Article

International Federation of Library Associations and Institutions
2018, Vol. 44(3) 183–194

DOI: 10.1177/0340035218773783
journals.sagepub.com/home/ifl

Delisting and ethics in the library: Anticipating the future of librarianship in a world that forgets

Katie Chamberlain Kritikos
University of Wisconsin-Milwaukee, USA

Abstract

Traditional librarian ethics protect privacy and promote information access. The right to be forgotten and delisting have the potential to create a new online information ecosystem that disrupts ethical norms and redefines the role of librarians. Along with Internet filtering, the right to be forgotten and delisting are the harbingers of coming changes to content regulation and information access online. Librarians should engage with right to be forgotten F and delisting issues now to prepare for possible future disruptions of information flow in the library and shifts in information policies and laws around the world. This paper articulates the legal and ethical issues associated with delisting, lays the foundation for an international dialogue on delisting, and signals the need for future research. The international librarianship community needs a larger discussion about the issues related to the right to be forgotten and delisting, particularly on laws and policies on free speech and privacy.

Keywords

Delisting, ethics, information access, librarianship, privacy, right to be forgotten

Submitted: 5 September 2017; Accepted: 31 January 2018.

Introduction

Imagine that on the Internet, personal information about you that is embarrassing, such as a mortgage foreclosure that occurred many years before, appears in Internet search results for your name (Google Spain, 2014). Or that even more sensitive and delicate personal information, such as intimate photographs taken in privacy and shared in the confidence of a relationship, now appear in the search results (Citron and Franks, 2014; Laird, 2013). Or, worse yet, that these intimate images of your body are not only online without your consent, but appear alongside other personally identifiable information (PII) like your real name, address, and phone number (Laird, 2013: 45–47). What recourse do you have to remove this personal information from very public, very accessible Internet search results?

The right to be forgotten (RTBF) offers a solution by delisting (not deleting) from search results embarrassing, outdated personal information (Google Spain, 2014), as in the first example, or "revenge pornography" (Citron and Franks, 2014: 346), as in the second. After the groundbreaking 2014 ruling of the Court of Justice of the European Union (CJEU) in *Google Spain v. Costeja*, European Union (EU) law requires that at the data subject's request, an Internet search engine "delist" personal information that is embarrassing, inflammatory, or irrelevant from the search results for her name (CJEU, 2014; Google Spain, 2014). (The CJEU, the EU's chief judicial authority that manages the uniform interpretation and application of EU law (CJEU, n.d.), should not be confused with the European Court of Human Rights (ECHR), the international court established by the European Convention on Human Rights (ECHR, n.d.). The *Google Spain v. Costeja* decision affirming the legality of the RTBF and delisting is a signal light

Corresponding author:
Katie Chamberlain Kritikos, School of Information Studies, University of Wisconsin-Milwaukee, Milwaukee, WI 53217, USA.
Email: kchambs@gmail.com.

on the coming train of change for content regulation and information access on the Internet.

Fueled by different views of privacy and free speech in the European Union and United States, the scholarly debate over the RTBF often focuses on whether delisting protects human dignity (European Commission, 2012, 2014), as in the former, or sanctions the removal or blockage of information access tantamount to censorship (Fleischer, 2011, 2015; Rosen, 2012), as in the latter. The idea that an individual has agency over search results has also sparked international treatment in the news and in the courts (Alba, 2017), from France (CNIL News, 2015) to Japan (Umeda, 2017) and from Brazil (Sganzerla, 2016) to India (Bhattacharya, 2017), to name a few. Overall, the RTBF and delisting have the potential create a new online information ecosystem, one where certain information may not be accessible (Jones, 2013, 2016). While this changing information landscape certainly implicates international law and policy, it also may create a new ethical conundrum for librarians, who are committed to information access and free speech as part of the provision of library services.

Traditional librarian ethics protect patron privacy and promote information access in the library context (Zimmer, 2013). Along with Internet filtering, the RTBF and delisting are the harbingers of continued challenges to content regulation and information access online. While much library and information science (LIS) literature addresses how Internet filtering implicates librarian ethics and information access (see, for example, US v. ALA, 2003; ALA Council, 2015; Jamali and Shahbaztabar, 2017), little research considers the effects of delisting on what Nissenbaum (2004: 137) calls the "norms of information flow" in the library. Because the RTBF and delisting have the potential to disrupt information access in the library, librarians should engage with the issues now to prepare for possible shifts in information policies and laws around the world. Potential issues for librarians to consider discussed further below include how the RTBF disrupts information flow in the library and whether helping a patron delist her personal information online falls within the context of privacy in the library, which traditionally pertains to patron records and reading behavior.

The RTBF and delisting are international issues that require an international conversation. This paper frames the legal and ethical issues associated with the RTBF and delisting and initiates a conversation about their potential future disruption of librarian ethics and the provision of library services. The following sections introduce the RTBF phenomenon, parse the differing privacy and free speech laws in the EU and US, and highlight examples of recent international RTBF cases.

The right to be forgotten phenomenon

Understanding the legal and ethical issues related to the RTBF and delisting has important implications not just for individuals, lawmakers, and search engine operators, but for librarians the world over. This section presents some general information on the RTBF phenomenon, including the CJEU's decision in *Google Spain v. Costeja* and the different reactions to the RTBF and delisting in the EU and the US.

Privacy and forgetting in the European Union

In the EU, the RTBF is based on personal privacy and agency over personal information flows (Castellano, 2012: 6; Rosen, 2012: 88). The very terminology for the RTBF comes from the French legal concept of *le droit à l'oubli*, or "right of oblivion" (Rosen, 2012: 88). Thus, being forgotten is a fundamental part of the longstanding norms of EU information law and policy. Indeed, the RTBF is in line with theories of forgetting as necessary to move forward and survive in modern society (see, for example, Augé, 2004).

