NOT FORGETTING JUST OBSCURING: AMERICAN AND EUROPEAN ATTEMPTS TO MAINTAIN PRIVACY IN THE DIGITAL AGE

By: John Corrado

TABLE OF CONTENTS

INTRODUCTION

The internet, an interconnected network of information systems, characterizes and defines the modern world. The "internet of things"[1] is constantly growing with new sources of information being added regularly.[2] Any person who has access to the internet can draw upon vast sums of knowledge about any number of subjects or people at a moment's notice.[3]

Many hail the internet as a positive force in the world because it gives individuals access to information needed to make well-informed decisions. The internet allows the masses to make their voices heard in extremely visible ways through social media networks. People are more connected and visible now than they have ever been. The internet allows for speed and efficiency in a great number of processes, from mundane shopping to important governmental functions. However, the internet has also led to a great collection, retention, and cataloging of personal information that poses a serious threat to personal privacy.[4]

Privacy has been identified as a fundamental human right, a way to protect an individuals' autonomy.[5] Attempts to produce a single definition of privacy have met with a great amount of scrutiny and uncertainty, as with many fundamental rights.[6] In the context of data systems, the most relevant iterations of privacy are (a) the right to be let

---

1 "The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction." Internet of Things, IoT Agenda, http://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT (last visited Jan. 9, 2017).

2 John Greenough, *How the 'Internet of Things' will impact consumers, businesses, and governments in 2016 and beyond*, BUSINESS INSIDER (Jul. 18, 2016), http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10; Jacob Morgan, *A Simple Explanation of the Internet of Things*, FORBES (May 13, 2014), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#626c4b556828.

3 Urs Hoelzel, *The Google Gospel of Speed*, GOOGLE (January 2012), https://www.thinkwithgoogle.com/articles/the-google-gospel-of-speed-urs-hoelzle.html (The average Google search speed is a tenth of a second.).

4 *See generally* Woodrow Hartzog, & Frederic Stuzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 387 (2013); Evan Selinger & Woodrow Hartzog, *Why you have the right to obscurity*, CSMONITOR (Apr. 5, 2015), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0415/Why-you-have-the-right-to-obscurity?cmpid=TW; Edith Ramirez, *Opening Remarks of FTC Chairwoman Edith Ramirez Privacy and the IoT: Navigating Policy Issues International Consumer Electronics Show Las Vegas, Nevada, Jan. 6, 2015*, https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf.

5 Alexandra Rengel, *Privacy as an International Human Right and the Right to Obscurity in Cyberspace,* 2 GRONINGEN J. INT. L. 33, 37 (2014).

6 Trina J. Magi, *Fourteen Reasons Why Privacy Matters*, 81 THE LIBR. Q.: INFO., COMMUNITY, POL'Y 187, 187-90 (2011).

alone, (b) the ability to control information about oneself, and (c) the protection of one's individuality or dignity.[7]

Modern governments have attempted to address the threat that cataloguing and centralizing information poses to privacy in various ways. This Note limits itself to how the United States and the European Union have attempted to address the threat that information systems pose to privacy. The United States had early run-ins with centralized information systems and consequently passed the Privacy Act of 1974, which regulates the behavior of federal agencies.[8] Despite the early start and recognition that easily accessible information could pose a threat to privacy rights, the American government has no overarching privacy law.[9] The European Union, on the other hand, has attempted to regulate information systems, including the internet, through its Data Protection Directive of 1995.[10]

In 2014, the Court of Justice of the European Union (CJEU), while interpreting the Data Protection Directive, declared the "right to be forgotten" in the E.U.[11] The "right to be forgotten" allows individuals to request the delisting of search results associated with their name from search engines.[12] Those data processors must then engage in an examination of the request and either remove the data or refuse the removal and offer an explanation.[13]

The CJEU ruling on the "right to be forgotten" has been controversial in many regards. Some people criticize the right to create memory holes, promoting censorship and lessening the quality of the internet by removing relevant data.[14] Numerous people have voiced strong concern about the clash between free speech and the "right to be

---

7 *Id*. at 189.

8 The Privacy Act of 1974, 5 U.S.C. §552a (1974).

9 Interestingly there is debate within the legislative history about just how far the Privacy Act should extend. A major concern of some legislators was the government's targeting of anti-war activists. The legislators feared that computers would make it too easy for the government to centralize and abuse information. There was foreshadowing of the issues we are currently facing, but Congress was unwilling to press the issue. HOUSE COMM. ON GOV'T OPERATIONS AND SENATE COMM. ON GOV'T OPERATIONS, 94TH CONG., 2D SESS., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974 – S. 3418 (PUB. L. NO. 93-579) SOURCE BOOK ON PRIVACY (1976) [hereinafter LEGISLATIVE HISTORY OF THE PRIVACY ACT].

10 Directive 95/46/EC of the European Parliament and Council of Oct. 24, 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive].

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

12 Data Protection Directive, *supra* note 10 at art. 12(b).

13 *Google Spain*, 2014 E.C.R. 317.

14 *Wikipedia warns that EU legislation will create 'Orwellian memory holes' in the internet,* INDEPENDENT; McKay Cunningham*, Free Expression, Privacy, and Diminishing Sovereignty in the Information Age: The Internationalization of Censorship*, 69 ARK. L.R. 71, 96 (2016); Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow,* 28 HARV. J. L. & TECH. 349 (2015).

forgotten", especially in the American context.[15] Some have hailed the decision a noble attempt to address growing privacy concerns with the continuing growth of the internet.[16] Others still have asserted that "the right to be forgotten" as it exists is really a right to obscurity, a position this Note concurs with.[17]

In Part I, this Note will define the right to obscurity and differentiate it from a "right to be forgotten." Then in Part II, this Note will examine the E.U. law and assert that as it stands the law actually establishes a right to obscurity. Part II will also assert that data holders are the pragmatic choice for initial removal requests. In Part III, this Note will examine how a narrow right to obscurity exists in the American context by looking at various statutes and examining how they promote obscurity. In Part IV, this Note will argue that a broader right to obscurity is compatible with United States law and is essential to the very rights it may at times conflict with.

I. THE RIGHT TO OBSCURITY VS. THE RIGHT TO BE FORGOTTEN

A. Defining a Right To Obscurity

In everyday conversation, obscure usually refers to a person who is not well known or who has a humble background.[18] People commonly say that public figures retire and fade into a life of obscurity, a shift from public and known to private and unknown. Less commonly, a person might say that a concept is obscure because it is not easily understood.[19] This focus on being unknown or not easily understood is at the heart of the right to obscurity.

A string of recent scholarship has focused on obscurity as a right.[20]

---

15 Robert Lee Bolton, *The Right to Be Forgotten Forced Amnesia in a Technological Age*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 132 (2014); Jeffrey Abramson, *Searching for Reputation: Reconciling Free Speech and the "Right To be Forgotten*", 17 N.C. J. L. & TECH. 1, 72 (2015); Robert Kirk Walker, Note, *The Right to be Forgotten*, 64 HASTINGS L.J. 257 (2012-2013); Rustad & Kulevska, *supra* note 14.

16 Mark Randazza, *We Need a Right to Be Forgotten*, CNN (May 15, 2014); Chelsea E. Carbone, *To Be Or Not To Be Forgotten: Balancing the Right to Know With The Right to Privacy in the Digital Age*, 22 VA. J. SOC. POL'Y & L. 525, 550 (2015); Abramson, *supra* note 15.

17 David Hoffman et. al., *The Right to Obscurity: How we can implement the Google Spain Decision*, 17 N.C. J. & TECH. 437 (2016); Woodrow Hartzog & Evan Selinger, *Surveillance as Loss of Obscurity*, 72 WASH. & LEE L. REV. 1343, 1359 (2015); Woodrow Hartzog & Evan Selinger, *Obscurity: A Better Way to Think About Your Data Than 'Privacy'*, THE ATLANTIC (Jan. 17 2013), http://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-thanprivacy/267283/ (last visited Oct. 12, 2016).

18 Woodrow Hartzog & Evan Selinger, *Obscurity and Privacy*, Routledge Companion to Philosophy and Technology (2014), at 2; *Obscure*, OXFORD ENGLISH DICTIONARY.

19 *Obscure*, *supra* note 18.

20 Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CAL. L. REV.

Obscurity has been defined as "reflecting of a state of unknowing."[21] The right to obscurity entails making information about an individual difficult to find or making the information about the individual difficult to understand.[22] The idea is that "[i]nformation is safe - at least to some degree - when it is hard to obtain or understand."[23] Obscurity does not require the deletion or removal of data from existence; rather it prevents wide dissemination of the information to the public by limiting access.[24] A right to obscurity is part of the right to privacy because it is a way to control the flow of information about oneself by making it less accessible or understandable to the general public.

