and/or face a criminal charge.[3]

[1] Tomohiro Kanda, 誹謗中傷・風評被害対策/削除 [*Deletion/Countermeasures Against Slander & Bad Rumor*], IT LAWYER TOMOHIRO KANDA, https://kandato.jp/deletion/ (last visited Oct. 31, 2017), *archived at* https://perma.cc/H5MD-A34Y. The term "personal right" is used in Japan to denote the right to various matters, such as life, body, liberty, honor, and chastity, other than financial interests. 法律学小辞典 [LAW DICTIONARY] 668 (Hiroshi Kaneko et al. eds., 2008), *bibliographic record at* https://lccn.loc.gov/2010371455.

[2] CIVIL CODE, Act No. 89 of 1896, *amended by* Act No. 44 of 2017, arts. 709 & 710.

[3] PENAL CODE, Act No. 45 of 1907, *amended by* Act No. 72 of 2017, art. 230.

B. Liability of Internet Hosting Providers

1. Liability with Respect to a Victim of Defamation

It is understood that an internet hosting provider (e.g., a website) may have an obligation to delete defamatory content. The Tokyo High Court has stated that this obligation derives from the general rule of reason.[4]

The Provider Liability Limitation Act limits the liability of internet hosting providers. When any rights of others, such as those concerning privacy, copyright, and trademarks, are infringed by the distribution of information via the internet, the internet hosting provider is not liable for any loss incurred from such infringement, unless

> (i) the provider knew that the infringement of the rights of others was caused by distribution of the information via its service; or
> (ii) it is regarded with reasonable grounds that the provider could have known the infringement of the rights of others was caused by the distribution. [5]

If it was technically impossible to take measures to prevent such information from being transmitted to unspecified persons, the provider is not liable.[6]

2. Liability with Respect to the Offender

When an internet hosting provider has taken measures to block transmission of information via the internet, the provider is not liable for any loss incurred by the sender of such information in cases where

> (i) there was a reasonable ground to believe that the rights of others were infringed without due cause by the distribution of the information; or
> (ii) the provider did not receive any notice of disagreement with implementation of measures to block the infringing information from its sender within seven days from the day the provider inquired the sender [sic] after a person alleging that his right was infringed by the distribution of information requested the provider to take measures to block the infringing information.[7]

---

[4] Heise 14 (ne) 4083, Tokyo High Ct. (Dec. 25, 2002), http://www.courts.go.jp/app/hanrei_jp/detail3?id=20111 (to see the text of the judgment, click characters besides PDF icon), *archived at* https://perma.cc/S5B5-H7FA & https://perma.cc/53XW-EKMH.

[5] 特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律 [Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders] (Provider Liability Limitation Act), Act No. 137 of 2001, *amended by* Act No. 10 of 2013, art. 3, para. 1, English translation (made prior to the 2013 amendment) *available at* http://www.japaneselawtranslation.go.jp/law/detail_main?re=02&ia=03&vm=02&id=2088 (last visited Oct. 31, 2017), *archived at* https://perma.cc/XRQ4-HK5T.

[6] *Id*.

[7] *Id*. art. 3, para. 2.

The measures to block the infringing information must be limited to those necessary for preventing transmission of such information to unspecified persons.[8]

Special provisions apply to information circulated during campaigns for public office. In such cases the sender's response period is reduced from seven days to two days. In addition, if the website does not provide the email address required under the Public Office Election Act during the period that the online campaign is conducted, the hosting service can block the webpage upon request.[9]

C. Request that Internet Hosting Provider Block Infringing Information

As stated in the previous section, the Provider Liability Limitation Act provides a procedure for requests that a hosting provider block or remove infringing information. When the alleged victim sends such a request to a hosting provider, the request must specify both the infringing information and the infringed right, and provide an explanation of the infringement.[10] Then, the provider notifies the person who posted the infringing information of the request. The provider either fulfills the request with the permission of the person who posted it or removes the content without the person's approval if the person fails to respond within seven days. If the person refuses permission, the Act allows the provider to assess the blocking request itself and block the information if it believes the request is legitimate.[11]

Business organizations established a council to develop guidelines for providers to follow when deciding what type of information must be blocked, and to explain the procedures under the Act. The Ministry of Internal Affairs and Communications (MIAC) served as an observer to the council.[12] The guidelines were published in 2002 and have been amended three times since then.[13]

Victims may receive assistance from regional Legal Affairs Bureaus of the Ministry of Justice. At first, a Bureau gives advice to a victim on filing a blocking request with a provider. If the provider does not respond or refuses to block the infringing information, the Bureau examines whether the person's right was infringed by the information. If it determines that an infringement of rights occurred, the Bureau itself may request that the provider block the

[8] *Id*.

[9] *Id*. art. 3-2.

[10] *Id*. art. 3, para. 2.

[11] *Id*.

[12] HIROYUKI KUWAKO, プロバイダ責任制限法に関する取り組み状況など [REGARDING IMPLEMENTATION OF THE PROVIDER LIABILITY LIMITATION ACT] 2 (Dec. 21, 2010), http://www.soumu.go.jp/main_content/000097094.pdf, *archived at* https://perma.cc/T8AR-2TB8.