1995 Data Protection Directive. At the time of the European Commission's 2012 Data Protection Regulation, discussed below, the lynchpin of existing EU legislation on personal data protection was Directive 95/46/EC3 (1995 Data Protection Directive) (European Parliament, 1995). The 1995 Data Protection Directive has two goals: (1) to uphold the fundamental right to personal data protection, and (2) to guarantee the free flow of personal data between EU member states (European Parliament, 1995: 1). Additionally, Council Framework Decision 2008/977/JHA protects personal data for the purposes of police and judicial cooperation in criminal matters (European Council, 2008). These goals attempt to balance individual privacy protection with the free flow of information.

While the 1995 Data Protection Directive provides "basic regulation of the protection of personal data" (Chelaru and Chelaru, 2013: 4), it does not provide an explicit RTBF. Some privacy law scholars, however, interpret parts of the data protection framework as a diluted version of forgetting and the RTBF (Ambrose and Ausloos, 2013: 6–7). For example, Article 12, Right of Access, covers a data subject's right to access her data and creates legal protection for personal data online (European Parliament, 1995: Article 12; Mantelero, 2013: 6). In particular, Article 12(b)

declares that each data subject has the right to "the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data" (European Parliament, 1995: Article 12(b); European Commission, 2014: p. 2).

2012 Data Protection Regulation. As the Explanatory Memorandum of the 2012 Data Protection Regulation states, "Rapid technological developments have brought new challenges for the protection of personal data" (European Commission, 2012: 1). The Internet and the social web have created a new digital world where users share their lives – and their data: "Individuals increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life" (European Commission, 2012: 1). The 2012 Data Protection Regulation thus recommends a new legal framework, proposing a regulation to protect the processing and free movement of individual personal data and a directive to protect the processing and free movement of individual personal data by legal authorities (Ambrose and Ausloos, 2013: 11; European Commission, 2012: 1).

In particular, Article 17 provides an explicit RTBF and references the "erasure" in Article 12(b) of the 1995 Data Protection Directive. Under Article 17, a data subject may request a "controller" (e.g. a search engine operator) to delist her personal information, transforming public information into private information (Jones, 2013: 371). Additionally, the controller must then inform third parties of the data subject's request to erase any links to or copies of the data, subject to certain limitations (European Commission, 2012: Article 17(a)-(d)).

Delisting removes personal information from online search results and prevents the future accessibility of that information via search engine searches. It is worth noting that *delisting* information from search results is not the same as permanently *deleting* this information from the Internet altogether (see Ash, 2016: 307; Edwards, 2017: 13). As Chelaru and Chelaru (2013: 7) note, Article 17's "remarkable novelty" comes from its placement of the burden of proof on the *controller* to show the necessity of keeping the information in search results, not on the *data subject* to show the necessity of delisting. This provision ensures that a data subject has the right to delisting; as a result, delisting has become a popular legal mechanism in the EU for protecting personal information in the name of privacy.

The RTBF case and the "man who wished to be forgotten"

Ultimately decided in 2014 by the CJEU, the seminal RTBF case to date is *Google Spain v. Costeja*. The plaintiff, a Spanish citizen, filed complaints with the Spanish data protection agency against *La Vanguardia*, a Spanish newspaper, and Google Spain and Google, Inc. when a link to the 1998 auction notice for his foreclosed home appeared in Google search results for his name (Ash, 2016: 307). Because the debt and foreclosure proceedings were resolved years ago, Costeja argued that listing the notice in search results was irrelevant and infringed his privacy rights (European Commission, 2014: 1) – even though the auction notice is part of the public record.

The issues before the CJEU were the:

- **Applicability of law**, or whether the 1995 Data Protection Directive applies to search engine operators like Google;
- **Territoriality of law**, or whether the 1995 Data Protection Directive, a European law, applies to Google Spain and Google even though the data processing server was in the United States; and
- **Right to be forgotten**, or whether individuals have the right to request the removal of links to their personal information from search engine results (European Commission, 2014: 1).

In its groundbreaking ruling in favor of the RTBF (Stupariu, 2015: 1, 37–44), the CJEU cited the two notable objectives of the 1995 Data Protection Directive: "protecting the fundamental rights and freedoms of natural persons (in particular the *right to privacy*) when personal information is processed, while removing obstacles to the *free flow of such data*" (CJEU, 2014: 1, emphasis added). In its balance of the right of personal privacy with information flow, the court ruled in favor of Costeja, holding that regarding the:

- **Applicability of law**, the 1995 Data Protection Directive applies to search engine operators (here, Google) as "controllers of personal data";
- **Territoriality of law**, the 1995 Data Protection Directive applies to search engine operators (here, Google) with subsidiaries operating in an EU member state (here, Google Spain), even though it may process data outside of Europe; and
- **Right to be forgotten**, individuals have the right, *subject to limitations*, to request the

> removal of links to their personal information from search engine results (European Commission, 2014: 1-2).

Thus, Google was required to comply with the 1995 Data Protection Directive, establishing the precedent that a search engine operator is responsible for processing personal information that appears on third-party websites and that a data subject may ask the operator to delist said information from search results for her name (CJEU, 2014: 1).

The ruling created what Peter Fleischer (2015), Global Privacy Counsel for Google, calls a "right to delist", or the right to have certain information removed from Internet search results. EU citizens may ask search engine operators to delist information that is "inaccurate, inadequate, or irrelevant or no longer relevant, or excessive" (CJEU, 2014: Para. 94; European Commission, 2014: 5). The CJEU took care to note that delisting is not an absolute right; requests are handled on a case-by-case basis, and:

> the right to get your data erased is not absolute and has clear limits . . . It only applies when personal data storage is no longer necessary or is irrelevant for the original purposes of the processing for which the data was collected. (European Commission, 2014: 4)

Thus, search engine operators handle delisting requests from EU citizens on a case-by-case basis.