The right to obscurity then allows individuals to make themselves, at least somewhat, unknown.[25] A person is obscure if an "observer does not possess critical information needed to make sense of the individual."[26] Such information includes "personal identity, social connections and personal or situational context."[27] A right to obscurity would also entail the ability to control critical information about oneself because control over that information is necessary to remain obscure.

Scholars have argued that obscurity is a means to protect privacy in the digital age.[28] By creating systems that obscure information, individuals who use those systems can maintain a private life by making it difficult to obtain critical information about themselves.[29] These systems would allow a person to remain relatively unknown and avoid constant scrutiny.[30]

However, obscurity is not an absolute right or protection.[31] Obscurity makes data difficult to find or understand, but it does not destroy the data, and therefore it can still be discovered.[32] Competent or capable individuals can still make efforts to obtain the relevant data and

---

1 (2013); Hartzog & Stutzman, *Obscurity by Design*, *supra* note 4; Rengel, *supra* note *5*.

21 Hartzog & Selinger, *The Case for Online Obscurity*, *supra* note 20; Rengel, *supra* note 5.

22 Hartzog & Selinger, *Obscurity and Privacy*, supra note 18.

23 *Id*. at 2.

24 Hartzog & Selinger, *Obscurity and Privacy*, *supra* note 18, at 2; Hartzog & Selinger, *Obscurity: A Better Way to Think About Your Data Than 'Privacy'*, *supra* note 17.

25 Obscurity is not to be confused with anonymity. Anonymity can be a means to obscurity but they are not the same. Obscurity does not require that a person is never identifiable, rather it require that a person is less easily identifiable. Hartzog & Stutzman, *The Case for Online Obscurity*, *supra* note 20, at 6.

26 Hartzog, *Case for Online Obscurity*, *supra* note 20, at 5.

27 *Id*.

28 Hartzog & Stutzman, *The Case for Online Obscurity*, *supra* note 20; Hartzog & Stutzman, *Obscurity by Design*, *supra* note 4; Hoffman et. al., *supra* note 17.

29 Hartzog & Stutzman, *Obscurity by Design*, *supra* note 4.

30 *Id*.; Hoffman et. al, *supra* note 17.

31 Hartzog & Selinger, *Obscurity and Privacy*, *supra* note 18 at 6. Hartzog & Selinger, *Obscurity: A Better Way to Think About Your Data Than 'Privacy'*, *supra* note 17.

32 Hartzog & Selinger, *Obscurity and Privacy*, *supra* note 18, at 6; Hartzog & Selinger, *Obscurity: A Better Way to Think About Your Data Than 'Privacy'*, *supra* note 17.

once they have it, the information is no longer obscure to them.[33] While this may seem to defeat the right, it is actually in keeping with it: obscurity is making the data difficult to find or understand; it is not about its total destruction. This is why obscurity stands in contrast to the right to be forgotten.

B. Defining a Right to be Forgotten

When people speak of forgetting, they are generally discussing the act of "losing remembrance" or "ceasing to remember."[34] When something is forgotten, it is defined as "not remembered, that has passed from the mind or out of remembrance."[35] For a person to forget something, it is required that they first know or have something to recall. A person cannot forget what they did not know. A "right to be forgotten" then should be a right to make people cease to remember that which they know.

The E.U.'s "right to be forgotten" has been ill defined and described as "an amorphous privilege that would allow individuals more control over their information."[36] The right has its roots in two different rights. The first right is the *droit à l'oubli*, which means the right to oblivion.[37] The second right is the in the right to erasure, which allows individuals to delete irrelevant or outdated data.[38] The right to be forgotten has been described as an individual's right to:

> [d]etermine the development of his life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past, especially when these events occurred many years ago and do not have any relationship with the contemporary context.[39]

Still others have characterized the right to be forgotten as the right "to

---

33 Hartzog & Selinger, Obscurity and Privacy, supra note 18 at 7; Hartzog & Selinger, *Obscurity: A Better Way to Think About Your Data Than 'Privacy'*, *supra* note 17.

34 *Forget*, OXFORD ENGLISH DICTIONARY.

35 *Forgetting*, OXFORD ENGLISH DICTIONARY.

36 Jasmine McNealy, *The Emerging Right to be Forgotten*, 12 INSIGHTS ON L. & SOC'Y 14 (2011-2012).

37 Allesandro Mantelero, *The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'*, 29 COMP. L. & SECURITY REV. (2013); Jeffery Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 89 (2011-2012) (The right oblivion is "a right that allows a convicted criminal who has served his time and been rehabilitated to object to the publication of the facts of his conviction and incarceration."); Walker, *supra* note 15, at 272 (Right to oblivion allows "[a] convicted criminal may object to the publication of the facts of her conviction once she has served her sentence.").

38 Meg Leta Jones & Jef Ausloos, *The Right to Be Forgotten Across the Pond*, 3 J. INFO. POL. 1, 1-2 (2013).

39 Mantelero, *supra* note 37.

have information deleted after a certain time, the right to have a clean slate, and the right to be connected only to present information."[40]

Legal scholars have struggled to define the E.U.'s "right to be forgotten," but have consistently focused on what forgetting implies.[41] The general concepts of memory loss or forcing amnesia have sparked fierce debate.[42] Scholars emphasize the idea that the "right to be forgotten" gives a person the ability to make information disappear after a period of time.[43] There is a recurring theme, that individuals have a right to make details about their past unavailable or no longer remembered.[44] For information to be forgotten it must be destroyed and rendered completely inaccessible.[45] It raises the specter of revising one's history for one's own personal needs.

C. Why the E.U.'s "Right to be Forgotten" is a Right to Obscurity

The right to obscurity and the right to be forgotten are different ways of dealing with the problem of data retention. The right to be forgotten focuses on losing remembrance of known information, while the right to obscurity focuses on making information harder to know. Forgetting raises many more questions than obscuring information. Information is constantly obscured on a regular basis via passwords, pseudonyms, paywalls, etc. However, it is much harder to declare information is constantly made forgotten.

Perhaps the reason scholars are having such a hard time defining the E.U.'s "right to be forgotten" is because the right is really about obscurity rather than forgetting. The E.U. law as it stands does not require or mandate that people forget what they know.[46] Nor does the E.U. law require the total deletion or removal of data from the internet.[47] Rather,

---

40 McNealy, *supra* note 36.

41 *Id*.; Bolton, *supra* note 15; Mantelero, *supra* note 37.

42 Bolton, *supra* note 15.

43 Mantelero, *supra* note 37.

44 Walker, *supra* note 15, at 272.

45 Drusel et. al., *The right to be forgotten – between expectations and practice*, European Network and Information Security Agency (2012), https://www.enisa.europa.eu/publications/the-right-to-be-forgotten; Floridi et al., *The Advisory Council to Google on The Right To Be Forgotten*, 3-4 (Feb. 6, 2015), https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view.

46 The Data Protection directive only requires that "irrelevant, outdated, or excessive data be removed upon request. It does not impose any requirements of forgetfulness. Data Protection Directive, *supra* note 10, art. 12(b). *See also*, Floridi et al., *supra* note 45, (The CJEU ruling, "[d]oes not have the effect of 'forgetting' information about a data subject," rather, "the information is still available at the source site, but its accessibility to the general public is reduced.").

47 Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), 2014 E.C.R. 317, ¶ 96. (The Google Spain case only requires the delisting of the article under the

the E.U. requires that information directly related to an individual be rendered less accessible upon request, by delisting a search result connected to their name, because it is information that the individual should have control over.[48] The E.U. has created a broad right to obscurity, because it makes an individual's personal information harder to find or understand.[49] The next two parts will examine both the E.U. and the U.S. laws and assert that they promote obscurity-based principles, not forgetfulness.

II. THE E.U.'S RIGHT TO OBSCURITY

A. The Data Protection Directive of 1995

In 1995, the E.U. passed the Data Protection Directive in order to "protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy with respect to the processing of personal data."[50] The Data Protection Directive also attempted to address the growing collection of personal information and the ease of access to such information due to new technology.[51] The Data Protection Directive applies to both "processing of personal data wholly or partly by automatic means" and non-automatic processing, which is part of "a filing system."[52]

The Data Protection Directive puts a large number of constraints on data controllers.[53] Data controllers are defined as any person or group of persons that "[d]etermines the purposes and means of the processing of personal data . . . ."[54] It requires that data be collected for a specified purpose,[55] not be excessive to that purpose,[56] and kept no longer than necessary for that purpose.[57] Particularly demanding is the requirement that data controllers ensure data about individuals is "accurate" and "kept

---

requester's search name.); (The news article still exists and a person can find it with different search terms.) *Id*. at ¶ 15. *See also* Dave Lee, *What Is the "Right To Be Forgotten"?*, BBC (May 13, 2014).

48 *Id*. at ¶ 100.

49 An article that is still accessible with different search terms is merely harder to find rather than be forgotten. Floridi et. al., *supra* note 45, at 4.