[13] Provider Liability Limitation Act Guidelines Review Council, プロバイダ責任制限法，名誉毀損・プライバシー関係ガイドライン [Provider Liability Limitation Act, Guidelines Relating to Defamation and Privacy] (May 2002, amended Dec. 2014), http://www2.telesa.or.jp/consortium/provider/pdf/provider_mguideline_20141226.pdf, *archived at* https://perma.cc/54AT-URMN, English translation *available at* http://www.telesa.or.jp/wp-content/uploads/consortium/provider/pdf/guidelines_defamation.pdf, *archived at* https://perma.cc/MJL8-ETZP.

information.[14] The guideline states that a provider blocks information when the Bureau requests it unless they find a reason not to do so.[15]

D. Disclosure of Identifiable Information of Offender by Service Provider

Because defamatory online postings are often done anonymously, it is hard for victims to identify offenders in order to take measures against them. The Provider Liability Limitation Act made it easier for victims to obtain information about the offender.

When a person's right has been infringed by the distribution of information via the internet, the person may demand that the internet service providers using the facilities that distributed the information to disclose identifiable information about the sender of the information that the provider possesses when the following conditions are met:

> (i) There is evidence that the right of the person demanding disclosure of identifiable information was infringed by the distribution of the infringing information; and
> (ii) The person who demands the information has a justifiable reason to obtain identifiable information of the sender, e.g. in case it is necessary for the person demanding the disclosure to exercise his or her rights to claim damages.[16]

Two inquiries may be needed to identify the sender: first an inquiry to the hosting provider to obtain the IP address and time stamps of the sender; and second to the internet service provider to obtain the name and address of the sender.[17]

When a provider receives such a demand, it must hear the opinion of the sender of the infringing information on whether the sender consents to the disclosure of his or her identifiable information, except where said provider is unable to contact the sender or where special circumstances exist.[18] However, even if the sender disagrees to the disclosure, the hosting provider can disclose the information if the disclosure request meets the above conditions.[19]

A person who receives the identifiable information of the sender must not unjustly damage the reputation or disturb the peaceful existence of the sender by using it without due cause.[20] The Act exempts a provider who discloses information from liability for any loss incurred by the

---

[14] インターネットを悪用した人権侵害をなくしましょう [*Let's Eliminate Human Rights Infringements via Internet*], MOJ, http://www.moj.go.jp/JINKEN/jinken88.html (last visited Oct. 27, 2017), *archived at* https://perma.cc/ABW4-QU7C.

[15] Provider Liability Limitation Act, Guidelines Relating to Defamation and Privacy, *supra* note 11, at 39.

[16] Provider Liability Limitation Act art. 4, para. 1.

[17] HIDEYUKI SEKIHARA, 基本講義プロバイダ責任制限法 [BASIC LECTURE ON PROVIDER LIABILITY LIMITATION ACT] 132 (2016), *bibliographic record at* https://lccn.loc.gov/2016516599.

[18] Provider Liability Limitation Act art. 4, para. 2.

[19] *Id*. art. 4, para. 1.

[20] *Id*. art. 4, para. 3.

person to whom the provider gave the information, unless there is a willful act or gross negligence on the part of the provider.[21]

E. Revenge Porn

The Revenge Porn Prevention Act criminalizes the provision of a private sexual image of another person without the person's approval via a means of telecommunication to an unspecified number of, or many, people.[22] In addition, the Act makes blocking revenge porn images upon the victim's request easier and faster than the procedure under the Provider Liability Limitation Act. The Act allows internet service providers to block transmission of suspected revenge porn images without the uploader's consent in cases where

> 1. the victim had requested the provider to block his/her sexual images by showing infringement of his/her honor by the image and the private nature of the image;
> 2. the provider had inquired the uploader if he or she consents to delete the image; and
> 3. the uploader did not object [to] the blocking of the image within two days. [23]

If the victim is deceased, his or her family member may request blocking.[24]

II. Removal of Information by Search Engines

There is no explicit legal provision that establishes the liability of owners of internet search engines for displaying search results that infringe a person's personal rights. Recent court decisions have discussed the obligation of search engine owners to remove webpages containing infringing content from search results upon request.[25]

Recently, the Supreme Court decided such a case without mentioning the so-called right to be forgotten. On January 31, 2017, the Supreme Court rejected a petitioner's demand that Google remove web search results that displayed reports of his arrest for child prostitution in 2011.[26] In this case, the Court set forth the general rule that the adverse effects of invasion of privacy versus the importance of the provision of search results must be weighed in individual cases, and when the right to privacy prevails, the person whose information was revealed may demand the deletion of the search results. The Court set forth the following elements to be considered in balancing the two:

---

[21] *Id*. art. 4, para. 4.

[22] 私事性的画像記録の提供等による被害の防止に関する法律 [Act on Prevention of Damage by Provision of Private Sexual Image Records], Act No. 126 of 2014, art. 3.

[23] *Id*. art. 4 (translation by author).

[24] *Id*.

[25] Katsuya Uga, 「忘れられる権利」について [*Concerning the "Right to Be Forgotten"*], QUARTERLY JURIST (No. 16) 24, 28–32 (2016 Summer), *bibliographic record at* https://lccn.loc.gov/2012273170.

[26] Heisei 28 (Kyo) 45 (Sup. Ct., Jan. 31, 2017), http://www.courts.go.jp/app/hanrei_jp/detail2?id=86482 (click Chinese characters beside the PDF icon), *archived at* https://perma.cc/E9BA-EMKC & https://perma.cc/ZT9R-PATB.

