Laws **2014**, *3*, 469–508; doi:10.3390/laws3030469

OPEN ACCESS

laws

ISSN 2075-471X
www.mdpi.com/journal/laws/

Article

Networked Memory Project: A Policy Thought Experiment for the Archiving of Social Networks by the Library of Congress of the United States

Chloé S. Georas

School of Law, University of Puerto Rico, P.O. Box 23349, San Juan 00931-3349, Puerto Rico;
E-Mail: cgeoras@law.upr.edu

Received: 18 February 2014; in revised form: 10 July 2014 / Accepted: 14 July 2014 / Published: 31 July 2014

Abstract: This article explores the challenges posed by an archival interest in the broad palimpsest of daily life left on social networks that are controlled by private corporations. It addresses whether social networks should be archived for the benefit of future generations and proposes a policy thought experiment to help grapple with these questions, namely, the proposal for the formation of the public interest-oriented Networked Memory Project by the Library of Congress for the archiving of social networks. My discussion of the challenges posed by this thought experiment will focus on the U.S. legal framework within which the Library of Congress operates and take Facebook. To the extent that social networks have user-generated contents that range from the highly "private" to "public" as opposed to other networked platforms that contain materials that are considered "public", the bar for the historical archival of social networks is much higher. Almost every archival effort must contend with the legal hurdle of copyright, but the archiving of social networks must also address how to handle the potentially sensitive nature of materials that are considered "private" from the perspective of the social and legal constructions of privacy. My theoretical exercise of proposing the formation of the Networked Memory Project by the Library of Congress responds to the need to consider the benefits of a public interest-oriented archive of social networks that can counter the drawbacks of the incidental corporate archiving taking place on social networks.

Keywords: social networks; Facebook; archive; memory; privacy; copyright; privatization; U.S. Library of Congress; deposit requirement; digital death

1. Introduction

This article explores the challenges posed by an archival interest in the broad palimpsest of daily life left on social networks [1,2] that are controlled by private corporations. It addresses whether social networks should be archived for the benefit of future generations and proposes a policy thought experiment to help grapple with these questions, namely, the proposal for the formation of the public interest-oriented Networked Memory Project by the Library of Congress for the archiving of social networks. My discussion of the challenges posed by this thought experiment will focus on the U.S. legal framework within which the Library of Congress operates and take Facebook as its test case given that it is the "undisputed leader [of] the U.S. social networking market with 166 million unique visitors in November [of 2011]" [3,4].

To the extent that social networks have user-generated contents that range from the highly "private" to "public" as opposed to other networked platforms that contain materials that are considered "public", the bar for the historical archival of social networks is much higher. Almost every archival effort must contend with the legal hurdle of copyright, but the archiving of social networks must also address how to handle the potentially sensitive nature of materials that are considered "private" from the perspective of the social and legal constructions of privacy. The "incidental" archiving of "private" multimedia communications [5] on social networks by corporations such as Facebook, whose purpose was not archival in and of itself, raises difficult normative questions regarding the techno-legal infrastructure that should be promoted for the archival of social network communications.

My theoretical exercise of proposing the formation of the Networked Memory Project by the Library of Congress responds to the need to consider the benefits of a public interest-oriented archive of social networks that can counter the drawbacks of the incidental corporate archiving taking place on social networks. However, this theoretical exercise may raise more questions than it can answer and its study of the mechanisms of archival is directed at exploring and discussing a series of extremely pertinent points, including privacy, ownership and the persistence of memory, many of which resonate across multiple disciplines. As such, this article's exploration of The Networked Memory Project as a thought experiment is less concerned with how social networks can be archived and more concerned with whether they can be archived and what issues would that raise from a legal and socio-cultural perspective.