50 Data Protection Directive, *supra* note 10, art. 1(1). Personal Data is defined in the Directive as "[a]ny information relating to an identified or identifiable natural person . . . ." *Id*. art. 2(a).

51 *Id*. Preamble 4.

52 *Id*. at art. 3(1). A filing system for the purposes of the Directive is "[a]ny structured set of personal data which are accessible according to specific criteria . . . ." *Id*. at art. 2(c).

53 *Id*. at art. 6, 7, 12, 14. All of these articles apply specifically to data controllers.

54 *Id*. at art. 2(d)

55 *Id*. at art. 6(b).

56 *Id*. at art. 6(c).

57 *Id*. at art. 6(e).

up to date."[58] However, data controllers may be exempt from these conditions if data is processed for "historical, statistical or scientific purposes."[59]

The Data Protection Directive gives the individual a series of rights regarding their personal information. Individuals have the right to access data about themselves contained in data controllers' systems.[60] The individual is allowed to request "the rectification, erasure or blocking of data" which does not comply with the directive because it is "incomplete or inaccurate."[61] The Data Protection Directive gives individuals the right to object "at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him."[62] The Data Protection Directive also gives the right "[t]o object . . . to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing."[63] The individual can also object to the disclosure of personal information to third parties.[64]

The Data Protection Directive itself has no "right to be forgotten."[65] In fact, the rights given to the individual are relatively narrow. They allow the individual to rectify, erase, or block data that was inaccurate or excessive for the purpose it was collected.[66] The Data Protection Directive does not demand, or require, forgetfulness. The Data Protection Directive provides an individual with the means to ensure a more private life through obscurity. It prevents the data processor from gathering or making available too much personal information, or at least makes sure the information is accurate.[67] It gives an individual the means to rectify unwarranted probing into or disclosure of personal information. The Data Protection Directive makes it the data holder's duty to ensure that the information is accurate and not excessive. The next section will discuss how the CJEU has interpreted the Data Protection Directive in the context of internet search engines in the case of *Google Spain v. AEPD*.

---

58 *Id*. at art. 6(d).
59 *Id*. at art. 6(b), 6(e).
60 *Id*. at art. 12(a).
61 *Id*. at art. 12(b).
62 *Id*. at art. 14(a).
63 *Id*. at art. 14(b).
64 *Id*.
65 *See also* Floridi et al., *supra* note 45.
66 Data Protection Directive, *supra* note 10, at art. 12(b).
67 *Id*.

B. Google Spain v. AEPD.

In 1998, *La Vanguardia*, a Spanish newspaper, publicized a real-estate auction and attachment proceedings regarding Mario Costeja Gonzalez (Costeja), a Spanish citizen living in Spain, at the direction of Spanish authorities.[68] When *La Vanguardia* digitized its editions, it catalogued articles such as Costeja's and made them widely available. Over a decade later when people searched Costeja's name on the internet, links to *La Vanguardia's* 1998 article would appear.[69]

In 2010, Costeja filed a complaint, requesting the removal of the articles and their links, with the Spanish Data Protection Agency (Agencia Española de Proteccion de Datos, "AEPD") against Google Inc., Google Spain, and La Vanguardia Ediciones SL, the producer of the *La Vanguardia* newspaper.[70] Costeja asserted that the links to articles were causing him financial hardship because he had paid off the debt and the articles conveyed misinformation about his current financial status.[71] *La Vanguardia* refused to remove the article because as it produced the article pursuant to Spanish law.[72] The AEPD dismissed the claim as it related to *La Vanguardia*.[73] However, the AEPD upheld the complaint regarding Google Inc. and Google Spain, ordering them to alter the search results.[74] Google appealed this decision with the Audience Nacional, which in turn referred questions regarding European law to the CJEU.[75]

The CJEU considered three major questions. First, the court considered the territorial scope of the Data Protection Directive.[76] Second, the court considered whether a search engine could be considered "a data processor and data controller" under the Data Protection Directive and what obligations this imposed on the search engine.[77] Third, the court considered if the Data Protection Directive gives a person the right "[t]o prevent indexing of the information relating to him personally, published on third parties' web pages, invoking his

---

68 *Google Spain*, 2014 E.C.R. 317, at ¶14.

69 Herke Kranenborg, *Google and the Right to Be Forgotten*, 1 EUR. DATA PROT. L. REV. 70 (2015).

70 *Google Spain*, 2014 E.C.R. 317, at ¶15. According to the CJEU Costeja requested, "[t]hat *La Vanguardia* be required either to remove or alter" the articles so his data was no longer visible. *Id*. "[O]r to use certain tools made available by search engines in order to protect the data." *Id*. Costeja also requested, "[t]hat Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so that they ceased to be included in the search results and no longer appeared in the links to *La Vanguardia*." *Id*.

71 Rustad & Kulevska, *supra* note 14, at 633; Herke Kranenborg, *supra* note 69, at 70.

72 *Google Spain*, 2014 E.C.R. 317, at ¶16.

73 *Id*.

74 *Id*. at ¶17.

75 *Id*. at ¶18.

76 *Id*. at ¶ 20.

77 *Id*.

wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion . . . ." [78]

The CJEU found that the territorial scope of the Data Protection Directive was very broad, having seemingly no limits.[79] It also found that a search engine was a data processor for the purposes of the Directive.[80] The court held that "exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' . . .", which expressly constitutes processing.[81] The CJEU also held that the act of indexing and displaying links to other pages qualified Google as a data controller because it "determines the purposes and means of the processing of personal data."[82] By holding that Google was both a data processor and a data controller, the CJEU subjected Google to more restrictions under the Data Protection Directive, including the requirement that "irrelevant, inaccurate, or excessive" data be removed upon request. [83]

The third question, which is the most relevant to the issue at hand, considered how far the rights "to rectification, blocking, and erasure"[84] and the "right to object"[85] extend under the Data Protection Directive.[86] The question was whether an individual could:

> [r]equire the operator of a search engine to remove from the list of results displayed following a search made on the basis of his name links to web pages published lawfully by third parties and containing true information relating to him, on the ground that that information may be prejudicial to him or that he wishes it to be 'forgotten' after a certain time.[87]

The CJEU ruled that an individual could in fact require a search engine to delist search result links to webpages based on a search of the individual's name.[88] The CJEU explained that all data controllers must ensure data quality standards.[89] Under Article 12(b) of the Data Protection Directive an individual had the right to request removal of data

---

78 *Id*.

79 *Id*. at ¶¶ 21-60.

80 *Id*. at ¶ 28.

81 *Id*.

82 *Id*. at ¶¶ 31-32. *See* Data Protection Directive, *supra* note 9, art. 2(d).

83 The data quality and legitimacy restrictions apply to data controllers under the Data Protection Directive. Data Protection Directive, *supra* note 10, art. 6-7.

84 *Id*. at art. 12(b).

85 *Id*. at art. 14(a).

86 *Google Spain*, 2014 E.C.R. 317, at ¶ 89.

87 *Id*.

88 *Id*. at Grand Chamber Ruling ¶¶ 3-4.

89 *Id*. at ¶¶ 93-95.

that is incompatible with the Directive.[90] Incompatibility can stem from data being "inadequate, irrelevant or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary."[91] The court explained that data, which was once useful and necessary, could become excessive over the course of time thus subjecting it to removal.[92]

The CJEU reasoned that search results could also be delisted based on Article 7(f).[93] Article 7(f) permits data processing that furthers the legitimate interest of the data controller, or third parties except where the individual's privacy rights outweigh the opposing interests.[94] According to the CJEU, Article 7(f) "necessitates a balancing of the opposing rights and interests concerned . . . ." [95] The CJEU held that Article 12(b) and Article 14(a) could be invoked to assert that the individual's privacy right outweighed the legitimate interest of the data controller or third parties.[96] The balancing test is very fact specific, focusing on the nature of information, the individual's public status and the public's interest in the information.[97] The CJEU ruled that generally, the individual's privacy right overrides the "[e]conomic interest of the operator of the search engine [and] also the interest of the general public in finding that information . . . ."[98] However, the CJEU also held that links to search results would not be removed if there were a preponderant public interest in having access to the information, which justified the invasion of privacy.[99]

The Court held that in this situation, Costeja had a strong privacy

---

90 Data Protection Directive, *supra* note 10, art. 12(b).

91 *Id*. at ¶ 92.

92 *Id*. at ¶ 94.

93 Id. at ¶ 75.

94 Data Protection Directive, *supra* note 10, art. 7(f).

95 *Google Spain*, 2014 E.C.R. 317 at ¶74.

96 *Id*. at ¶ 75.

97 *Id*. at ¶ 81. ("Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.").