As noted above, to *delist* information from search results does not permanently *delete* it from the Internet (see Ash, 2016: 307; Edwards, 2017: 13). According to the Advisory Council to Google on the Right to Be Forgotten:

> Once delisted, the information is still available at the source site, but its accessibility to the general public is reduced because search queries against the data subject's name will not return a link to the course publication . . . *only the link to the information has been removed, not the information itself*. (Floridi et al., 2015: 4, emphasis added)

The Advisory Council to Google also suggests criteria by which the search engine operator should evaluate delisting requests (e.g. the data subject's role in public life; the nature, source, and timing of the information) (Floridi et al., 2015: 7–14) and advises on implementing delisting procedures (Floridi et al., 2015: 15–20).

On its very first day of court-ordered compliance with the 1995 Data Protection Directive in 2014, Google received 12,000 delisting requests (EuropeNews.net, 2014). By the following summer of 2015, it had received over 300,000 requests and delisted 40% of the 1.1 million web addresses evaluated (Ash, 2016: 308). And as of January 2017, Google had received over 670,000 requests and delisted 43% of the 1.8 million web addresses evaluated (Edwards, 2017: 13). Ironically enough, "In trying to restore his privacy, [Costeja] made himself not merely a public figure but a historic one. He would forever be remembered as the man who wished to be forgotten" (Ash, 2016: 308). The man who wanted to protect his privacy via delisting his personal information became the very poster child for forgetting.

2015 reform of EU data protection rules

The European Commission prioritized the RTBF when it began reforming EU data protection laws in 2012 (Jones, 2013: 371). As Viviane Reding (2012), then the European Commission's Vice President, declared: "If an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system".

In December 2015, the European Parliament, Council, and Commission agreed on new data protection rules that created a "modern and harmonised data protection framework across the EU" (European Commission, 2015; Edwards, 2017). The goals to "make Europe fit for the digital age" and to generate a digital single market (European Commission, 2015) resulted in:

- **Regulation (EU) 2016/679**, which repeals the 1995 Data Protection Directive and focuses on personal data processing and the "free movement" of such personal data (European Commission, 2015). Regulation 679 was approved on May 24, 2016, and will become effective on May 25, 2018 (European Commission, 2016a; European Commission, 2015); and
- **Directive (EU) 2016/680**, which repeals Council Framework Decision 2008/977/JHA, mentioned above, and focuses on personal data processing by police and judicial cooperation in criminal matters. Directive 680 was approved on May 5, 2016, and EU member states must adopt it into their national laws by May 6, 2018 (European Commission, 2016b; European Commission, 2015).

Criticism of delisting in the United States

Because the *Google Spain v. Costeja* decision created a legal RTBF in the European Union, a new kind of content regulation in addition to, for example, Internet

filtering exists on the Internet that removes information from search engine results. Now a data subject who is an EU citizen may request that a search engine operator delist certain personal information about her from Internet search results for her name. The legal removal of content from the Internet via delisting in certain jurisdictions around the world could create a new online information ecosystem, one where some information may not be accessible (Jones, 2013, 2016). Delisting also disrupts the norms of information law and policy in the United States, including traditional conceptions of the rights to free speech and privacy.

Right to free speech in the United States

The First Amendment of the US Constitution states that "Congress shall make no law . . . abridging the freedom of speech . . . ." Critics view the RTBF and delisting as "rewriting history" at best and "censorship," or the removal or blockage of access to certain information and infringes free speech and free expression, at worst (Jones, 2013: 371).

Other scholars argue that delisting undermines the constitutional right to free speech (Rosen, 2012) and dilutes the quality of the Internet (Mayes, 2011). Due to the challenge of defining the RTBF's exact meaning, scope, and applicability (Richards, 2015: 90), some critics also contend that only personal information put online by the data subject herself qualifies for delisting (Walker, 2012).

Right to privacy in the United States

As with free speech, the RTBF and delisting can also conflict with US views of the right to privacy (Mayes, 2014). While the EU laws discussed above protect personal information, the US Constitution does not explicitly protect privacy, though many state constitutions do so (Ambrose and Ausloos, 2013: 8). Rather, privacy is an "evolving concept" in the United States (Jones, 2013: 374), and there is no "coherent, homogenous federal legal system of data and privacy protection . . . U.S. privacy protection is scattered and spread across a variety of state and federal laws that typically apply to specific groups of people" (Stupariu, 2015: 52). Consequently, many US critics of the RTBF do not view delisting as part of the right to privacy (Bennett, 2012; Bolton, 2014; Rosen, 2012). When viewed alongside US information law and policy norms, the RTBF is thus not what former European Commission Vice President Viviane Reding (2012) called a "modest expansion of existing data privacy rights", but as a "sweeping new privacy right" that is "the biggest threat to free speech on the Internet in the coming decade" (Rosen, 2012: 88).

Cross-border application of delisting

Based on the different norms of privacy and free speech in the European Union and United States, "Europeans and Americans have diametrically opposed approaches to the [RTBF] problem" (Rosen, 2012: 88). Some believe that the RTBF may exist in Europe, but not in the United States. For example, a recent report of the Advisory Council to Google on the RTBF indicated that the right should only apply within *European* jurisdictions (Floridi et al., 2015: 19–20). Limiting the RTBF to EU jurisdictions, however, does not solve the problems of delisting. The digital world, and the personal information shared, collected, and disseminated online, transcends the physical borders of countries and continents.

To truly protect privacy, information scholars urge international law- and policymakers to reach a unified understanding of the RTBF and its cross-border application and implementation (see, for example, Ausloos, 2012: 151; Bennett, 2012: 192–193; Richards, 2015: 90–92). The RTBF and delisting are international issues without borders or boundaries, appearing in the news of countries such as Canada (Alba, 2017; Blanchfield, 2016), Indonesia (Halim, 2016), and Ireland (Carolan, 2017), among others, and in the courts. The following provides a sample of countries with recent judicial decisions on the RTBF.