- the nature of the information;
- the extent to which the information is spread by the search results;
- the extent of adverse effects for the person who is the subject of the search;
- the public status of the searched person;
- the purpose and meaning of the presentation of the information on the websites;
- change of society, if any, between the posting of the information and the present time; and
- necessity of the description on the posting.[27]

The Court decided the issue under the framework of the general right to privacy without recognizing the right to be forgotten.[28]

The MIAC established a research group in May 2017 to discuss the treatment of online information that individual subjects do not want to be spread. The group is examining whether any measures should be recommended.[29]

Search engine companies have established their own policies to deal with requests to delete particular search results. According to Yahoo Japan's policy, it will not show a link to a web page on its search results if a court order is issued to the website manager to delete the contents, or if it decides there is an urgent need not to show the link because of highly infringing content, such as revenge-porn images.[30] Google states that it will remove children's pornographic images and, upon request, content that infringes a copyright from its search results. In addition, it will delete highly confidential personal information, such as national identification numbers, sexual images of persons uploaded without consent, and individuals' private medical information.[31]

[27] *Id*. (translation by author).

[28] Nobuyuki Sato, 最高裁は「忘れられる権利」を否定したのか？ [*Did the Supreme Court Deny the "Right to Be Forgotten"?*], WESTLAW JAPAN 判例コラム [Case Column], 臨時号 [Extra], No. 108, at 7, https://www.westlawjapan.com/pdf/column_law/20170609.pdf, *archived at* https://perma.cc/QHN7-P3LZ.

[29] Press Release, MIAC, インターネット上に公開された個人に関する情報等の取扱いに関する研究会」の開催 [Convening Study Group for Dealing With Personal Information Made Public Online] (May 16, 2017), http://www.soumu.go.jp/menu_news/s-news/01kiban18_01000019.html, *archived at* https://perma.cc/UN33-XMQ6.

[30] Yahoo Japan, 検索結果の非表示措置の申告を受けた場合のヤフー株式会社の対応方針について [*Policy on Responses by Yahoo Japan to Requests of No-Showing of Search Results*] (Mar. 30, 2015), https://s.yimg.jp/i/docs/publicpolicy/blog/20150330/Policy.pdf, *archived at* https://perma.cc/RV27-9ZGH.

[31] *Removal Policies*, GOOGLE, https://support.google.com/websearch/answer/2744324 (last visited Oct. 31, 2017), *archived at* https://perma.cc/BJ3K-RP7E.

New Zealand

Kelly Buchanan
Chief, Foreign, Comparative, and
International Law Division I

SUMMARY New Zealand's Harmful Digital Communications Act 2015 is intended to deter and mitigate "serious emotional distress" caused to individuals by digital communications, including text messages and the posting of information online, and to provide victims with a quick and efficient means of redress. It sets out a list of ten "communication principles," which include concepts drawn from other legislation, including the Privacy Act 1993 and Harassment Act 1997, and from causes of action such as defamation and the tort of intentional infliction of emotional distress. Individuals can complain to an independent agency about communications that breach these principles, and online content hosts must take certain steps to resolve complaints about information published on their sites in order to benefit from provisions that protect them from criminal or civil liability. The Act enables individuals to apply to the District Court for orders to remove harmful online content and other remedies, and establishes a new criminal offense of causing harm by posting a digital communication.

There is no "right to be forgotten" as such under New Zealand law. However, along with the Harmful Digital Communications Act 2015, there are other mechanisms through which inaccurate or offensive information online can be corrected or addressed.

I. Introduction

In 2015, the New Zealand Parliament passed the Harmful Digital Communications Act 2015 (the Act).[1] The introduction of the legislation in 2013 followed the submission of a ministerial briefing by the New Zealand Law Commission,[2] which examined the area of cyber bullying and "revenge porn" as part of its broader project on regulatory gaps with respect to "new media."[3] The resulting statute provides for a new complaint mechanism for information posted online about individuals, involving an "approved agency" that assists in resolving complaints, as well as a new civil process and criminal penalties for serious breaches of the Act. Online content hosts,

[1] Harmful Digital Communications Act 2015, http://www.legislation.govt.nz/act/public/2015/0063/latest/whole.html, *archived at* https://perma.cc/4TP2-KY37. *See* Kelly Buchanan, *New Zealand: Legislation Aimed at Preventing and Punishing Cyber Bullying Passed*, GLOBAL LEGAL MONITOR (July 6, 2015), http://www.loc.gov/law/foreign-news/article/new-zealand-legislation-aimed-at-preventing-and-punishing-cyberbullying-passed/, *archived at* https://perma.cc/7G5X-T6XK.

[2] NEW ZEALAND LAW COMMISSION, HARMFUL DIGITAL COMMUNICATIONS: THE ADEQUACY OF CURRENT SANCTIONS AND REMEDIES (Ministerial Briefing Paper, Aug. 2012), http://www.lawcom.govt.nz/sites/default/files/projectAvailableFormats/NZLC%20MB3.pdf, *archived at* https://perma.cc/GF4Z-CR77.

[3] *Regulatory Gaps and New Media*, NEW ZEALAND LAW COMMISSION, http://www.lawcom.govt.nz/our-projects/regulatory-gaps-and-new-media (last visited Oct. 26, 2017), *archived at* https://perma.cc/XTE4-VYKF.

such as websites and social media platforms, are protected from liability under the Act, provided they take certain steps to resolve complaints and remove content.[4]

The offense provisions and the provisions related to content host liability came into effect in July 2015, while the provisions related to complaint processes and civil proceedings came into effect in November 2016, at which time the Act was fully in force.[5]

II. Harmful Digital Communications Act 2015

A. Purpose and Scope of the Act

The purpose of the Act is to

> (a) deter, prevent, and mitigate harm caused to individuals by digital communications; and
> (b) provide victims of harmful digital communications with a quick and efficient means of redress.