98 *Id*. Some have interpreted the CJEU's language in a later paragraph which says as "that [the right to privacy] override[s], as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name", *Id*. at ¶96, as meaning privacy is a "super human right" under EU law. Martin Husovec, *Should We Centralize the Right to Be Forgotten Clearing House?*, CENTER FOR INTERNET & SOC'Y (May 30, 2014) (quoting Hans Peter Lehofer, *EuGH: Google muss doch vergessen – das Supergrundrecht auf Datenschutz und die Bowdlerisierung des Internets*, e-comm (May 13, 2014), http://blog.lehofer.at/2014/05/eugh-google-muss-doch-vergessen-das.html), http://cyberlaw.stanford.edu/blog/2014/05/should-we-centralize-right-be-forgotten-clearing-house. However, the court was restating a balancing test in which there must be a significant public interest or right at stake to justify the violation of privacy based on the search of a person's name.

99 *Google Spain*, 2014 E.C.R 317 at ¶ 97.

interest in having the links to the articles removed in search results based on his name.[100] The information was old and sensitive, relating to past financial mishaps. Meanwhile, the public and Google had a limited interest in accessing the information based on Costeja's name.[101] Google was required to remove links to the article in searches based on Costeja's name.[102]

Some claim that the CJEU's decision is a dangerous blow to freedom of expression.[103] However, the CJEU did not deal with a freedom of expression interest in Costeja's case. Google's interest was one of economic concern, and the newspaper (which would have a freedom of expression interest) was exempt from the proceedings.[104] The public had a marginal interest in finding old financial information about a private citizen's financial troubles. In this context, the CJEU said it was better to delist the results based on a search of Costeja's name. [105] It is very possible that different inputs in the balancing test could lead to different results.

While called the "right to be forgotten," referring to the passage of time and discussing consigning information to oblivion, the CJEU never actually mandates forgetting.[106] Instead, the CJEU closely followed the Data Protection Directive, applied it to search engines and clarified the requirements of the Directive.[107] The CJEU gave an individual the right to restrict access to information by delisting search results found under his name, which is obscuring not forgetting.[108] The articles are still located on *La Vanguardia's* website and can be found under different search terms in Google.[109] Google did not forget Costeja; in reality it removed links to articles that appeared in the search results based on a search of Costeja's name making it harder for others to know. People all

---

100 *Id*. at ¶ 98.

101 *Id*.

102 *Id*.

103 *See* Rosen, *supra* note 37 (Google global privacy counsel suggests that right to be forgotten may be "used to justify censorship"); Marcus Wohlsen, *For Google, the 'Right to Be Forgotten' Is an Unforgettable Fiasco*, WIRED, July 3, 2014, http://www.wired.com/2014/07/google-right-to-beforgotten-censorship-is-an-unforgettable-fiasco/.

104 *Google Spain,* 2014 E.C.R 317 at ¶16. Further, the Data Protection Directive exempts "[t]he processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression . . . ." Data Protection Directive, art. 9.

105 *Google Spain*, 2104 E.C.R. 317, at ¶¶ 96-98.

106 *Id*.

107 Hoffman et. al, *supra* note 17; Floridi, *supra* note 45. *See also* Data Protection Directive, supra note 10, at art. 6, 12(b), 14.

108 *See supra* Part I.A; Floridi, *supra* note 45.

109 Floridi, *supra* note 45, at 3-4; Rustad & Kulevska, *supra* note 14, at 365; Rich Trenholm, *Google Must Delete Search Results on Request, Rules EU Court,* CNET (May 13, 2014), https://www.cnet.com/news/google-must-delete-search-results-rules-european-court/ (quoting Bill Echikson, *Google's Head of Free Expression*, who noted that "only the original publisher can take the decision to remove such content" and "[o]nce removed from the source webpage, content will disappear from a search engine's index").

over the world know of Costeja's quest to get the articles delisted, so it seems hard to say anything has been forgotten. However, in Europe a person cannot find the *La Vanguardia* articles on Costeja just by searching his name. The CJEU broadened the Data Protection Directive's right to obscurity, but it did not create a "right to be forgotten."

C. The General Data Protection Regulation.

In 2016, the European Council adopted the General Data Protection Regulation ("GDPR"), which does not go into effect until 2018.[110] The GDPR maintains many of the same features as the Data Protection Directive; however, it changes some rules in order to update the statute.[111] It noted that the GDPR, "[r]espects all fundamental rights . . . , in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information . . . ."[112]

Many have voiced a concern over the explicit inclusion of the "right to be forgotten" in Article 17, which is really just a clarification of the rights laid out in the Data Protection Directive and, is better understood as a right to obscurity. Article 17 is very similar to Article 12 of the Data Protection Directive.[113] Article 17 gives an individual the right to "obtain from the controller the erasure of personal data concerning him" because the data is "[n]o longer necessary in relation to the purposes for which they were collecte . . ."[114] or because the individual objects to processing of data because the individual's privacy interest outweighs the legitimate interest of the data controller or third parties.[115] The law remained virtually unchanged; it only made explicit

---

110 Regulation (EU) 2016/679 of the European Parliament and Of the Council, General Data Protection Regulation, art. 99, 2016 OJ (L 119/1).

111 General Data Protection Regulation, *supra* note 110, Preamble 6-8, 2016 OJ (L 119/1) (discusses the recent technological advances and the need for uniformity in the European law.).

112 *Id*. at preamble 4.

113 *See* Data Protection Directive, *supra* note 10, at art. 12.

114 General Data Protection Regulation, *supra* note 110, at art. 17(1)(a). The General Data Protection Regulation also gives the individual the right to request erasure when they withdraw consent to processing where the processing was based on consent. *Id*. art. 17(1)(b). It also allows the individual to request erasure when the "personal data [has] been unlawfully processed." *Id*. at art. 17(1)(d).

115 *Id*. at art. 17(1)(c). This subsection gives the individual to request removal of data when they object "[t]o the processing pursuant to Article 21(1) and there are no overriding legitimate grounds. *Id*. Article 21(1) is the right to object to processing "which is based on point (e) or (f) of Article 6(1) . . ." *Id*. at art. 21(1). Processing based on article 6(1)(f) is processing "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data . . . ." *Id*. at art. 6(1)(f). This maze of cross references says in essence that the individual can request removal of data where their privacy interests outweigh/override the legitimate interests of the data controller or third parties.

the individual's rights and obligations of data controllers. The individual has the right to invoke the balancing test annunciated by the CJEU in *Google Spain*. Article 17 is still only a right to make data less accessible and in some limited instances the right to have total removal of data.

The individual's "right to be forgotten" is also now explicitly inapplicable in instances where data processing is necessary "for exercising the right of freedom of expression and information."[116] The individual cannot request the removal of data where the processing is necessary "for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes" in accordance with E.U. law.[117] These exemptions existed in the Data Protection Directive, although more cryptically in a series of cross-references.[118]

The E.U. has never created a "right to be forgotten;" rather it gives the individual more control over their personal information. The GDPR gives the individual the right to limit access to their personal information, to limit use of their personal information,[119] and to correct erroneous personal information.[120] This is more in line with a right to obscurity as it is about making information harder to know, rather than the ultimate destruction of known information.

D. Data Controllers are the Practical Choice for Removal Requests.

There is a popular argument that putting the burden on data controllers, especially search engines, like Google, is unduly burdensome.[121] However, when looking at the responsibilities laid out by the Data Protection Directive (soon to be replaced by the GDPR) and the rights the Directive seeks to protect, the data controller is the practical choice for handling removal requests.

---

116 *Id*. at art. 17(3)(a).

117 *Id*. at art. 17(3)(d).

118 *Id*. at art. 9 ("exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression."). The enumerated Chapters include the right to erasure and the right object. *Id*. art. 12, 14. "Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 [the right to erasure] and 21 when such a restriction constitutes a necessary measures to safeguard . . . the protection of the data subject or of the rights and freedoms of others." *Id*. at art. 13(g). Presumably, these freedoms include freedom of expression, freedom of information etc.

119 *Id*. at art. 18, 2016 OJ (L 119/1).

120 *Id*. at art. 16.

121 James Ball, *'Right to be forgotten' ruling creates a quagmire for Google et al*., THE GUARDIAN (May 13 2014), https://www.theguardian.com/commentisfree/2014/may/13/right-to-be-forgotten-ruling-quagmire-google; Kashmir Hill, *The 'Right To Be Forgotten' Is A Nightmare To Enforce*, FORBES (July 24 2014), http://www.forbes.com/sites/kashmirhill/2014/07/24/the-right-to-be-forgotten-is-a-nightmare-to-enforce/#7f85457347ed.

First, it is the data controller's obligation to ensure that the data processing is legitimate and accurate.[122] The individual requesting removal based on the Data Protection Directive is asking the data controller to fulfill their legal obligation.[123] It makes more sense to have the initial discussion between the parties rather than to lodge a complaint with an agency or sue upon the violation. Litigation should be a last resort for both parties as it leads to a quicker more cost-effective resolution.