France

French law and policy treats privacy as a matter of dignity and human rights. As mentioned above, the RTBF terminology comes from the *droit à l'oubli*, the French legal concept of the "right of oblivion" (Rosen, 2012: 88). The Commission nationale de l'informatique et des libertés (CNIL), the regulatory body overseeing the enforcement of data privacy laws, received many delisting requests in the wake of the *Google Spain v. Costeja* decision in 2014. To manage these requests, a 2015 CNIL order requires Google to delist a data subject's personal information across *all* of its domain names (e.g. .fr, .uk, .com) (CNIL, 2015). A press release stated that, "In accordance with the CJEU judgement, the CNIL considers that in order to be effective, delisting must be carried out on all extensions of the search engine and that the service provided by Google search constitutes a single processing" (CNIL, 2015).

Outcry erupted from free speech traditionalists, among them Peter Fleischer, Global Privacy Council for Google, who argues for a European but not a

global RTBF: "We believe that no one country should have the authority to control what content someone in a second country can access" (Fleischer, 2015). The case between the CNIL and Google is currently pending before the European Court of Justice, one of the three courts that comprises the CJEU, as Case C-507/17 (ECJ, n.d.; Hern, 2017). The implications of a high court order limiting the RTBF to EU jurisdictions remain to be seen.

Japan

In contrast with the EU view of privacy in *Google Spain v. Costeja* and the French CNIL order, Japan's Supreme Court rejected a data subject's request that Google delist the search results for his 2011 arrest for child prostitution and pornography (Heisei, 2017; Umeda, 2017). Though the lower court had recognized the data subject's rights to privacy and to be forgotten, and ordered Google to delist these search results (Kyodo, 2016), the Tokyo High Court reversed the ruling and the Supreme Court affirmed it on the basis that the RTBF was not yet a ripe (i.e. timely) issue to adjudicate alongside the right of personal privacy (Umeda, 2017).

Brazil

Like the high court in Japan, Brazil's Superior Court of Justice (STJ) ruled unanimously against the imposition of the RTBF on Google and other search engine operators due to concerns over search engine authority, censorship, and information access (Sganzerla, 2016; STJ, 2016). According to a report on the ruling, "forcing search engines to adjudicate removal requests and remove certain links from search results would give too much responsibility to search engines, effectively making them into *digital censors*" (Sganzerla, 2016, emphasis added). An appeal is pending in Brazil's Supreme Court (Sganzerla, 2016).

India

Unlike the courts in Japan and Brazil, the Karnataka High Court in India approved and applied the RTBF to the case of a young woman seeking to delist search results for a prior marriage annulment to protect her privacy and reputation (Bhattacharya, 2017). Seeking harmony with western privacy law and acknowledging the need for sensitivity to women, the Court found that its ruling is: "in line with the trend in Western countries of 'right to be forgotten' in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned" (Bhattacharya, 2017). That the Karnataka High Court looked to the West for guidance on how to interpret the RTBF and privacy indicates a possible growing global consensus to prioritize the protection of privacy over the provision of information access.

Delisting disrupts the norms of information flow and librarian ethics

The interplay between information access and delisting disrupts not just international law and policy, but librarian ethics as well. Traditionally, libraries are the cornerstone of intellectual freedom and information access (ALA Council, 1996, 2008, 2014; IFLA, 1999) and librarians have a professional imperative to protect patrons' rights to privacy and to receive information in the library (Givens, 2014). The RTBF and delisting, however, alter the norms of information flow in libraries and create the potential for a new online information ecosystem, one where some information may not always be accessible (Jones, 2013, 2016).

Before considering some of the unintended consequences of delisting for patron privacy and information access in the library, the next section provides a brief overview of librarian ethics. Due to considerations of space, it focuses on the ethical standards of the American Library Association (ALA) and International Federation of Library Associations (IFLA).

US approaches to privacy and ethics in the library

While librarians typically must balance ethical principles with legal obligations, a potentially disruptive new legal regime like the RTBF and delisting could disrupt the ethical foundations of librarianship. To address privacy issues in US libraries, a set of "librarian ethics" that exist alongside librarians' legal obligations emerged from documents and ethical frameworks that the ALA has refined and codified over time (Magi and Garnar, 2015). This section first introduces the concept of contextual integrity before highlighting some of the ALA's official statements on privacy and ethics.

Contextual integrity and information flow in the library. As guardians of privacy and free speech, librarians preserve what Nissenbaum (2004,2009) calls contextual integrity of patron privacy while providing information access. "Contextual integrity" refers to the sharing of personal information in different spaces, or *contexts*, that have their own norms and expectations, from the home to the workplace to the library: "Each of these spheres, realms, or contexts involves, indeed may even be defined by, a distinct set of norms, which

governs its various aspects such as roles, expectations, actions, and practices" (Nissenbaum, 2004: 137). According to Zimmer (2013: 45), "the context of the library brings with it specific norms of information flow that protect patron privacy". Librarians traditionally manage information flows in the library context by providing information access and by protecting patron privacy (for example, patron reader records are private and patron PII is confidential). Based on this understanding of privacy in the library, librarians must safeguard patron information in library records, but are not responsible for privacy outside of the library context.

Code of Ethics. Initially adopted in 1939, the ALA's *Code of Ethics* establishes general policies to guide ethical decision making in libraries, focused on the principle that, "We have a special obligation to ensure the free flow of information and ideas to present and future generations" (ALA Council, 2008). Indeed, "ensuring free and unfettered information access is a cornerstone of the librarian profession and the ALA's Code of Ethics. Librarians have a rich history of protecting patron privacy . . . " (Zimmer, 2013: 51). Considering the RTBF and delisting under this ethical framework, how can librarians "ensure the free flow of information and ideas" while respecting patrons who no longer want certain personal information to be searchable online?