"Harm" is defined in the Act to mean "serious emotional distress;" a "digital communication" means any form of electronic communication, including "any text message, writing, photograph, picture, recording, or other matter" that is communicated electronically. The term "individual" refers to natural persons only. An "online content host" "means the person who has control over the part of the electronic retrieval system, such as a website or an online application, on which the communication is posted and accessible by the user."[6]

B. Communication Principles

The Act lists the following "communication principles," which the approved agency and the courts must take into account:

1. A digital communication should not disclose sensitive personal facts about an individual.
2. A digital communication should not be threatening, intimidating, or menacing.
3. A digital communication should not be grossly offensive to a reasonable person in the position of the affected individual.
4. A digital communication should not be indecent or obscene.
5. A digital communication should not be used to harass an individual.
6. A digital communication should not make a false allegation.

[4] *Harmful Digital Communications: Key Parts of the Act*, MINISTRY OF JUSTICE, https://www.justice.govt.nz/justice-sector-policy/key-initiatives/harmful-digital-communications/key-parts-of-the-act/ (last updated Oct. 2, 2017), *archived at* https://perma.cc/TJA5-96QB.

[5] Harmful Digital Communications Act 2015, s 2; Harmful Digital Communications Commencement Order (No 2) 2016, http://www.legislation.govt.nz/regulation/public/2016/0226/latest/whole.html, *archived at* https://perma.cc/L355-T3TH.

[6] Harmful Digital Communications Act 2015, s 4.

7. A digital communication should not contain a matter that is published in breach of confidence.
8. A digital communication should not incite or encourage anyone to send a message to an individual for the purpose of causing harm to the individual.
9. A digital communication should not incite or encourage an individual to commit suicide.
10. A digital communication should not denigrate an individual by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability.

The legislation therefore applies with respect to cyber bullying and harassment, "revenge porn," and defamatory statements, among other types of harmful communications.

In essence, a digital communication may be deemed harmful if it

1. Is directed at an individual; and
2. Makes that person seriously emotionally distressed; and
3. It has or could seriously breach of one or more of the 10 communication principles in the Act.[7]

C. Complaint Processes

1. Complaints to an Independent Agency

Netsafe, an "independent, non-profit online safety organisation,"[8] was designated to be the "approved agency" under the Act in May 2016.[9] It has the following functions and powers with respect to alleged harmful communications:

> (a) to receive and assess complaints about harm caused to individuals by digital communications;
> (b) to investigate complaints;
> (c) to use advice, negotiation, mediation, and persuasion (as appropriate) to resolve complaints;
> (d) to establish and maintain relationships with domestic and foreign service providers, online content hosts, and agencies (as appropriate) to achieve the purpose of this Act;
> (e) to provide education and advice on policies for online safety and conduct on the Internet;
> (f) to perform the other functions conferred on it by or under this Act, ...[10]

[7] *The HDC Act and Netsafe*, NETSAFE (Nov. 25, 2016), https://www.netsafe.org.nz/hdc-act/, *archived at* https://perma.cc/GH5D-MPEX.

[8] *About Netsafe*, NETSAFE, https://www.netsafe.org.nz/aboutnetsafe/ (last visited Oct. 31, 2017), *archived at* https://perma.cc/DZW2-95WC.

[9] Harmful Digital Communications (Appointment of Approved Agency) Order 2016, http://www.legislation.govt.nz/regulation/public/2016/0102/latest/whole.html, *archived at* https://perma.cc/TB2S-G46R.

[10] Harmful Digital Communications Act 2015, s 8(1).

Netsafe explains its role in receiving and handling complaints about online statements as follows:

> Netsafe takes complaints of harmful digital communications and informs people about the options that are available to them to remedy the situation. Our service aims to lessen the harm caused to people targeted online by using persuasion, mediation and negotiation to help reach a resolution for both parties involved. Netsafe cannot punish people for their actions online, or force them to take action.[11]

It further explains that

> We'll tell you what you can do to keep safe, and if there's anything that can be done to stop the abuse. We may try to work with the person who is harassing you to get them to stop—but we won't contact them unless you say it's OK.
>
> We might also be able to contact the person or the organisation that runs the website, app or service that the messages or posts are on and ask for their help to resolve the issue.[12]

A toll-free number and an online form are available for people to report online abuse and can be used by the person who is the target of the abuse or by someone else on his or her behalf.[13]

2. Involvement and Protection of Online Content Host

The Act provides that an online content host is protected from civil or criminal proceedings if, when it receives a notice of complaint about specific content, it complies with provisions setting out the steps that it must take in response to such complaints. These include[14]

- providing a copy of the notice of complaint to the content author within forty-eight hours of receipt, and notifying the author that he or she may submit a counter-notice to the host within forty-eight hours after receiving the notification;
- if the host is unable to contact the content author, the host must take down or disable the specific content as soon as practicable, but no later than forty-eight hours after receiving notice of the complaint;
- if the author submits a counter-notice refusing to consent to the removal of the specific content, the host must leave that content in place and notify the complainant of the author's decision and, if the author consents, provide the complainant with personal information that identifies the author;

[11] *The HDC Act and Netsafe*, *supra* note 7.

[12] *Help with Online Harassment, Bullying & Abuse*, NETSAFE (Oct. 29, 2017), https://www.netsafe.org.nz/hdc/, *archived at* https://perma.cc/2M25-J3BR.