Second, the Data Protection Directive seeks to protect the individual's privacy.[124] Individuals who are requesting delisting, or removal of data, are generally seeking to restore themselves to obscurity.[125] If an individual is required to go before a court or to an agency for initial removal requests, they may be discouraged from doing so because of the public exposure such a request would lead to.[126] Judicial decisions are public record and agency decisions may be subject to public disclosure laws.[127] This is essentially urging the individual to make further available the information they wish to restrict. This would completely subvert the right to obscurity laid out by E.U. law, by making more accessible what the individual requested be obscured.

III. THE U.S.'S LIMITED RIGHT TO OBSCURITY.

The U.S. has its own form of the right to obscurity. While the European version of the right is far more expansive, the U.S. right exists in a limited and specific number of circumstances. This Part will examine how the right to obscurity exists within the context of the Freedom of Information Act, and the Privacy Act of 1974 in regards to government agencies.[128] In the consumer context, a right to obscurity exists in the form of the Fair Credit Reporting Act and in Federal Trade Commission guidance documents.[129] This Part will also examine, perhaps the most

---

122 *See supra* Part II.A- II.B.

123 *See supra* Part II.B.

124 Data Protection Directive, *supra* note 10, at art. 1(1).

125 *See Google Spain*, 2104 E.C.R. 317 (Costeja specifically requested private information be delisted to avoid further embarrassment.); Sylvia Tippmann &Julia Powles, *Google accidentally reveals data on 'right to be forgotten' requests*, THE GUARDIAN (July 15 2015), https://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests.

126 *Google Spain*, 2104 E.C.R. 317.

127 *See* Decisions of CJEU are published online, https://europa.eu/european-union/about-eu/institutions-bodies/court-justice_en.

128 Freedom of Information Act, 5 U.S.C. §552 (1966); Privacy Act of 1974, 5 U.S.C. §552a (1974).

129 Fair Credit Reporting Act, 15 U.S.C. §1681 (1970); FTC, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policy Makers*, ii, (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

expansive version of the right to obscurity in the United States, the Children's Online Privacy Protection Act. [130]

A. The Freedom of Information Act: Privacy Exemptions.

In the 1950s, the American populace became very concerned with the expanding power and secrecy of federal agencies.[131] This concern led to the push for more open and transparent government. In 1966, with the passage of the Freedom of Information Act ("FOIA") a new era of accessibility to federal agency records was ushered in.[132] The average American citizen now possesses the right to request records from a federal agency and a federal agency is required to produce them.[133] Congress created FOIA with the intention of shedding light on government actions so that the governed may hold their governors accountable.[134] FOIA, however, acknowledges that there is a vast amount of private information contained within the agency documents and disclosure of private information should be limited.[135]

FOIA contains nine exemptions that attempt to limit, or obscure, the type of information released to the public.[136] The most relevant exemption for the purpose of this discussion is Exemption 6. Exemption 6 protects against the disclosure of "personnel, medical or similar files . . . which would constitute a clearly unwarranted invasion of personal privacy."[137] The Supreme Court has interpreted similar files broadly, so that any file containing information that would be found in a medical or personnel file falls under the protection of this exemption.[138]

When deciding if the disclosure of a "medical, personnel, or similar file" would constitute a clearly unwarranted invasion of privacy the court engages in a balancing test.[139] The court weighs the individual's privacy interest against the public's interest in disclosure of the

---

130 Children's Online Privacy Protection Act, 15 U.S.C §§6501-6505 (1998).

131 Clarifying and Protecting the Right of the Public to Information, H. R. 1497, 89th Cong. (2d Sess. 1966); *History of FOIA*, EFF, https://www.eff.org/issues/transparency/history-of-foia. (Last visited, Jan. 9, 2017).

132 Department of Justice, *About FOIA*, DOJ, https://www.justice.gov/open/foia.

133 Freedom of Information Act, 5 U.S.C. §552(a)(3) (1966).

134 NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978).

135 5 U.S.C. §552(b)(1)-(9). The exemptions generally protect three kinds of information (1) personal information, (2) corporate/trade secrets, (3) police records or records that affect national security. BREYER ET. AL, ADMINISTRATIVE LAW AND REGULATORY POLICY 772 (2011).

136 5 U.S.C. §552(b)(1)-(b)(9).

137 5 U.S.C. §552(b)(6).

138 U.S Dep't of State v. Washington Post Co., 456 U.S. 595, 601 (1982).

139 Dep't of Air Force v. Rose, 425 U.S. 352, 371 (1976); *Wash. Post Co*., 456 U.S. at 599; Dep't of State v. Ray, 502 U.S., 164, 175 (1991); Dep't of Defense v. Fed. Labor Relations Authority, 510 U.S. 487, 495 (1994).

information.[140] A person must have some privacy interest at stake in order for the exemption to apply, but the requirement is only some nontrivial privacy interest.[141] According to the Supreme Court, an individual has a privacy right in the disclosure of personal information.[142] Once the person's privacy interest is established, a court considers whether the private information informs the public "what the government is up to."[143] If the information does not illuminate the government's actions and instead only serves as a source of embarrassment or harm to the private individual the court will refuse the disclosure of the record, or at the very least require the redaction of private information.[144]

Central to the exemption is the idea that private information can harm the individual when made public and disclosure should be limited. In *Department of Air Force v. Rose*, the Supreme Court acknowledged the need to redact personally identifying information in disciplinary files because the information though at one time public could harm the individuals.[145] According to the Court, the information, while known to some, was unknown to the broader public and dissemination could threaten the individual's privacy.[146] Similarly, in United States *Department of State v. Ray*, the Supreme Court rejected disclosing interviews of asylum seekers, because disclosure could lead to persecution of the individuals.[147] The relevant authorities had knowledge of the interviews and the public did not need to know personal details about the people seeking to enter the United States.[148] Neither case commanded destruction of the records in question, rather a refusal to further disseminate the records to the general public.

FOIA's Exemption 6 falls in with the right to obscurity because it limits the dissemination and access to information and gives the individual more control over their information. FOIA acknowledges that disclosure of agency information has value, but there is risk involved when that information is private in nature. Individuals give private information to agencies for various reasons, and if people know that private information can be divulged upon request, it could reduce cooperation. FOIA addresses this concern by insuring that the information remains obscure.

---

140 *Rose*, 425 U.S. at 371; *Wash. Post Co.*, 456 U.S. at 599; *Ray, 502 U.S.*, at 175; *Fed. Labor Relations Auth.*, 510 U.S. at 495.

141 *FLRA*, 510 U.S. at 500-02.

142 DOJ v. Reporter's Commc'n. for Freedom of Press, 489 U.S. 749, 763 (1989) (Privacy includes the "individual's control of information concerning his or her person").

143 *FLRA*, 510 U.S. at 495.

144 *Rose*, 425 U.S. at 373-75.

145 *Id.* at 381.

146 *Id.*

147 *Ray*, 502 U.S. at 164.

148 *Id.*

B. The Privacy Act of 1974.

While the 1950s saw a push for government transparency, with the closing of the Vietnam War, Watergate, and the expansion of computing power, the 1970s instead saw a push for privacy.[149] Members of the public and Congress became increasingly concerned with the digitization and centralization of government data.[150] The idea that the government would be able to centralize various personal documents and have them retrievable on a moment's notice was of great concern.[151] Especially with the probing and at times invasive questions federal agencies asked employees and citizens alike.[152] There was a fear that allowing the government to so closely observe and gather data would limit the actions of private citizens.[153] This fear led to the push for the Privacy Act of 1974. Originally, Congress intended to set up a Privacy Commission that would have been tasked with investigating and monitoring the risks posed by government and private databases.[154] However, this version of the bill was never passed and instead the Privacy Act of 1974 was put into effect without it.[155]

The Privacy Act of 1974 prevents disclosures of agency records about individuals without their consent. The statute provides that "no agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains . . . ."[156] The Privacy Act of 1974 limits the disclosure of personal information without the express consent of the individual. Indeed, agencies are expected to take steps to

---

149 Privacy Act of 1974 Legislative History, *supra* note 8.

150 Several Congressmen voiced concern over the ability to centralize information particularly about dissidents after the tumult surrounding the draft during the Vietnam war. *Id*. at 83-85; 1260-80.

151 *Id*. at 5. Sen. Sam J. Ervin Jr., Protecting privacy will "require foresight and the ability to forecast the possible trends in information technology and the information policies of our Government and private organizations before they actually take their toll in widespread invasions of the personal privacy of large numbers of individual citizens. Congress must act before sophisticated new systems of information gathering and retention are developed, and before they produce widespread abuses." *Id*. "One of the most obvious threats the computer poses to privacy comes in its ability to collect, store, and disseminate information without any subjective concern for human emotion and fallibility." *Id*. at 6.