Library Bill of Rights. The ALA also adopted the *Library Bill of Rights* in 1939, creating a formal policy statement on intellectual freedom that entitles everyone to free thought and expression and to the free access of library materials (ALA Council, 1996; Magi and Garnar, 2015). In particular, Article III states that, "Libraries should challenge censorship in the fulfillment of their responsibility to provide information and enlightenment" and Article IV states that, "Libraries should cooperate with all persons and groups concerned with resisting abridgment of free expression and free access to ideas" (ALA Council, 1996: Articles III and IV). The RTBF creates a problem for librarian ethics: Is delisting censorship (the removal or blockage of access) of information? Does it prevent librarians from "resisting abridgment of free expression and free access to ideas"?

2014 Interpretation of the Library Bill of Rights. Despite the ALA's longstanding commitment to librarian ethics, patron privacy is perennially challenged, such as through government attempts to gain access to patron records via the USA PATRIOT Act (Foerstel, 2004). More recently, the ALA issued *Privacy: An Interpretation of the Library Bill of Rights*, which notably affirms that, "Everyone . . . who provides governance, administration or service in libraries has a responsibility to maintain an environment respectful and protective of the privacy of all users" (ALA Council, 2014). In a world that delists, how do librarians protect privacy? Are they responsible just for patron information in library records, or for any personal information pertaining to that individual?

ALA statement on the RTBF. At the time of this writing, the ALA has not issued a formal statement on the RBTF (Freeman, 2016). The issue, however, has been discussed and debated at formal ALA meetings (see, for example, Carlton, 2016).

IFLA approaches to privacy and ethics in the library

IFLA also promotes librarian ethics through a set of documents and frameworks that address privacy and information access (IFLA, 1999, 2015, 2016b).

1999 Statement on Libraries and Intellectual Freedom. Prepared by the Freedom of Access to Information and Freedom of Expression (FAIFE) Committee and approved by IFLA's Executive Board in 1999, the *Statement on Libraries and Intellectual Freedom* (1999 Statement) states that IFLA "defends and promotes intellectual freedom as defined in the United Nations Universal Declaration of Human Rights" and "asserts that a commitment to intellectual freedom is a core responsibility for the library and information profession" (IFLA, 1999). IFLA finds that privacy is an essential component of intellectual freedom. As such, libraries and library staff must ethically "adhere to the principles of intellectual freedom, uninhibited information access and freedom of expression and to recognize the privacy of library use" (IFLA, 1999). But the RTBF creates a conundrum for the "uninhibited information access and freedom of expression" and "privacy of library use": Is delisting the censorship of information?

The 1999 Statement's list of 11 intellectual freedom principles includes the affirmation that, "Library users shall have the right to personal privacy and anonymity. Librarians and other library staff shall not disclose the identity of users or the materials they use to a third party" (IFLA, 1999). But in a world that delists, how do librarians protect privacy? Based on the 1999 Statement, it seems that librarians are ethically required to protect only a patron's privacy in the library as it pertains to her identity or materials used.

2015 Statement on Privacy in the Library. Prepared by the FAIFE Committee and approved by the Governing Board, IFLA's recent *Statement on Privacy in the Library* (2015 Statement) notes that Article 12 of the United Nations' *Universal Declaration of Human Rights* defines privacy as human right: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation" (ILFA, 2015: 1, quoting *Universal Declaration on Human Rights*). It also cites IFLA's *Code of Ethics*, which "identifies respect for personal privacy, protection of personal data, and confidentiality in the relationship between the user and library or information service as core principles" (IFLA, 2015: 1, quoting *IFLA Code of Ethics for Librarians and Other Information Workers*).

Considering the human rights element of personal privacy and the ethical obligation of librarians to protect patrons' privacy again raises the challenge of delisting. The norms of information flow in the library context protect privacy from unwanted infringement by third parties, which librarians can achieve by "decid[ing] what kind of personal data they will collect on users and consider[ing] principles of data security, management, storage, sharing and retention" (IFLA, 2015: 2). But the 2015 Statement also recommends that: "Data protection and privacy protection should be included as a part of the media and information literacy training for library and information service users. This should include training on *tools to use to protect their privacy*" (IFLA, 2015: 2, emphasis added).

The call for better information literacy training for library patrons seems to extend beyond traditional library protection of reader records and PII to "tools to protect their privacy." Does this training include using Google's delisting request tool, or just internal library tools? Does helping a patron access and complete a delisting request amount to sanctioning censorship that violates librarian ethics?

2016 Statement on the Right to Be Forgotten. Like the Statement on Privacy in the Library, IFLA's Statement on the Right to be Forgotten (2016 Statement) also cites the United Nation's Universal Declaration of Human Rights and IFLA's Code of Ethics in its discussion of concerns related to delisting, which include:

- **Integrity of and access to the historical record**. IFLA dedicates itself to protecting information access, including the preservation of the historical record. Notably, IFLA "sees information on the public Internet as published information that may have value for the public or for professional researchers and so should, in general, not be intentionally hidden, removed or destroyed" (IFLA, 2016b);
- **Free information access and free expression**. IFLA also dedicates itself to protecting the freedoms of expression and information access. The RTBF and delisting violate these ideals; for example, "[t]he ideal of freedom of access to information cannot be honoured where information is removed from availability or is destroyed . . . When links to information are removed, for many, this results in a loss of access to information" (IFLA, 2016b); and
- **Privacy of the individual**. IFLA dedicates itself to protecting personal privacy in libraries, which, "as upholders of the public good, are sensitive to concerns around personal privacy in the context of the Internet" (IFLA, 2016b). Regarding the RTBF and delisting, "The degree to which libraries and librarians will find a particular application of RTBF to be acceptable, in the context of the more general library concern for access to information, will depend upon the particular circumstances of the application" (IFLA, 2016b).