[13] *Report to Netsafe*, NETSAFE, https://www.netsafe.org.nz/report/ (last visited Oct. 31, 2017), *archived at* https://perma.cc/3WJ8-KJMA.

[14] Harmful Digital Communications Act, s 24(2).

- if the author does not submit a valid counter-notice, the host must take down or disable the specific content within forty-eight hours after notifying the author.

Netsafe may lodge a notice of complaint on behalf of the complainant.[15]

The protection of the host from liability "does not apply if the host does not provide an easily accessible mechanism that enables a user to contact the host about specific content" in the manner provided for in the Act.[16]

The provisions outlined above are referred to as the "safe harbour" process.[17] In essence, in order to claim safe harbor, a content host must

- make it easy for people to contact you with complaints about content posted by another person—your contact details need to be:
  - easy for users to find on your website;
  - set up so it is easy for people to make a complaint that contains the information outlined in the Act ([sample forms are provided]) and
- follow specific steps within the fixed timeframes when you receive a complaint.[18]

D. Civil Actions and Criminal Penalties

1. Civil Proceedings

The Act allows civil proceedings to be brought in the District Court by an affected individual, by his or her parent or guardian, by a "professional leader" of a school (e.g., a school principal), or by the police "if the digital communication constitutes a threat to the safety of an individual."[19] In order for proceedings to be brought, Netsafe must have received a complaint about the communication "and had a reasonable opportunity to assess the complaint and decide what action (if any) to take."[20] Furthermore, the threshold for the District Court to grant an application is that there has been a "threatened serious breach, a serious breach, or a repeated breach" of one

[15] *Id.* s 25(1).

[16] *Id.* s 25(2).

[17] *See Safe Harbour Provisions*, MINISTRY OF JUSTICE, https://www.justice.govt.nz/justice-sector-policy/key-initiatives/harmful-digital-communications/safe-harbour-provisions/ (last updated Sept. 7, 2016), *archived at* https://perma.cc/5XSA-8K5H.

[18] *Id.*

[19] Harmful Digital Communications Act 2015, s 11. *See also Harmful Digital Communications*, MINISTRY OF JUSTICE, https://www.justice.govt.nz/courts/civil/harmful-digital-communications/ (last visited Oct. 31, 2017), *archived at* https://perma.cc/E66G-37G3; *Applying for a Harmful Digital Communications Order*, MINISTRY OF JUSTICE, https://www.justice.govt.nz/courts/civil/harmful-digital-communications/applying-for-a-harmful-digital-communications-order/ (last visited Oct. 31, 2017), *archived at* https://perma.cc/2B7R-U2QV; *Respond to an Application or Interim Harmful Digital Communications Order*, MINISTRY OF JUSTICE, https://www.justice.govt.nz/courts/civil/harmful-digital-communications/respond-to-an-application-or-interim-harmful-digital-communications-order/ (last visited Oct. 31, 2017), *archived at* https://perma.cc/LB9H-GGQM.

[20] Harmful Digital Communications Act 2015, s 12(1).

or more communication principles, and the breach "has caused or is likely to cause harm to an individual."[21]

Following either a hearing or a determination based on the written material provided to it,[22] the District Court can make one or more of the following orders against a defendant:

> (a) an order to take down or disable material;
> (b) an order that the defendant cease or refrain from the conduct concerned;
> (c) an order that the defendant not encourage any other persons to engage in similar communications towards the affected individual;
> (d) an order that a correction be published;
> (e) an order that a right of reply be given to the affected individual;
> (f) an order that an apology be published.[23]

The Court can also issue orders against an online content host, including that it take down the material or disable public access to it, release the identity of the author to the Court, publish a correction, or give a right of reply to the affected individual.[24] It can make interim orders, as well as final orders.[25]

In deciding whether or not to make an order, the Court must have regard to certain factors, including the level of harm caused or likely to be caused by the communication, the purpose of the communicator, the context and subject matter of the communication, the extent to which the communication has spread, the age and vulnerability of the affected individual, the truth or falsity of the statement, whether the communication is in the public interest, the conduct of the defendant and the affected individual, and the technical practicalities and cost of the order.[26] The Court must also act consistently with the New Zealand Bill of Rights Act 1990, which protects, among other rights, the right to freedom of expression.[27]

2. Offenses and Penalties

The Act introduces a new offense of causing harm by posting a digital communication. The elements of this offense are

[21] *Id.* s 12(2).

[22] *Id.* s 17.

[23] *Id.* s 19(1).

[24] *Id.* s 19(2).

[25] *Id.* s 19.

[26] *Id.* s 19(5).

[27] *Id.* s 19(6). New Zealand Bill of Rights Act 1990, s 14, http://www.legislation.govt.nz/act/public/1990/0109/latest/whole.html, *archived at* https://perma.cc/2F3T-N9W5.

- posting a digital communication with the intention that it cause harm to the victim;
- posting the communication would cause harm to an ordinary reasonable person in the position of the victim; and
- posting the communication causes harm to the victim.[28]

The court "may take into account any factors it considers relevant," including

> (a) the extremity of the language used;
> (b) the age and characteristics of the victim;
> (c) whether the digital communication was anonymous;
> (d) whether the digital communication was repeated;
> (e) the extent of circulation of the digital communication;
> (f) whether the digital communication is true or false;
> (g) the context in which the digital communication appeared.[29]

A person convicted of this offense is liable to a term of imprisonment of up to two years or a fine not exceeding NZ$50,000.[30] If the defendant is a body corporate, the punishment is a fine of up to NZ$200,000.[31]

It is also an offense under the Act to fail to comply with an order of the court, with the penalties being imprisonment for up to six months or a fine of up to NZ$5,000 for a natural person, or a fine of up to NZ$20,000 for a body corporate.[32]

E. Relationship with Existing Provisions and Causes of Action

The principles in the Act draw on and complement various existing provisions and causes of action under New Zealand law. The Ministry of Justice stated in its departmental report on the bill, provided to the relevant parliamentary committee, that "[t]he principles are a plain language expression of New Zealand law which is intended to be accessible and understood by internet users, serving both educational and deterrent functions."[33] The departmental report included a table showing the legal sources for each of the principles:

---

[28] Harmful Digital Communications Act 2015, s 22(1).