152 For federal agents, such questions included whether a person believed in Christ, whether a person was a homosexual, what a person's relationship with their mother was like, whether they had a satisfying sex life, etc. *Id*. at 558, 830-31.

153 *Id*. at 4.

154 *Id*. at 9-28 as an example of the initial bill. The current Privacy Act is about disclosure and no new agency is formed. *See* 5 U.S.C. 552a.

155 *Legislative History of the Privacy Act of 1974*, DOJ, https://www.justice.gov/opcl/legislative-history.

156 The Privacy Act of 1974, 5 U.S.C. §552a(b).

prevent any unauthorized disclosure of personal information.[157]

The Privacy Act of 1974 also gives the individual the ability to request copies of their personal records and make amendments to said records.[158] The statute states that an individual may "gain access to his record or to any information pertaining to him which is contained in the [agency] system, permit him and upon his request . . . to review the record and have a copy made of all or any portion thereof in a form comprehensible to him . . . ."[159] The statute further provides that an individual may "request amendment of a record pertaining to him . . . ."[160] The agency must then "make any correction of any portion thereof that the individual believes is not accurate, relevant, timely, or complete" or provides an explanation as to why no correction is needed.[161]

The Privacy Act of 1974 imposes requirements on how the agency maintains and disseminates an individual's personal information. The agency must only maintain records with "such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[162] The agency is expected to retrieve personal information directly from the individual rather than from third parties when it is practicable.[163] The agency must ensure that records are reasonably timely, relevant, accurate and complete when making a determination about an individual.[164] The agency must not maintain records on how the individual exercises their right to freedom of speech unless a statute authorizes such a record, the individual authorizes the record, or there is a law enforcement purpose.[165]

The Privacy Act, like FOIA, implicitly acknowledges the individual's right to obscurity. The legislative history demonstrates that Congress was conscious and concerned with the damaging effect that easy access to personal data could have on privacy and, in the long-term, individual freedom. While the final version of the Privacy Act did not

---

157 Big Ridge, Inc. v. Fed. Mine Safety & Health Review Commc'n, 715 F.3d 631, 650 (7th Cir. 2013).

158 5 U.S.C. §552a(b).

159 5 U.S.C. §552a(d)(1).

160 *Id*. at (d)(2).

161 *Id*. at §(d)(2)(B)(i)-(ii).

162 *Id*. at §(e)(1)

163 *Id*. at §(e)(2) (An agency shall "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs").

164 *Id*. at §(e)(5) (Agency shall "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.").

165 *Id*. at §(e)(7) (Agency shall "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity").

establish all Congress hoped for the Privacy Act creates an obscuring mechanism.[166] Much like the Data Protection Directive, the Privacy Act allows individuals to limit disclosure and access to personal information. A personal record cannot be disclosed without the individual's consent.[167] Similar to the Data Protection Directive, the individual has the ability to request and amend inaccurate, untimely, irrelevant or incomplete data.[168]

The Privacy Act also demands that the data collected on individuals be relevant to the purpose for which it was collected. However, the Privacy Act is much narrower than the Data Protection Directive because it applies only to agencies. Even in its narrow application, the Privacy Act demonstrates that the American legal system acknowledges the need for obscurity.

C. The Fair Credit Reporting Act.

The Fair Credit Reporting Act ("FCRA") was passed to ensure that consumer reporting agencies release fair and accurate reports of consumer credit history.[169] The FCRA prevents misinformation from being used against consumers for determinations about employment or credit.[170] The law applies to consumer reporting agencies, those who supply information to consumer reporting agencies, and those who use consumer reports (such as employers).[171] The FCRA applies specifically to consumer reports, which are any form of communication that are used for credit, insurance, employment or any other purpose authorized by the act.[172] The FCRA focuses on obscurity by giving the individual access to and control over their information, as well as limiting the access of others to that information. The FCRA contains many provisions similar to those in the E.U.'s Data Protection Directive.

The FCRA limits access to consumer files.[173] The FCRA only allows consumer reporting agencies to disclose consumer reports for permissible purposes listed in the act.[174] It is not necessary to go into

---

166 *Legislative History of the Privacy Act of 1974*, U.S. Dep't of Justice, https://www.justice.gov/opcl/legislative-history.

167 The Privacy Act of 1974, 5 U.S.C. §552a(b).

168 *Id*. at §(d)(2)(B)(i)-(ii).

169 Fair Credit Reporting Act, 15 U.S.C. § 1681(a).

170 *Id*.; Matthews v. Worthen Bank & Trust Co., 741 F.2d 217 (8th Cir. 1984).

171 15 U.S.C. §§ 1681b, 1681m, 1681s-2.

172 15 U.S.C. § 1681a.

173 *A Summary of Rights Under the Fair Credit Reporting Act*, FTC, https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

174 15 U.S.C. §1681b(a), (f). §1681b(a) lists the permissible purposes which include judicial order to furnish a consumer report, a request by consumers to produce a report about themselves, and requests where the person is engaged in a transaction involving or necessitating use of credit information. §1681b(f) explicitly states that the only valid grounds for giving a consumer report

detail of each permissible purpose, however it is important to note that disclosure is limited.[175] The FCRA prevents agencies from disseminating presumably true information maintained by the consumer reporting agency.[176] An individual also has the right to request their information be removed from consumer reporting lists and to not have their information released to any third parties in transactions the individual has not initiated.[177] If an employer is requesting the consumer report, the agency must get the individual's consent before releasing it.[178]

The FCRA limits the type of information maintained in consumer reports. The FCRA excludes "civil suits, civil judgments, and records of arrest that from date of entry, antedate the report by more than seven years or until the governing statute of limitations has expired, whichever is the longer period."[179] It further excludes, "any other adverse item of information, other than records of convictions of crimes which antedates the report by more than seven years".[180] This is necessarily true information that the consumer agency may not disclose in a consumer report.

The FCRA compels consumer reporting agencies to maintain accurate, complete and up to date information.[181] The FCRA gives individuals the ability to request access to consumer reports about themselves and contest information within the report.[182] The consumer reporting agency is required to investigate the matter within thirty days.[183] However, the consumer reporting agency is not required to investigate invalid or frivolous requests.[184] If the information is inaccurate or unverifiable, the consumer reporting agency must correct or delete the information from its records.[185] The consumer reporting agency is also required to inform the person that produced the information that the record has been disputed[186] or altered.[187] The FCRA also requires that consumer reporting agencies take steps to ensure that the inaccurate, incomplete, or unverifiable information does not reappear on the

---

are the one's listed in the statute.

175 15 U.S.C. §1681b.

176 15 U.S.C. §1681c (a) (lists information which is impermissible to include, not because it is untruthful but because of the expiration of a time period.).

177 15 U.S.C. §1681b(e).

178 15 U.S.C. §1681b(b)(2).

179 15 U.S.C. §1681c(a)(2).

180 *Id*. at §1681c(a)(5).

181 15 U.S.C. § 1681i(a)(1).

182 *Id*.

183 *Id*.

184 *Id*. at § 1681i(a)(3)

185 *Id*. at § 1681i(a)(5)(A)(i).

186 *Id*. at § 1681i(a)(2).

187 *Id*. at §1681i(a)(5)(A)(ii).

consumer report.[188]

People or organizations that provide information about individuals to consumer agencies also have duties to ensure that the information is accurate and complete.[189] If a furnisher of information knows or finds out that the information is inaccurate, the furnisher is obligated to inform the consumer reporting agency.[190] Individuals are given the right to contest the information's accuracy with the person or entity that provided the information.

The statue promotes limiting access to and dissemination of personal information while allowing the individual the right to remove inaccurate or outdated data. These rights fall in line with the right to obscurity. However, the FCRA contains an actual "right to be forgotten" because information, which is true but harmful, must be deleted from the record after a set period.[191] As stated in Part I, this is forgetting because it is the removal of that which is known. Nevertheless, the statute does not require the absolute destruction of information rather the statute requires the personal information retained by consumer reporting agencies be fair and accurate representations of the individual.

D. The Children's Online Privacy Protection Act.

The Children's Online Privacy Protection Act ("COPPA") was passed in 1998 in order to prevent deceptive or unfair practices concerning the collection, use and disclosure of personal information from and about children on the internet.[192] COPPA applies to operators of websites or services directed at children or operators who have actual knowledge that they are collecting or maintaining personal information[193] from or about children.[194] For the purposes of COPPA, a child is "any individual under the age of 13." [195] An operator is "any person who operates a Web site located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such Web site or online service, or on whose behalf such information is collected or maintained . . . ."[196]

---

188 *Id*. at § 1681i(a)(5)(C).

189 15 U.S.C. § 1681s-2(a)(1).

190 *Id*.

191 15 U.S.C. §§ 1681c(a)(2), (a)(5).