The 2016 Statement concludes by exhorting librarians to participate in policy discussions about the RTBF and a list of professional imperatives that preserve information access, such as opposing removal of links from the results of name searches of public figures and advocating transparent criteria and processes for search engines' RTBF determinations. But the list also suggests that librarians should: "Support individuals who request assistance in finding more information on the application of the right to be forgotten to their individual circumstances," indicating that at least under IFLA's interpretation of ethical norms and information flows in the library, librarians should educate patrons about the RTBF and delisting.

2013 and 2016 Trend Reports. In addition to the official statements described above, the IFLA Trend Report included the redefinition of the boundaries of data protection and privacy as one of five major factors that will influence the future of the international information ecosystem (IFLA, 2013). The 2016 update revisited the paramount importance of privacy, data protection, and information security (IFLA, 2016a). The update also specifically mentions the RTBF, noting that "unanticipated side effects of our online activities [leave] behind a permanently visible digital footprint" (IFLA, 2016a: 7).

Delisting considerations for librarians

As described above, librarians traditionally protect and defend patron privacy in the library context, but delisting may change the norms of information flows and privacy in the library. The RTBF's disruption of contextual integrity in the library may require a redefinition or expansion of patron privacy protection.

Though yet to receive extensive treatment in the LIS literature, the RTBF has not gone unnoticed by the domain's professional organizations, such as the ALA and IFLA, or its scholars. For example, Edwards (2017: 14) identifies the RTBF as a possible "conflict in the making" for the professional imperatives of librarianship like information access and preserving the historical record, echoing the ALA and IFLA statements discussed above. Because the RTBF and delisting can alter the norms of information flow and librarian ethics in the future, the following lists possible issues that librarians around the world should consider now in preparation.

- **Information flows**. How does the RTBF disrupt information flow in the library? Delisting revokes access to certain information in search engine results, implicating the rights to read and to receive information in libraries. But delisting also can protect the privacy of the data subject, which can include sensitive PII. Recall that delisting is not the same as permanently deleting information from the Internet.
- **Personal information**. Does it matter whether the personal information that the patron wants to delist is public and factual, such as the mortgage foreclosure in *Google Spain v. Costeja*, or is sensitive and embarrassing, such as revenge pornography? What if the patron seeks to delist PII?
- **Intellectual freedom**. Does helping a patron delist information online protect that patron's privacy and maintain confidentiality, or does it undermine free speech and unfettered information access?
- **Patron privacy**. Does helping a patron delist her personal information online fall within the context of privacy in the library, which traditionally pertains to patron records and reading behavior?
- **Delisting requests**. Delisting can alter the norms of information flow in the context of the library by removing certain information online from availability and accessibility. What if patron asks a librarian for help with a delisting request? Can the librarian refuse to help a patron locate a delisting request form or to fill it in? Or is the librarian now obliged to help protect this patron's privacy? Based on IFLA's *Statement on the Right to be Forgotten* (IFLA, 2016b), it appears that librarians are ethically bound to educate patrons about the RTBF tools available to them.

Conclusion and future research

The relationship between privacy, free speech, and delisting is critical for the future of librarianship worldwide. This paper anticipates the RTBF and delisting's potential disruption of librarianship and seeks to initiate an international dialogue between librarians, scholars, and advocacy groups. Delisting, while legally applicable only in EU jurisdictions at the time of this writing, nevertheless implicates privacy and information access in libraries around the world. It might also create a new role for librarians, who must educate themselves and patrons about the RTBF and delisting and may create and implement new polices that reflect the evolving online information ecosystem.

Going forward, librarians should engage with RTBF and delisting issues now to prepare for possible future disruptions of information flow in the library and shifts in information policies and laws around the world. Some of the considerations for librarianship are the possible effects of delisting on patron privacy and free speech in the library and the possible new responsibilities of the librarian in a new online information environment. Future research is needed on the potential of delisting and the RTBF to disrupt librarian ethics and the provision of library services. Possible projects include cross-cultural studies of librarianship norms and practices around the world and formulation to formulate best practices to guide the management of delisting in the library.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Alba D (2017) The world may be headed for a fragmented 'splinternet'. *Wired*, 7 July. Available at: https://www.wired.com/story/splinternet-global-court-rulings-google-facebook/ (accessed 2 February 2018).

ALA (American Library Association) Council (1996) Library Bill of Rights. ALA.org. Available at: http://www.ala.org/advocacy/intfreedom/librarybill (accessed 2 February 2018).

ALA (American Library Association) Council (2008) Code of Ethics. ALA.org. Available at: http://www.ala.org/tools/ethics (accessed 2 February 2018).

ALA (American Library Association) Council (2014) Privacy: An Interpretation of the Library Bill of Rights. ALA.org. Available at: http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy (accessed 2 February 2018).

ALA (American Library Association) Council (2015) Privacy: An Interpretation of the Library Bill of Rights. ALA.org. Available at: http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/internet-filtering (accessed 2 February 2018).

Ambrose M L and Ausloos J (2013) The right to be forgotten across the Pond. *Journal of Information Policy* 3: 1–23.

Ash T G (2016) *Free Speech: Ten Principles for a Connected World*. New Haven, CT: Yale University Press.

Augé M (2004) *Oblivion*. Trans. de Jager. M. Minneapolis, MN: University of Minnesota Press.

Ausloos J (2012) The 'right to be forgotten' – worth remembering? *Computer Law & Security Review* 28(2): 143–152.

Bennett SC (2012) Right to be forgotten: Reconciling EU and US perspectives. *Berkeley Journal of International Law* 30(1): 161–195.

Bhattacharya A (2017) In a first, an Indian court upholds the 'right to be forgotten'. *Livelaw*. Available at: http://www.livelaw.in/first-indian-court-upholds-right-forgotten-read-order/ (accessed 2 February 2018).