[29] *Id.* s 22(2).

[30] About US$34,503, at a current exchange rate of US$1 to NZ$1.44917. XE CURRENCY CONVERTER, http://xe.com (last visited Nov. 13, 2017).

[31] *Id.* s 22(3).

[32] *Id.* s 21.

[33] MINISTRY OF JUSTICE, HARMFUL DIGITAL COMMUNICATIONS BILL: DEPARTMENTAL REPORT FOR THE JUSTICE AND ELECTORAL COMMITTEE 18 (Apr. 2014), https://www.parliament.nz/resource/en-NZ/50SCJE_ADV_00DBHOH_BILL12843_1_A387162/5eed063f4373109478ee70bbfdf1a96747aa2719, *archived at* https://perma.cc/3AVX-CGZ9.

No.	Principle	Sources
1	A digital communication should not disclose sensitive personal facts about an individual.	• Tort of invasion of privacy; • Information principle 11 in the Privacy Act 1993; • intimate visual recording offences in the Crimes Act 1961 (sections 216G – 216N)
2	A digital communication should not be threatening, intimidating, or menacing.	• Intimidation provisions in the Crimes Act 1961 (sections 306-308) and Summary Offences Act 1981 (section 21)
3	A digital communication should not be grossly offensive to a reasonable person in the complainant's position.	• New offence in clause 19
4	A digital communication should not be indecent or obscene.	• intimate visual recording offences in the Crimes Act 1961 (sections 216G – 216N) • sexual grooming provisions in the Crimes Act (section 131B)
5	A digital communication should not be part of a pattern of conduct that constitutes harassment.	• Harassment Act 1997
6	A digital communication should not make a false allegation.	• Tort of intentional infliction of emotional distress • Law of false attribution • Law of defamation
7	A digital communication should not contain a matter that is published in breach of confidence.	• Law of breach of confidence
8	A digital communication should not incite or encourage anyone to send a message to a person with the intention of causing harm to that person.	• Inciting or counselling a person to commit an offence in the Crimes Act 1961 (s 311) • Incitement to suicide offence in the Crimes Act (section 179)
9	A digital communication should not incite or encourage another person to commit suicide.	• Incitement to suicide offence in the Crimes Act (section 179)
10	A digital communication should not denigrate a person by reason of his or her colour, race, ethnic or national origins, religion, gender, sexual orientation, or disability.	• Human Rights Act 1993

Source: Reprinted (with design modifications) from MINISTRY OF JUSTICE, HARMFUL DIGITAL COMMUNICATIONS BILL: DEPARTMENTAL REPORT FOR THE JUSTICE AND ELECTORAL COMMITTEE 18 (Apr. 2014), https://www.parliament.nz/resource/en-NZ/50SCJE_ADV_00DBHOH_BILL12843_1_A387162/5eed063f4373109478ee70bbfdf1a96747aa2719, *archived at* https://perma.cc/3AVX-CGZ9.

The Act does not exclude existing actions in relation to online statements—for example, suing for defamation or intentional infliction of emotional distress—but rather allows affected individuals to access simpler processes in order to have the matter addressed relatively quickly.

Netsafe notes on its website that "taking a defamation case is a big undertaking in New Zealand," involving the need to engage a lawyer.[34]

III. The "Right to be Forgotten" and New Zealand Law

New Zealand's courts and legislation have not recognized a "right to be forgotten" similar to that in recent decisions of the European Court of Justice (essentially, "a right to have unwanted personal information deleted from a search engine's result listings"[35]). An assistant privacy commissioner, Joy Liddicoat, explained in 2015 that the Office of the Privacy Commissioner does not have a position on such a right and wants to hear a variety of views.[36] However, she noted that, so far, there does not appear to be "any pressing need to address this issue in New Zealand," and that

> [p]erhaps this is because New Zealand law also differs from European law in significant ways, for example there is no concept of "data controller" or "data processor" as well as other legal differences. Perhaps also, it is because while there may not be a right to be forgotten in New Zealand, there is a wide range of other mechanisms that, put together, provide a strong basis for ensuring personal information can be corrected. The Privacy Act provides a right to request correction of information and to include a statement of asserting why information is disagreed with if a correction is not made. . . .[37]

A privacy law lecturer, Steven Price, has also expressed the view that a "right to be forgotten" is not necessary in New Zealand, and that

> we already have the ability to have material removed for various privacy reasons via a variety of mechanisms – the courts can grant injunctions preventing the publication or continued publication of private facts where publication is highly offensive and there's no countervailing public interest.
>
> The Press Council, Online Media Standards Authority and Broadcasting Standards Authority can rule on complaints and the first two can order removal of material in some cases.

The Harmful Digital Communications Act will add to this when its civil regime comes into force, in particular because it contains the power to make takedown orders.[38]

---

[34] *Defamation and False Allegations*, NETSAFE (Sept. 22, 2015), https://www.netsafe.org.nz/defamation-and-false-allegations/, *archived at* https://perma.cc/Y2HT-ZGAP.