The article is divided as follows: First, I address the regulatory model of analysis put forward by Lessig, consisting of social norms, laws, code and markets, in order to frame the discussion of the succeeding sections. Second, I discuss why the Library of Congress is ideally situated for the public archiving of social networks in light of: (a) the unique historical role of the Library of Congress in the U.S. and its related deposit requirement; (b) the emergence of a new self-archiving subject engaged in a uniquely democratic and plural construction of cultural memories through novel online processes taking place on social networks; and, (c) the need to counter the danger posed by the escalating privatization of institutions of memory in the context of digital archival projects. Third, I explore the implications of the different socio-legal constructions of privacy for the archiving of the multimedia communications that take place on social networks. Fourth, I analyze how the debate surrounding digital death, which is at a crossroads of complex property and privacy claims of both corporate online service providers and the heirs of deceased account holders, impacts the public interest-oriented

archiving of social networks. Fifth, I discuss the copyright hurdles to the digital archiving of social networks by the Library of Congress, including an analysis of the limitations of the current framework of the deposit requirement, the library exception and the fair use doctrine. Sixth, I analyze the limitations and dilemmas posed by the incipient social network-related internet preservation projects at the Library of Congress. Seventh, I explore the thought experiment of forming the Networked Memory Project at the Library of Congress, through a hybrid two-pronged strategy, wherein: (a) all communications on social networks that are posted under a "Public" setting, meaning that they are visible to all the members of the social network, could be archived through the mandatory deposit requirement, subject to privacy-protection measures; and, (b) all communications that fall below the bar of the "Public" setting, including postings to a circle of "Friends" irrespective of its size, could require another archival strategy that envisions the discretionary nature involved in sharing contents that are considered more private.

2. Lessig's Regulatory Framework: Making Encoded Values Visible and Accountable

Lessig's rich theorization of the regulatory forces that come into play in the internet provides a framework to analyze the challenges of archiving social networks. His critical understanding of technology considers how technology structures human activities and is inevitably implicated in the social, moral and legal dilemmas that societies must address. Lessig's approach emphasizes that the internet is infinitely malleable to the extent that the "code" of cyberspace (meaning its technical architecture) can be changed. As a result, for Lessig there is no underlying nature or essence to the internet [6]. However, although the architecture of cyberspace is neutral, Lessig makes the important proviso that the "choice about which [architecture] to enable […] is not in any sense neutral" ([6], p. 522). For Lessig the architecture of cyberspace is a form of power and, as such, should be subject to critical interrogation rather than taken for granted. Inspired by Unger, Lessig stresses that "we should interrogate the necessities of any particular social order and ask whether they are in fact necessities, and we should demand that those necessities justify the powers that they order" [7]. By questioning power, we are able to examine the constraints we can do something about. Politics becomes "how we decide, how that power is exercised, and by whom" ([7], p. 78).

Since "[c]yberspace demands a new understanding of how regulation works" ([7], p. 5), Lessig proposes a new regulatory framework to understand how human behavior is constrained that responds to the uniqueness of the challenges posed by the technical architecture of cyberspace. The regulatory framework proposed looks at the synergy between the following constraints of human behavior: code/architecture (West Coast Code), laws (East Coast Code), social norms and markets. An analysis of the project of archiving social networks must thus engage with how social norms, laws, code and markets interface in ways that enable and/or undermine the collection and preservation of the novel forms of communication taking place on social networks [8].

Shifting social norms and practices relative to networked technologies are integral to understanding the limitations, potential and ambiguity of these new technologies. In particular, there are two areas where we see profound shifts in social practices that have implications for archiving projects: first, the emergence of social subjects actively and self-reflexively engaged in archiving as part of their everyday lives [9]; and, second, changing cultural conceptions of privacy in online forms of expression that undermine the traditional distinction between "public" and "private" spheres [10]. In terms of

legal forms of regulation, copyright and privacy laws are crucial in defining the scope of archiving efforts. Whereas copyright law is particularly anachronistic and inhibitory to archiving projects, the legal privacy framework of privacy is not sufficiently nuanced to accommodate the complex scales of visibility deployed by people on social networks [11].

Similar to social norms and laws as regulatory forces, code or the technical architecture of cyberspace constrains and enables particular patterns of behavior while making impossible others. Yet here Lessig states that code writers are inadvertently becoming lawmakers given that they are embedding certain social values at the expense of others.