192 Children's Online Privacy Protection Act, 15 U.S.C. § 6502; 16 C.F.R. §312.1 (1998).

193 Personal information is a defined term meaning any "individually identifiable information about an individual collected online."15 U.S.C. §6501(8). This includes names, home addresses, email addresses, phone numbers etc. *Id*.

194 15 U.S.C. §6502(a)(1); 16 C.F.R. §312.3.

195 15 U.S.C. §6501(1).

196 15 U.S.C. §6501(2); 16 C.F.R. §312.2.

COPPA required the Federal Trade Commission ("FTC") to promulgate regulations compelling operators to "provide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information."[197] COPPA also requires that operators "obtain verifiable parental consent for the collection, use, or disclosure of personal information from children."[198]

COPPA gives parents the right to access and control the use of their child's personal information. COPPA gives the parent the right to request that the operator furnish the personal information maintained on their child.[199] A parent has the right to prevent the operator from storing or using their child's information on the operator's website.[200] The parent may also prevent the operator from collecting more information about their children in the future.[201] This points to obscurity because it limits access to information and provides control over the information. It allows a child to have their information remain unknown.

COPPA imposes numerous restrictions and duties on the operators of websites that gather information from children. Operators must obtain parental consent before using, maintaining or disclosing a child's information.[202] Even when operators have consent, they are subject to the duties imposed by COPPA. For example, operators have a duty to maintain a child's personal information only for as long as is reasonably necessary, and to delete unnecessary information.[203] Additionally, operators must ensure that what personal information they do have is reasonably secure and confidential.[204] Operators are prohibited from "conditioning a child's participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity."[205]

COPPA strongly promotes the obscurity of children's personal information. The law gives parents the ability to control and limit access

---

197 15 U.S.C. §6502(b)(1)(A)(i).

198 *Id*. at §6502(b)(1)(A)(ii); 16 C.F.R. §312.5.

199 *Id*. at §6502(b)(1)(B)(i).

200 *Id*. at §6502(b)(1)(B)(ii).

201 *Id*.

202 15 U.S.C. §6502(b)(1)(A)(ii).

203 Pursuant to its authority under COPPA the FTC requires that "an operator of a Web site or online service shall retain personal information collected online from a child for only as long as is reasonably necessary to fulfill the purpose for which the information was collected." 16 C.F.R. §312.10.

204 15 U.S.C. §6502(b)(1)(D) (The regulations shall "require the operator of such a website or online service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children."); 16 C.F.R. 312.8 ("The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.").

205 15 U.S.C. §6502(b)(1)(C).

to their children's private information. Again, COPPA does not require forceful forgetting of known information. The law instead imposes that the information be used for specific purposes and that the information remain private unless there is consent to disclose the information to third parties. This is in keeping with the right to obscurity because it focuses on making information harder to know, thereby promoting the child's privacy.[206] Oddly, the expansive rights that are given to parents on behalf of their children have no parallel for the parents themselves or anyone over the age of 13. One would expect that when parents are given rights on behalf of their children it is because their children cannot yet exercise those rights themselves. However, in the case of COPPA parents are given rights on behalf of their children that they themselves lack and that their children will lose at the ripe age of 13.

E. FTC's Guidance on Privacy.

While the U.S. Congress has not passed any broad privacy law concerning data collection by businesses, the FTC has consistently urged for more privacy protections.[207] In 2012, the FTC issued a report providing recommendations to policy makers and businesses about how they should address privacy in the modern era.[208] The FTC urged businesses to adopt a privacy framework, which describes the best business practices for companies dealing with private information.[209] Congress has not acted upon the recommendations made by the FTC report. However, some private business has adopted self-regulatory agreements and implemented privacy protections based on FTC recommendations.[210]

The FTC's privacy framework focused on four major areas. First, the FTC focused on the scope of the privacy framework. The framework was to apply to "commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device, unless the entity collects only non-sensitive data from fewer than 5,000 consumers per year and does not share the data with third

206 The FTC requires that disclosure to third parties be limited and that the types of data collected be limited pursuant to COPPA. Complying with COPPA: FAQ, FTC, https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#Disclosure.

207 FTC, *supra* note 129.

208 *Id*.

209 *Id*. at v-vi.

210 The Digital Advertiser's Alliance adopted self-regulatory principles for online behavioral advertising, based on a 2009 FTC report, which have been continually updated with the FTC's recommendations. Digital Advertiser's Alliance, *The DAA Self-Regulatory Principles*, DAA, http://www.aboutads.info/principles/ (last visited Jan. 1 2017).

parties."[211] The primary concern over this formulation was stifling flexibility and innovation.

Second, the FTC urged for privacy by design, meaning that privacy is implemented at every phase of the product or service.[212] According to the FTC, this required companies to "incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy."[213] Reasonable collections limits collection of personal information "consistent with the context of a particular transaction."[214] The framework requires companies to "implement reasonable restrictions on the retention of data" and to "dispose of it once the data has outlived the legitimate purpose for which it was collected."[215] Retention periods and deletion practices are flexible based on the context of the collection.[216] Privacy by design also requires that the information collected by companies be accurate, which could only be achieved through access to information contained by companies.[217]

Third, the FTC recommended that consumers be given choice over how data was collected and with whom it was shared with based on the context of the collection.[218] The FTC explained that in some instances companies would not be required to give consumers a choice on how their data was collected. Companies do not need to "provide choice before collecting and using consumer data for practices that are consistent with the context of the transaction or the company's relationship with the consumer, or are required or specifically authorized by law."[219] When using or collecting data inconsistent with the context, the company is expected to offer choice in a meaningful and relevant manner.[220] The FTC suggests, "companies should obtain affirmative express consent before (1) using consumer data in a materially different manner than claimed when the data was collected; or (2) collecting sensitive data for certain purposes."[221]

Fourth, the FTC recommended increased transparency on the

---

211 FTC, *supra* note 173, at 22.

212 *Id*.

213 *Id*. at 30.

214 *Id*. at 27.

215 *Id*. at 28.

216 *Id*. at 28-29.

217 The FTC noted that reasonable accuracy would be dependent on the sensitivity of the information. *Id*. at 30. Some information, like information used to determine benefits, requires more accuracy than others do. *Id*.

218 *Id*. at 35-60; *see also Agency Calls on Companies to Adopt Best Privacy Practices*, FTC (March 26, 2013), https://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy.

219 FTC, *supra* note 173, at 48.

220 *Id*. at 48-50.

221 *Id*.at 76.

collection and use of consumer data.[222] The FTC urged companies to make "clearer, shorter, and more standardized" privacy notices "to enable better comprehension and comparison of privacy practices."[223] The FTC also urged companies to provide greater access to and knowledge about the information that companies maintained about consumers. Companies are expected to provide reasonable access to the data they maintain proportionate to the sensitivity of the data and nature of its use.[224] Greater access allows for more meaningful choice and increased accuracy of the data.

The FTC report broadly supports a right to obscurity. The privacy framework is concerned with giving consumers access to their personal information, control over their personal information and limiting disclosure of the information. These are all ways to prevent the information from being known by unintended parties; in other words, it promotes the individual's right to be obscure. The FTC's privacy framework seeks to hold collectors of private information accountable to maintaining that information's privacy and giving the individual control over how such information is being used.

IV. A BROAD RIGHT TO OBSCURITY IS COMPATIBLE WITH U.S. LAW.

While the United States has a right to obscurity, it exists in a myriad of laws with specific applicability.[225] The U.S. law stands in contrast to the E.U. where the Data Protection Directive provides a widely applicable right to obscurity.[226] Much of the argument against the right has focused on it being "the right to be forgotten" and that such a right poses to great a risk to freedom of expression.[227] No "right to be forgotten" truly exists in the law and rather the right at issue is the right to obscurity. Arguments against the right have focused on the negative implications of forced forgetfulness, of creating memory holes and stifling expression.[228] However, a broad right to obscurity along the lines of the E.U. law would not impose forgetfulness. Instead, it would give the individual more control over their personal information and would

222 *Id*. at 60.

223 *Id*. at 64.

224 *Id*. at 71. The FTC also noted that its support "[of] an "eraser button," through which people can delete content that they post online." *Id*. at 70. Explaining that, "many companies already offer this type of feature, which is consistent with the principles of data access and suppression." *Id*. However, it did note that such a button may present First Amendment concerns. *Id*. at 71.

225 See *supra* Part III.

226 See *supra* Part II.

227 See *supra* Part I.

228 See *supra* Part III.A.

prevent wide dissemination of the information from the outset.