Blanchfield M (2016) Google, B.C. firm duel over free speech, copyright in Supreme Court battle. *Toronto Star*, 6 December. Available at: https://www.thestar.com/business/2016/12/06/google-bc-firm-duel-over-free-speech-copyright-in-supreme-court-battle.html (accessed 2 February 2018).

Bolton R (2014) The right to be forgotten: Forced amnesia in a technological age. *John Marshall Journal of Information Technology and Privacy Law* 31(2): 133–144.

Carolan M (2017) Google argues 'right to be forgotten' ruling is unworkable. *Irish Times*, 18 May. Available at: https://www.irishtimes.com/news/crime-and-law/courts/high-court/google-argues-right-to-be-forgotten-ruling-is-unworkable-1.3088145?mode=amp&ref=yfp (accessed 2 February 2018).

Carlton A (2016) Should there be a right to be forgotten? Librarians debate EU privacy laws at Midwinter. *American Libraries Magazine*. Available at: https://americanlibrariesmagazine.org/blogs/the-scoop/should-there-be-a-right-to-be-forgotten/ (accessed 2 February 2018).

Castellano PS (2012) The right to be forgotten under European law: A constitutional debate. *Lex Electronica* 16(1): 1–30.

Chelaru E and Chelaru M (2013) Right to be forgotten. *Annales Universitatis Apulensis – Series Juriprudentia* 16: 1–8.

Citron D and Franks M A (2014) Criminalizing revenge porn. *Wake Forest Law Review* 49(2): 345–392.

CNIL (Commission Nationale de l'informatique et des libertés) (2015) CNIL orders Google to apply delisting on all domain names of the search engine. *CNIL News*, 12 June. Available at: http://www.cnil.fr/english/news-and-events/news/article/cnil-orders-google-to-apply-delisting-on-all-domain-names-of-the-search-engine/ (accessed 2 February 2018).

CJEU (Court of Justice of the European Union) (2014) Press Release No. 70/14, Judgment in Case C-131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González* (Luxembourg). *Curia*. Available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf (accessed 2 February 2018).

CJEU (Court of Justice of the European Union) (n.d.) General presentation. *Curia*. Available at: https://curia.europa.eu/jcms/jcms/Jo2_6999/ (accessed 2 February 2018).

Edwards E (2017) Libraries and the right to be forgotten: A conflict in the making? *Journal of Intellectual Freedom and Privacy* 2(1): 13–14.

European Commission (2012) 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. *European Parliament*. Available at: http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_EN.pdf (accessed 2 February 2018).

European Commission (2014) Fact sheet on the 'right to be forgotten' ruling (C 131/12). *Europa.eu*. Available at: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (accessed 2 February 2018).

European Commission (2015) Press release: Agreement on Commission's EU data protection reform will boost Digital Single Market. *Europa.eu*, 15 December. Available at: http://europa.eu/rapid/press-release_IP-15-6321_en.htm (accessed 2 February 2018).

European Commission (2016a) Regulation of the European Parliament and of the Council of 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). Regulation (EU) 2016/679. *EurLex*. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC (accessed 2 February 2018).

European Commission (2016b) Directive of the European Parliament and of the Council of on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the

prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. Directive (EU) 2016/680. *EurLex*. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC (accessed 2 February 2018).

European Council (2008) Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. *Official Journal of the European Union*. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008F0977 (accessed 2 February 2018).

ECHR (European Court of Human Rights) (n.d.) The court in brief. *European Court of Human Rights*. Available at: http://www.echr.coe.int/Documents/Court_in_brief_ENG.pdf (accessed 2 February 2018).

ECJ (European Court of Justice) (n.d.) *Google*, Case C-507/17. *Curia*. Available at http://curia.europa.eu/juris/liste.jsf?language=en&num=C-507/17 (accessed 2 February 2018).

European Parliament (1995) Directive 95/46/EC 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. *EurLex*. Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 (accessed 2 February 2018).

EuropeNews.net (2014) Removal of Google personal information could become work intensive. *EuropeNews.net*, 1 June. Available at: http://www.europenews.net/index.php/sid/222490797 (accessed 2 February 2018).

Fleischer P (2011) Foggy thinking about the right to oblivion. In: *Privacy . . . ?* Available at: http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html (accessed 2 February 2018).

Fleischer P (2015) Implementing a European, not global, right to be forgotten. In: *Google Europe Blog*. Available at:http://googlepolicyeurope .blogspot.com/2015/07/implementing-european-not-global-right.html (accessed 2 February 2018).

Floridi L et al. (2015) The advisory council to Google on the right to be forgotten. Google Advisory Council, 6 February. Available at: http://www.cil.cnrs.fr/CIL/IMG/pdf/droit_oubli_google.pdf (accessed 2 February 2018).

Foerstel H (2004) *Refuge of a Scoundrel: The Patriot Act in Libraries*. Westport, CT: Libraries Unlimited.

Freeman M (2016) Google embraces version of right to be forgotten. In: Intellectual Freedom Blog, 18 March. Available at: http://www.oif.ala.org/oif/?p=6258 (accessed 2 February 2018).

Givens C (2014) *Information Privacy Fundamentals for Librarians and Information Professionals*. New York: Rowman and Littlefield.

Google Spain [*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Case C 131/12] (2014, 13 May) (Spain). Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doc&mode=lst&dir=&occ=first&part=1&cid=133613 (accessed 2 February 2018).

Halim H (2016) Press exempt from right to be forgotten. *The Jakarta Post*, 6 December. Available at: http://www.thejakartapost.com/news/2016/12/06/press-exempt-right-be-forgotten.html (accessed 2 February 2018).

Heisei 28 (Kyo) 45 (2017) *Courts in Japan*. Available at: http://www.courts.go.jp/app/hanrei_jp/detail2?id=86482 (accessed 2 February 2018).