> As the world is now, code writers are increasingly lawmakers. They determine what the defaults of the Internet will be; whether privacy will be protected; the degree to which anonymity will be allowed; the extent to which access will be guaranteed. They are the ones who set its nature ([7], p. 79).
>
> We can build, or architect, or code cyberspace to protect values that we believe are fundamental. Or we can build, or architect, or code cyberspace to allow those values to disappear. There is no middle ground ([7], p. 6).

As the "'built environment' of social life in cyberspace" ([7], p. 121), code can be a great threat to established liberties in ways that we may yet not even grasp. Rather than take the built environment of a social network such as Facebook for granted, the thought experiment at hand for the archival of social networks must evaluate the implications of how their technical architectures draw the boundaries between communications that are considered "private" and "public" relative to the cultural practices surrounding, and legal definitions of, privacy. In addition, to the extent that the architectures of social networks archive as part of the very functionality and design of their platforms, it points to a scenario of default ownership by the online service provider of the contents produced by users irrespective of what the terms of service may stipulate to the contrary. Although users of Facebook, for instance, successfully resisted the company's efforts to claim ownership over the contents generated by them, there still remain many gaps in terms of the status of said contents, particularly upon death [12].

In the regulatory synergy between East and West Coast Code, Lessig is not sure which should be most feared. Technological and legal architectures can interact in unpredictable ways, either entrenching or undermining each other.

> It is not clear which code one should fear more. The conflict displaces values in both spheres, but cooperation threatens values as well […].
>
> This conflict between code and law should push us to consider principle. We should think again about the values that should guide, or constrain, this conflict between authorities. […] [C]yberspace is not inherently unregulable; […] its regulability is a function of its design. Some designs make behavior more refutable; others make behavior less regulable. Government […] can influence the design of cyberspace in ways that enhance government's ability to regulate ([6], p. 534).

Although Lessig believes that commerce has "done its part-for commerce, and indirectly, for governments" ([7], p. 61), he calls for an analysis of the values that should guide governmental regulation in cyberspace because the "final step will require action by the government" ([7], p. 61).

Archival projects are a forceful illustration of how market forces, combined with increasing copyright protections, are leading to the privatization of institutions of memory and are working against public interest-oriented preservation projects in networked societies. Governmental regulation is needed to counter the detrimental effect of market forces and corporate interests because, ultimately, the invisible hand of the market will not magically solve the regulatory gap [13].

Lessig furthers his critique of the assumption of inherent unregulability in his discussion of how "[i]ndirection misdirects responsibility", namely,

> [w]hen a government uses other structures of constraint to effect a constraint it could impose directly, it muddies the responsibility for that constraint and so undermines political accountability. If transparency is a value in constitutional government, indirection is its enemy. It confuses responsibility and hence confuses politics ([7], pp. 133, 136).

Although Lessig is not on principle opposed to indirect regulation, he nevertheless is concerned by how through indirection the government can achieve goals without confronting the cost of pursuing them directly. The biggest cost is to political transparency in a democracy where regulations should be public. As part of addressing these questions in the context of an archival project for Facebook, the encoded values that underlie Facebook's architecture must be scrutinized in order to determine whose interests are ultimately being privileged and at whose expense and whether an alternate architecture can be proposed that responds more transparently to the underlying normative dilemmas raised by the technical design and existing regulatory gaps. Should social networks be able to archive indefinitely the contents generated by users and acquire default ownership over them? In what way should users be empowered, in terms of ownership and privacy concerns, relative to the online service provider? How should the collective societal interest in the archival of the cultural production occurring on social networks be factored into the equation? Should there be a different approach to "private" as opposed to "public" contents? The analysis of the challenges posed by the archival of social networks exemplifies how the technical malleability of their platforms poses very high stakes if they are not responsive to the normative principles that should guide legal regulation.

3. Why the Library of Congress?

In this section I discuss why the Library of Congress is ideally situated for the public archival of social networks in light of the unique historical role of the Library of Congress in the U.S. and its related deposit requirement; the emergence of a new self-archiving subject engaged in a uniquely democratic and plural construction of cultural memories through novel online processes taking place on social networks; and, the need to counter the danger posed by the escalating privatization of institutions of memory in the context of digital archival projects.