A broad right to obscurity could exist in the U.S. for three reasons. First, the U.S. legal system already engages in balancing of individual rights.[229] Several areas of the legal system curtail free speech for the purpose of public interest or the protection of individual liberties. Second, well-crafted exemptions could lessen the worrying implications of a right to obscurity. Tort law already contains the "newsworthiness doctrine" for the disclosure of otherwise private information.[230] Third, privacy and control of one's personal information is a prerequisite for free speech.[231]

As to the first point, the U.S. courts engage in balancing individual rights, including free speech, in numerous situations.[232] As discussed above, in the context of FOIA, when a person requests a government document with an individual's private information, the court will weigh the public interest in knowing what the government is up to against the individual's right to privacy.[233] Often the individual's right to privacy will outweigh the public's right to know.[234] Copyright law requires courts to balance freedom of expression against the copyright holder's rights to restrict dissemination of expression.[235] Copyright law has developed mechanisms to ensure that free speech is not unduly curtailed.[236]

In the case of the right to obscurity, the law would be balancing an individual's right to privacy against another's freedom of expression. The E.U.'s law provides an imperfect example of what considerations would go into a balancing test.[237] It would require considering the sensitivity of the information, the context of the information, the effect or usefulness to public interest, and the interest in freedom of speech.[238] Scholarship suggests that U.S. law would heavily weigh the scale toward of freedom of expression, but this does not negate or lessen the value of privacy protections.[239] Most often, the type of expression that conflicts with

---

229 *See* T. Alexander Aleinikoff, *Constitutional Law in the Age of Balancing*, 96 YALE L.J. 943 (1987); Jud Mathews and Alec. S. Sweet, *All Things in Proportion? American Rights Doctrine and the Problem of Balancing*, 60 EMORY L.J. 799 (2011).

230 Walker, *supra* note 15; Carbone, *supra* note 16.

231 See ADAM MOORE, PRIVACY RIGHTS MORAL AND LEGAL FOUNDATIONS (2011); Magi, *supra* note 6; Selinger & Hartzog, *Obscurity and Privacy, supra* note 18; Bolton, *supra* note 15.

232 *See* Aleinikoff, *supra* note 229; Mathews & Sweet, *supra* note 229, at 797. The Supreme Court has specifically engaged in balancing freedom of expression for symbolic speech. United States v. O'Brien, 391 U.S. 367 (1968); David S. Bogen, *Balancing Free Speech*, 38 MD. L. REV. 387 (1979).

233 *See supra* Part III.A.

234 *Id*.

235 235Erwin Chemerinsky, *Balancing Copyright Protections and Freedom of Speech: Why the Copyright Extension Act is Unconstitutional*, 36 LOY. L.A. L. REV. 83 (2002); Steven J. Horowitz, *A Free Speech Theory of Copyright*, 2009 STAN. TECH. L. REV. 2, 7-8.

236 Chemerinsky, *supra* note 222; Horowitz, *supra* note 222.

237 *Google Spain,* 2014 E.C.R. 317, at ¶ 75.

238 *Id*.

239 McKay Cunningham, *Free Expression, Privacy, and Diminishing Sovereignty in the*

privacy rights is of a commercial variety. The Supreme Court has held that not all speech is equal, and has been more willing to curtail commercial speech.[240] In any event, the law is capable of balancing individual rights against one another when it is necessary.

Second, explicit exemptions could lessen the more worrying aspects of the right to obscurity. Exemptions that apply specifically to "matters materially affecting the public interest" or that are "newsworthy" would provide a safety valve against abuse of obscurity rights.[241] Specific exemptions for criminal records and news publishers could be crafted.[242] Already existing under U.S. law is the "newsworthiness doctrine" for the tort of public disclosure of private information.[243] The newsworthiness doctrine protects any publication of truthful facts obtained lawfully.[244] A similar provision could be encapsulated in an expansive privacy law. However, the key to effective obscurity based laws would be limiting the ways in which private information is disclosed rather than waiting until after the private information becomes public.

Third, and perhaps most important, privacy is necessary to have true freedom of expression.[245] In order to freely express oneself a person must be able to make autonomous choices. A free expression is one that that the individual chooses to make, not one that is dictated to them. Surveillance and observation are a direct limitation on autonomy because they can either eliminate choice entirely or change the nature of choice.[246] A person behaves differently in private than they do in public; they speak differently with intimate partners than they do with a total stranger. If

---

Information Age: The Internationalization of Censorship, 69 ARK. L. Rev. 71, 88 (2016).

240 *See* Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 758 (1985) ("We have long recognized that not all speech is of equal First Amendment importance."); Ohralik v. Ohio Star Bar Ass'n, 436 U.S. 447, 456 (1978) (Ruling that commercial speech is a "subordinate position in the scale of First Amendment values"); Cass R. Sunstein, *Low Value Speech Revisited*, 83 NW. U. L. REV. 555, 557 (1989) (arguing that protecting free speech depends on "making distinctions between low and high value speech, however difficult and unpleasant that task may be").

241 The balancing test enunciated in *Google Spain* provides an example. 2014 E.C.R. 317. The General Data Protection Regulation further clarified ". . .[t]he controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims." *supra* note 123, at art. 21(1).

242 General Data Protection Regulation, *supra* note 110, at art. 17(3), 2016 OJ (L 119/1).

243 Dora Georgescu, *Two Tests Unite to Resolve the Tension Between the First Amendment and the Right of Publicity*, 83 FORDHAM L. REV. 907 (2014); Cunningham, *supra* note 227; Walker, *supra* note 15, at 266.

244 Fla. Star v. B.J.F., 491 U.S. 524, 533 (1989); Cunningham, *supra* note 227, at 88.

245 *See* Moore, *supra* note 231, at Chapter 7; Magi, *supra* note 6*;* Hartzog & Seligner, *supra* note 18; Bolton, *supra* note 15.

246 Jeffrey H Reiman, *Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Information Technology of the Future*, *in* PRIVACIES: PHILOSOPHICAL EVALUATIONS, 194–214 (Beate Rossler, ed., Stanford University Press, 2004); Magi, *supra* note 14, at 193.

every piece of information becomes public or knowable it changes the way individuals behave.[247] Will one visit a website one may truly want to visit if it can subject one to ridicule, will one voice a preference to friend if that preference can be lambasted by anyone? FOIA was created based on a similar assumption that making citizens aware of what their government was up to would create greater accountability, thereby changing government behavior.[248] However, the value of such observation is questionable when it is about private citizens because it is unclear whom citizens are being held accountable to and for what.

Further, a lack of privacy leads to self-censorship.[249] Individuals will anticipate observation and change their speech to conform with norms, for fear of repercussions not only legal but also societal.[250] Individuals will be less likely to voice unpopular views if they know that anything they say will be scrutinized.[251] Constant scrutiny prevents individuals from being able to develop and hone their ideas before bringing them to the public, which is necessary for free expression. Losing control over what information is collected and to whom it is disseminated makes individuals more conscious and less likely to say or do what they truly wish to.[252] The First Amendment exists to prevent censorship and promote peaceful discourse, but eroding privacy leads to the very censoring the First Amendment sought to prevent. While at times freedom of expression and privacy may clash, both are necessary for a free and open society.

V. CONCLUSION

While called the "right to be forgotten," the E.U. law would be better understood as a right to obscurity. The E.U. law does not focus on imposing forgetfulness, instead it focuses on promoting individual control and limitations on third party access to personal information. The E.U. imposes obligations on those who collect private information to ensure the accuracy, relevance, and protection of personal information. The CJEU did not create a new right with its decision, but it clarified an

247 The famous example is Jeremy Bentham's panoptic on prison. Magi, *supra* note 14 at 194; Thomas McMullan, *What does the Panopticon Mean in the age of digital surveillance,* THE GUARDIAN (Jul. 23, 2015), https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham. A panopticon works by putting individuals in a cell where they know they can be observed, but not when they are being observed. Magi*, supra* note 5, at 104.

248 *FLRA*, 510 U.S. at 495.

249 Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 448 (1980); Magi, *supra* note 5, at 194.

250 Magi, *supra* note 5.

251 *Id*.

252 *Id*.

existing right under the E.U.'s existing legal regime. The Data Protection Directive and the GDPR create obscurity rights that limit access and use of personal data.

The U.S. contains a number of laws which are far more limited in application, but provide parallel rights to E.U. law. Indeed, the Privacy Act of 1974, which existed many years before the E.U.'s law, contains many of the rights that appear in the E.U. law. Again, the U.S. laws promote obscurity by allowing access, control, and limiting dissemination of personal information. There is no requirement of forgetting known information, or permanent destruction, instead it focuses on preventing public access to information.

A broader right to obscurity would be compatible with and useful to U.S. law. The U.S. already balances and at times curtails freedom of expression. Explicit exemptions could limit the worrying implications of a broader right to privacy. While a broad right to obscurity may raise free speech concerns, it is necessary to protect and promote freedom of speech. A free and open society cannot exist if every piece of private data could be examined, exposed and subjected public scrutiny at any moment. Attempts to promote privacy should emphasize limitations on disclosure instead of restrictive tools after the information has been released. Privacy is better served by proactive measures, as once the information is disclosed it is difficult and at times impossible to rescind.