[35] James Greenland, *Privacy Week 2016 – A "Right to be Forgotten"?*, NEW ZEALAND LAW SOCIETY (May 12, 2015), https://www.lawsociety.org.nz/news-and-communications/latest-news/news/privacy-week-2016-a-right-to-be-forgotten2, *archived at* https://perma.cc/29UL-73VT.

[36] Speech, Joy Liddicoat, The Right to be Forgotten 6 (IT and Online Law Conferences, May 7, 2015 (Auckland, New Zealand) & May 8, 2015 (Wellington, New Zealand)), https://www.privacy.org.nz/assets/Files/Speeches-presentations/Right-to-be-Forgotten-Joy-Liddicoat.pdf, *archived at* https://perma.cc/VUG8-UVLA. *See also* John Edwards, *A Right to be Forgotten in New Zealand*, PRIVACY COMMISSIONER (July 1, 2014), https://www.privacy.org.nz/blog/right-to-be-forgotten/, *archived at* https://perma.cc/EF6B-8LVD.

[37] Liddicoat, *supra* note 36, at 7.

[38] Greenland, *supra* note 35.

Russia

Nerses Isajanyan
Foreign Law Consultant

SUMMARY In Russia the right to be forgotten was formally recognized in 2016. It allows an individual to request that a search engine operator remove links to information that is incorrect or outdated. In addition, civil and criminal laws protect the rights to privacy and to one's image; these rights can be used as the basis for removal from the internet of information about a person's private life.

I. Privacy Laws

The right to privacy is incorporated in articles 23 and 24 of the Russian Constitution.[1] Article 137 of the Criminal Code, entitled "Invasion of Personal Privacy," provides for a monetary fine of up to 200,000 rubles (approximately US$3,380) and up to two years of deprivation of liberty for the illegal collection or spreading of information about the private life of a person, without his/her consent, where the information concerns personal or family secrets.[2] This article has been used in Russia to prosecute revenge pornography cases.[3]

Article 152-1 of the Civil Code[4] protects the image of an individual. Publication and further use of an individual's image, including photos and video recordings, are allowed only with the consent of the citizen. Such consent is not required if the image is used in the public interest or was obtained in a public area, or the individual posed for a fee. If the individual's image is disseminated on the internet he/she can demand the removal of the image as well as a prohibition on its further distribution.[5]

---

[1] KONSTITUTSIA ROSSIISKOI FEDERATSII [CONSTITUTION OF THE RUSSIAN FEDERATION], Dec. 12, 1993, http://constitution.kremlin.ru (in Russian), *archived at* https://perma-archives.org/warc/J45J-XJE2/http://constitution.kremlin.ru, available in English on the website of the Ministry of Foreign Affairs of the Russian Federation, *at* http://archive.mid.ru//ns-osndoc.nsf/8f2968034408093843256 9ea00361529/d0bd6a5ba542c949c32575dd004009ee?OpenDocument, *archived at* https://perma-archives.org/warc/U27E-YVJ5/http://archive.mid.ru//ns-osndoc.nsf/8f2968034408093843256 9ea00361529/d0bd6a5ba542c949c32575dd004009ee?OpenDocument.

[2] UGOLOVNYI KODEKS ROSSISKOI FEDERATSII [CRIMINAL CODE OF THE RUSSIAN FEDERATION] No. 63-FZ, June 13, 1996, SOBRANIE ZAKONODATELSTVA ROSSIISKOI FEDERATSII [SZRF] June 17, 1996, No. 25, item 2954, http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891 (in Russian), *archived at* https://perma.cc/N8FX-NZJX, unofficial English translation *available at* http://www.wipo.int/edocs/lexdocs/laws/en/ru/ru080en.pdf, *archived at* https://perma.cc/43WT-78TJ.

[3] *A Resident of Volgograd Will Be Sentenced for Publishing Another's Intimate Pictures*, V1.RU (Oct. 25, 2011), http://v1.ru/text/news/448861.html (in Russian), *archived at* https://perma.cc/2S7Z-5BL7.

[4] GRAZHDANSKIY KODEKS ROSSIISKOI FEDERATSII [CIVIL CODE OF THE RUSSIAN FEDERATION], No. 51-FZ, Nov. 30, 1994, SZRF Dec. 5, 1994, No. 32, item 3301, http://pravo.gov.ru/proxy/ips/?docbody=&nd=102033239, *archived at* https://perma.cc/R6HC-TQ72, unofficial English translation *available at* http://www.wipo.int/edocs/lexdocs/laws/en/ru/ru083en.pdf, *archived at* https://perma.cc/5WY8-F7KY.

[5] *Id.* art. 152-1, para. 3.