3.1. Brief History of the Library of Congress and the Deposit Requirement

According to the website of the Library of Congress, it is the oldest federal cultural institution of the U.S. and the largest library in the world [14]. The top priorities of the Library include "to acquire, organize, preserve, secure and sustain for the present and future use of Congress and the nation a comprehensive record of American history and creativity and a universal collection of human

knowledge" [15]. This reflects the American Library Association's commitment to advocating for the "value of libraries and librarians in connecting people to recorded knowledge in all forms" ([16], s. 1.3) and is in keeping with the mission of libraries as institutions of memory concerned with the collection and preservation of knowledge for future generations.

The historical development of the copyright system of the U.S. has recognized the importance of preservation and access to knowledge [17]. When the U.S. Constitution states that Congress has the power to "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors, the exclusive Right to their respective Writings and Discoveries" [18], Congress raises the banner of "progress" as the rationale for the enactment of laws to protect copyrights and patents. "[A]s evidenced by the fact that all of the early copyright bills were called "Act[s] to promote learning", the authors of this legislation believed that something greater was at stake" than merely protecting the rights of authors ([17], p. 1025).

Under the current incarnation of the deposit requirement, the owner of copyright (or of the exclusive right of publication) in a work published in the United States must deposit a copy within three months after the date of such publication [19]. Although the deposit requirement, first established under in 1846, "initially served primarily as record evidence of copyright protection, […] the preservation and access attributes of deposit came to be recognized as part of the copyright balance" ([17], p. 1026). Thus, the deposit requirement put teeth into Congress's commitment to the goal of ensuring the collection and access to the cultural production of the past and explains why much of the enormous collection of the Library of Congress consists of works submitted in compliance with the deposit laws and regulations [20].

The historical impetus of the deposit requirement was for the collection to "be complete, without a single omission. We wish for every book, every pamphlet, every printed or engraved production, however apparently insignificant. Who can tell what may not be important in future centuries?" ([17], p. 1026; [21]). This statement, made in 1850, is a good indicator of the democratic and pluralistic spirit of the deposit requirement and points to the unknowable relevance of materials in the future. The phenomenon of social networks in general, and Facebook in particular, was unforeseeable at the time the deposit requirement came into focus as a collection and preservation strategy, but definitely has become an integral part of the cultural and collective palimpsesting of "American history and creativity", the preservation of which is among the main missions of the Library of Congress [15]. As a government institution that plays a leading role in preserving a comprehensive record of American history and counts with the deposit requirement as a unique instrument in fulfilling this goal, the Library of Congress is uniquely situated to accomplish the project of archiving social networks.

3.2. "Archive You": New Self-Archiving Historical Subject

In the past letter writing and diaries have been an important component of how people chronicled their lives and became sources for understanding the way people represented their location in society and their relations to others. As such, their value from an archival perspective has been immense. Nonetheless, the archival of letters and diaries has generally concerned the communications of famous people like political or literary figures. This in part has to do with the fact that writing itself was the prerogative of an educated elite whereas most people were not literate. In contrast, the new forms of public and private expression available on the participatory user-generated platforms of

social networks pose a unique archival opportunity in that they can provide a more democratic and pluralistic landscape of the lives of people throughout history. In this way, social networks pose the possibility of the uncomfortable "permanence" of unofficial and previously ephemeral accounts of significant events [22,23].

What is even more interesting is the "immortalization" of the "insignificant", the intimate and detailed landscaping of people's everyday lives, which does not respond to the strictures of official authorial intent or to a teleological unfolding. The participatory and interactive spaces question the authoritarian notion of authorship in favor of a collectively created reservoir of fleeting emotions, impressions, comments and links that are being recorded at a grand scale for the first time in history ([22], p. 410; [24]). The constant postings can amount to a new form of autobiography, no longer controlled by an ad hoc teleology of a unified voice looking at the past to cohere it into a semblance of order, but rather subject to the "random" and "live" happenings shared through social networks. No longer lost in the rubble of ignored histories, these digital palimpsests can be preserved, distributed and replayed and, ultimately, can alter the historiographical record of the future as well as the boundaries between official and un-official accounts of the past.