Hern A (2017) ECJ to rule on whether 'right to be forgotten' can stretch beyond EU. *The Guardian*, 20 July. Available at: https://www.theguardian.com/technology/2017/jul/20/ecj-ruling-google-right-to-be-forgotten-beyond-eu-france-data-removed (accessed 2 February 2018).

IFLA (International Federation of Library Associations) (1999) Statement on libraries and intellectual freedom. IFLA.org. Available at: https://www.ifla.org/publications/ifla-statement-on-libraries-and-intellectual-freedom (accessed 2 February 2018).

IFLA (International Federation of Library Associations) (2013) IFLA trend report. IFLA.org. Available at: http://trends.ifla.org/http:// (accessed 2 February 2018).

IFLA (International Federation of Library Associations) (2015) Statement on privacy in the library environment. IFLA.org. Available at: https://www.ifla.org/files/assets/hq/news/documents/ifla-statement-on-privacy-in-the-library-environment.pdf (accessed 2 February 2018).

IFLA (International Federation of Library Associations) (2016a) IFLA trend report 2016 update. IFLA.org. Available at: https://trends.ifla.org/files/trends/assets/trend-report-2016-update.pdf (accessed 2 February 2018).

IFLA (International Federation of Library Associations) (2016b) Statement on the right to be forgotten. IFLA.org. Available at: https://www.ifla.org/node/10272 (accessed 2 February 2018).

Jamali HR and Shahbaztabar P (2017) The effects of Internet filtering on users' information-seeking behaviour and emotions. *Aslib Journal of Information Management* 69(4): 408–425.

Jones ML (2013) It's about time: Privacy, information life cycles, and the right to be forgotten. *Stanford Technology Law Review* 16(2): 369–422.

Jones ML (2016) *Ctrl + Z: The Right to Be Forgotten*. New York: NYU Press.

Koops B-J (2011) Forgetting footprints, shunning shadows: A critical analysis of the 'right to be forgotten' in big data practice. *SCRIPTed* 8(3): 229–256.

Kyodo (2016) Japanese court recognizes 'right to be forgotten' in suit against Google. *Japan Times*, 27 February. Available at: http://www.japantimes.co.jp/news/2016/02/27/national/crime-legal/japanese-court-recog

nizes-right-to-be-forgotten-in-suit-against-google/#.WOVE99IrI2w (accessed 2 February 2018).

Laird L (2013) Victims are taking on websites for posting photos they didn't consent to. *ABA Journal* 99: 44–50.

Magi T and Garnar M (eds) (2015) *Intellectual Freedom Manual*. 9th edn. Chicago, IL: American Library Association.

Mantelero A (2013) The EU proposal for a general data protection regulation and the roots of the 'right to be forgotten'. *Computer Law and Security Review* 29(3): 229–235.

Mayes T (2011) We have no right to be forgotten online. *The Guardian*, 21 May. Available at: https://www.theguardian.com/commentisfree/libertycentral/2011/mar/18/forgotten-online-european-union-law-internet (accessed 2 February 2018).

Nissenbaum H (2004) Privacy as contextual integrity. *Washington Law Review* 79(1): 119–157. Available at: https://www.nyu.edu/projects/nissenbaum/papers/washingtonlawreview.pdf (accessed 2 February 2018).

Nissenbaum H (2009) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Reding V (2012) EU data protection reform 2012: Making Europe the standard setter for modern data protection rules in the digital age. Speech given at: *Innovation conference digital, life, design*, Munich, Germany, 22 January. Available at: http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm (accessed 2 February 2018).

Richards N (2015) *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. New York: Oxford University Press.

Rosen J (2012) The right to be forgotten. *Stanford Law Journal Online* 64(1): 88–92.

Sganzerla T (2017) Brazil superior court rules in Google's favor, against 'right to be forgotten'. *Global Voices*, 21 November. Available at: https://globalvoices.org/2016/11/21/brazil-superior-court-rules-in-googles-favor-against-right-to-be-forgotten/ (accessed 2 February 2018).

STJ (Brazil Superior Court of Justice) (2016) Request for right to forget cannot be directed to Google. *Migalhas*, 16 November. Available at: http://www.migalhas.com.br/Quentes/17, MI248798,51045-Pedido+de+direito+ao+esquecimento+nao+pode+ser+direcionado+ao+Google (accessed 2 February 2018).

Stupariu I (2015) *Defining the right to be forgotten: A comparative analysis between the EU and the US*. LLM Short Thesis, Central European University, Hungary. Available at: http://www.etd.ceu.hu/2015/stupariu_ioana.pdf (accessed 2 February 2018).

Tene O and Polonetsky J (2013) Big data for all: Privacy and user control in the age of analytics. *Northwestern Journal of Technology and Intellectual Property* 11(5): 242–273.

Umeda S (2017) Japan: Google does not have to delete search results related to arrest. *Library of Congress Global Legal Monitor*. Available at: http://www.loc.gov/law/foreign-news/article/japan-google-does-not-have-to-delete-search-results-related-to-arrest/?loclr=eaglm (accessed 2 February 2018).

United States v. American Library Association, Inc., 539 US 194 (2003) Available at: http://caselaw.findlaw.com/us-supreme-court/539/194.html (accessed 2 February 2018).

Walker RK (2012) The right to be forgotten. *Hastings Law Journal* 64(1): 257–286.

Zimmer M (2013) Patron privacy in the '2.0' era: Avoiding the Faustian bargain of library 2.0. *Journal of Information Ethics* 22(1): 44–59.

Author biography

Katie Chamberlain Kritikos is a doctoral candidate at the School of Information Studies and research assistant at the Center for Information Policy Research at the University of Wisconsin-Milwaukee. She researches issues related to information law and policy including privacy, technology, and digital civil rights. Katie received her B.A. (2006) in English from the University of Alabama and J.D. (2009) and M.L.I.S. (2010) from the University of Illinois.