II. Right to Be Forgotten

A. Scope of the Law

The right to be forgotten was introduced in Russia on July 1, 2016, after amendments[6] to the Law on Information, Information Technologies and Protection of Information[7] came into effect. Russia had earlier passed a law in 2015 that allowed government agencies to shut down websites that violated the requirements of the Law on Personal Data.[8] The same law required that all data on Russian citizens be stored on servers located in the territory of Russia. The 2016 law on the right to be forgotten is generally consistent with the European Union (EU) regulations on this issue. However, unlike the EU regulations, the right to be forgotten in Russia is not based on legislation on the protection of personal data.[9]

The law requires search engine operators to remove from search results information that was illegally obtained, or is inaccurate or irrelevant (outdated), at the request of the applicant. Information is deemed irrelevant if it has lost its significance to the applicant because of subsequent events or actions taken by the applicant; it must be removed irrespective of whether or not it damages the reputation of the applicant.[10] An applicant cannot request the removal of information concerning events that point to the commission of criminally punishable acts where the corresponding terms for criminal prosecution have not expired, and likewise cannot seek removal of information about the commission of a crime for which the conviction has not been canceled or expunged.[11] After the operator's intervention the challenged information will still remain on the website, but the search engine will not show links to it.[12]

The law only applies to search engine operators who link to third-party websites. Thus, the law does not apply to social media websites or other websites with internal search engines. Moreover, the law applies only to search engines that distribute advertising aimed at attracting the attention of consumers located in Russia. Search engines operated by the government and municipalities are exempt from the scope of the law.[13]

---

[6] Law No. 264-FZ of July 13, 2015, ROSSIISKAYA GAZETA [ROS. GAZ.] [RUSSIAN GAZETTE (official gazette)] No. 6725 (154) of July 26, 2015, https://rg.ru/2015/07/16/informacia-dok.html, *archived at* https://perma.cc/PRV8-GSSX.

[7] Zakon ob Informatsii, Informatsionnykh Tekhnologiyakh i o Zaschite Informatsii [Law on Information, Information Technologies] No. 149-FZ, July 27, 2006, SZRF July 31, 2006, No. 31 (Part 1), item 3448, http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264, *archived at* https://perma.cc/B5LU-Q69T.

[8] Law No. 242-FZ of July 21, 2014, ROS. GAZ. No. 163 of July 23, 2014, https://rg.ru/2014/07/23/persdannye-dok.html, *archived at* https://perma.cc/82KD-ZWRD.

[9] A.V. Krotov, *Right to Be Forgotten in Russia*, *available at* http://xn----7sbbaj7auwnffhk.xn--p1ai/article/14979 (Jan. 9, 2016) (in Russian), *archived at* https://perma.cc/K5T6-VK7Y.

[10] Tatiana Shadrina, *Now Everyone Can Remove Incorrect Information about Himself from the Web*, RG.RU (Dec. 14, 2016), https://rg.ru/2016/01/01/zabvenie-site.html (in Russian), *archived at* https://perma.cc/43WT-W7KY.

[11] Law on Information, Information Technologies art. 10-3.

[12] Shadrina, *supra* note 10.

[13] Law on Information, Information Technologies art. 2.

B. Procedures and Practice

The application to remove information must be filed in person and must contain the following information:

- The applicant's last name, first name, patronymic, passport details, and contact information (telephone and/or fax number, email address, postal address)
- Information about the links that are the subject of the termination request
- The index of the webpage on which the information is posted
- The basis for terminating the links
- The applicant's consent to the processing of his/her personal data[14]

A search engine operator may ask the applicant to provide an identity document or additional explanations if the application is incomplete or inaccurate. Within ten business days from receipt of the application or additional explanation the search engine operator must either cease issuing links to the information in question containing the name of the applicant, or send a reasoned refusal to the applicant. The operator must not disclose information about the existence of the application.

Under the Code of Civil Procedure an applicant whose request for removal is refused may file a claim in court at his/her place of residence.[15] The maximum penalty for a search engine operator's failure to comply with the law is one million rubles (approximately US$16,900).[16]

According to data provided by search engine operator Yandex, only 27% of around 3,600 applications had been granted as of March 2016. Applications were filed on the basis that the information was outdated (51%), inaccurate (30%), or irrelevant for other reasons (25%); obtained in violation of the law (19%); or concerned expunged criminal records (23%) or events containing signs of a crime where the term for criminal prosecution had expired (3%). The large percentage of refusals was explained by the lack of tools to verify the authenticity of the claims. Other search engine operators, such as Google and Mail.ru, reported similar numbers.[17]

---

[14] *Id.* art. 10-3.

[15] GRAZHDANSKIY PROTSESSUALNYI KODEKS ROSSIISKOI FEDERATSII [CIVIL PROCEDURE CODE OF THE RUSSIAN FEDERATION], No. 138-FZ, Nov. 14, 2002, SZRF Nov. 18, 2002, No. 46, item 4532, art. 402, http://pravo.gov.ru/proxy/ips/?docbody=&nd=102078828, *archived at* https://perma.cc/CY8C-QVT8.

[16] KODEKS ROSSISKOI FEDERATSII OB ADMINISTRATIVNYKH PRAVONARUSHENIAKH [CODE OF THE RUSSIAN FEDERATION ON ADMINISTRATIVE OFFENSES], No. 195-FZ, Dec. 30, 2001, art. 17.15, SZRF Jan. 7, 2002, No. 1 (pt. 1), item 1, http://pravo.gov.ru/proxy/ips/?docbody=&nd=102074277&intelsearch=%E0%E4%EC%E8%ED%E8%F1%F2%F0%E0%F2%E8%E2%ED%FB%F5+%EF%F0%E0%E2%EE%ED%E0%F0%F3%F8%E5%ED%E8%FF%F5 (in Russian), *archived at* https://perma.cc/V7MK-SJTM.

[17] *"Yandex" Rejected Two-Thirds of Requests under the Law on the "Right to Oblivion"*, RBC.RU (Mar. 25, 2016), http://www.rbc.ru/technology_and_media/25/03/2016/56f5166a9a7947a70d78f725?from=main (in Russian), *archived at* https://perma.cc/9JXK-3SP6.