Digital memory "collapses the assumed distinction between modern 'archival' memory and traditional 'lived' memory by combining the function of storage and ordering on the one hand, and of presence and interactivity on the other" ([22], p. 410). In a "networked environment, cultural production becomes a form of cultural preservation and social remembering" to the extent that "preservation is being merged into people's ongoing cultural engagements—commercial, civic, and private" [25] even when the purpose of the engagements is not explicitly targeted at preservation. Schnapp has called this participatory process of memorialization "archive you" [26]. Social networks exemplify how people have inadvertently become their own historians through the angst for self-memorialization that preserves the minutest details of living. We "have become pack-rats [a]rchivists are everywhere, official and self-made" [27]. Digital technologies have led to the emergence of the self-archiving subject, who although may individually consider his/her actions in terms of the immediacy of his/her own life and relations, is simultaneously engaged in a process of collective cultural memorialization when he/she documents, comments, narrates, contextualizes, classifies or merely selects contents to upload to social networking platforms.

The emergence of the internet poses new archival challenges for the Library of Congress, not only in terms of the digital incarnation of materials that have been traditionally subject to deposit requirement such as books and periodicals, but more importantly in terms of the historical emergence of this new self-archiving subject engaged in a uniquely democratic and plural construction of cultural memories through novel online processes taking place on user-generated platforms such as Facebook. The archiving of social networks has the potential to democratize the historic and cultural record of humanity given the active participation of previously excluded, silenced or ignored voices such as those of sexual, racial and colonial minorities, who have "posted" their way back into history.

3.3. Privatization of Institutions of Memory

A great challenge for the archiving of social networks is the escalating privatization of institutions of memory in the context of digital archival projects. According to Pessach, the emergence of networked communication technologies is leading to a broadly-conceived privatization of memory

institutions whereby goods provided by the government and other non-profit public-interest institutions are shifting to a market-oriented model. On the one hand, social networking platforms of Facebook and Myspace and other corporate media such as Corbis and Getty Images (for the collection, digitization and licensing of visual works), online music stores (e.g., iTunes) and the Google Library Project, are substituting the social functions of traditional institutions of memory. On the other hand, copyright law and its licensing schemes are changing the "cultural DNA" of traditional institutions of memory ([25], p. 97). In the shift from tangible control of physical cultural objects to the digitization of said works, traditional institutions of memory are now subordinated to copyright usage limitations such as contractual restrictions and technological protection measures included in licensing agreements. The shift is symptomatic of the "viral effect of privatization" and has limited the independence and freedom of traditional institutions of memory ([25], p. 99).

As the "undisputed leader [of] the U.S. social networking market with 166 million unique visitors in November [of 2011]" and more than 845 million active users worldwide as of February 2012 [28], Facebook has already amassed a huge archive, which includes 10,000 times more photos than the Library of Congress [29], in order to offer its "free" web-based social network services. However, there is an inherent contradiction between the democratic, participatory and empowering production by people on content-sharing platforms such as Facebook and the commercial corporate media's reliance on advertising, capacity to censure contents and to make alliances with content owners to limit the incorporation of creative work into user-generated content. The greatest risk of corporate dominance in the field of memory is that "society's landscape of history and culture will be considerably a mirror of corporate media's perceptions and representations 'of' and 'about' the pasts and presents of society" to the extent that "corporate media will focus on preserving mostly its own contemporary raw materials", which "tend to concentrate on particular types of commercial cultural representations [that] do not necessarily reflect a pluralistic wingspan of society at any given time" ([25], pp. 114–15). The potential impoverishment of the historical record at the hands of corporate interests shows the high stakes involved in the call for developing a regulatory framework that promotes a non-profit public interest-oriented approach to conservation.

The Library of Congress, as a public institution whose mission includes the acquisition, organization and preservation of a "comprehensive record of American history and creativity and a universal collection of human knowledge" [15], is in a privileged position to counter the detrimental effects of incidental corporate archiving that can undermine the democratic plurality of the historic record. The Library of Congress is already taking steps in this direction through the archival of public Tweets and a selection of Facebook pages of political candidates [30]. The drawback of these strategies is that they depend on donations and negotiated agreements that entail a piecemeal collection of the historical memory being generated on social networks. This is precisely why in the thought experiment of the Networked Memory Project, the first prong, discussed ahead, explores the possibility of redefining the contours of the deposit requirement of the Library of Congress to encompass "public" communications and postings on social networks, namely those that are visible to all members of a social network such as Facebook. The exercise of considering the extension of the applicability of the mandatory deposit requirement to said "Public" communications addresses whether it would enable a much more comprehensive record of the past for the benefit of future generations.

Nevertheless, even in the context of archiving the "public" communications of social networks it is necessary to consider the need for privacy protection measures, which addressed in the final two sections of this article. And clearly, the privacy challenges are much greater when addressing the possibility of archiving communications that are considered "private". Thus, in order to frame the privacy dilemmas raised by archiving "public" and "private" communications on social networks, it is first necessary to grapple with the socio-legal debates on privacy that propose a networked understanding of privacy.

4. Networked Privacy: The Case for "Public Privacy"?

In this section I explore socio-legal debates that address a networked understanding of privacy in order to frame the privacy dilemmas raised by archiving social networks.

The hegemonic paradigm concerning privacy has been erected on liberal political theory, namely, an atomistic conception of civil society comprised by a sum of autonomous individuals who wield their liberty, rationality and autonomy to assert their interest in having a private sphere protected from the invasions of others and the state. According to Alan Westin, whose influential work on privacy in the late 1960s became the basis for data protection laws in countries of the first world such as the United States and France [31], individuals must restrict surveillance in their struggle for freedom and remain vigilant relative to the implications of technology because it can seriously undermine the "libertarian equilibrium among the competing values of privacy, disclosure, and surveillance" [32]. To the extent that for Westin the more socially interactive the individual becomes, the more his privacy is threatened, the focus becomes the control of information from private to public spaces. The circumscription of the privacy debate to the flow of information means that "privacy is no longer grounded in the social interaction of subjects, but becomes located in the individual's unilateral control over keeping information on the internal side of the boundary" ([31], p. 201). In this way, privacy has been conceived as a right that individuals possess to control information about themselves and to ensure that only the "right people should use the right information for the right purposes" [33]. This conception of privacy leads to its problematic conflation with data protection [34].

Regan and Steeves critique the individualist underpinnings of the liberal theory of privacy. For Regan it is not just the individual that is better off when privacy is protected, but also "society is better off as well when privacy exists" [35]. Privacy "serves not just individual interests but also common, public, and collective purposes" and thus even if privacy became less important to an individual or group of individuals "it would still be important as a value because it serves other crucial functions beyond those that it performs for a particular individual", namely "social interests in privacy" [35]. Steeves deepens the analysis by proposing that privacy does not reside within the constraints of solitude nor procedures to control access to personal information, but rather "it is intersubjectively constituted through social interaction [and] is the boundary between self and other that is negotiated through discursive interaction between two or more social actors" ([31], p. 206). As such, privacy is more than a claim to a collective right and becomes a dynamic process of social construction of intersubjectively negotiated boundaries ([31], p. 193).

The paradigm shift to the "network society", marked by flows of information, capital, technology and symbols, which "are the expression of processes dominating our economic, political and symbolic life" [36], has ultimately lead to the social condition of ubiquitous computing, understood as "the

embedding of networked sensing, calculating, and responsive machines throughout spaces [that] alters both these architectures of visibility and the ability to negotiate the sense and meaning of spaces" ([34], p. 303). The limitations of the traditional privacy model with its neat divide between "activities in a private place [as] private" and "activities in a public place [as] public" ([34], p. 311) are particularly acute under the aegis of ubiquitous computing and its complex processes of identity construction. Protecting privacy as data protection focuses on the "protection from the excesses of administrative management" rather than "facilitating active engagement in the cocreation of the informational/geographic/social landscape" ([34], p. 309). It is why Phillips contends that "[t]he question is not how to protect our privacy; it is how to be public, how to engage in public life, how to figure out one's situation, identity, and desires in community" ([34], p. 313). Rather than lowering the thresholds of privacy or "invading their own privacy", people are engaged in a process of redefining boundaries that still remains to be understood in its full-fledged complexity, opting for invisibility, anonymity and/or re-genderings in certain contexts and greater or lesser visibility in others. Network societies enable users, some with greater expertise than others, to navigate different scales of spatiality and deploy shifting privacy boundaries according to the multiple subject positionalities of their online and offline lives.

From the strictly legal perspective of the privacy torts of public disclosure of private facts and intrusion upon seclusion, disclosure of a private fact turns it into a public fact, which in turn entails no protection for republication [37]. Consequently, under the current legal regime public disclosure precludes privacy claims. For purposes of social networks and user-generated platforms, this either/or legal structure offers no nuances to capture the complexity of the selective ranges of visibility people believe they are engaged in when they share information. Stahilevitz's work is on point here because it explores whether a person has a reasonable expectation of privacy in facts disclosed to a small group ([38], p. 943). Through social networking theory, he argues that a single disclosure should not bar a privacy claim when said disclosure would not have entailed broad public knowledge of the disclosed fact ([38], p. 973). In his examination of the jurisprudence, Stahilevitz is critical of how "what constitutes a "private" matter for the purposes of privacy tort law is not obvious" because the "courts are not being terribly explicit or precise about why particular disclosures waive privacy expectations and others do not" ([38], p. 946).

Similarly, Paton-Simpson contends that contrary to the prevalent privacy law assumption that reasonable people intend to waive privacy rights by appearing in public spaces, "[s]uch factors as the privateness of many 'public' places, dispersion of information over space and time, anonymity, social rules, and the transience of much of what appears in public all contribute to expectations of public privacy" ([39], p. 346) The failure to take precautions should not signify a waiver of privacy to the extent that "public privacy is an important and valuable component of the overall level of privacy for an individual or society" ([39], p. 308). Thus, it can be valid to claim privacy "despite exposure to a large number of people in a public place, if they are all from a particular sub-group in society, such as others of the same sex or people attending a particular church" ([39], p. 323). This claim falls under the rubric of "public privacy" and is clearly useful to capture the nuances of the complex cultural practices taking place on social networks.

According to Gelman, the rigidity of privacy law fails to "capture the value of the blurry edge of […] social networks" ([40], p. 1319), meaning that "one's social network comprises a finite set of

nodes linked by discoverable interdependencies" wherein a person "cannot at any given moment list those people who comprise their social network" ([40], p. 1329). In other words, privacy law cannot assimilate that not all information shared on a social network is meant for the entire world to see. Thus, there is a clear tension between the "aura of privacy" of social networks that suggest "they are for limited disclosure of information to a defined social network of "friends" and the law that "fails to recognize limited disclosures when they occur on a public network" ([40], p. 1329).

Part of the problem lies in that the way users deploy the spatial dynamics of selective visibility can lead to "social convergence."

> The story of social network sites is the story of what danah boyd calls "social convergence." Our social roles are contextual and audience-specific, but when multiple audiences are present simultaneously, it may not be possible to keep up [all] performances at once. […] Facebook performances leak outwards, while facts inconsistent with our Facebook performances leak inwards. The paradox of Facebook is that the same mechanisms that help it create new social contexts also help it juxtapose them. It offers social differentiation but delivers convergence—which its users experience as a violation of privacy ([40], pp. 1177–78).

Thus, the world of ubiquitous computing dramatizes the inevitable tension between the commons generated by the "peer-to-peer individual-empowering ecology" and its endemic potential to become a "privacy nightmare" ([40], p. 1189).

Despite the transgressive and innovative forms through which subjects negotiate being "public" in a world of ubiquitous computing, in the process they are also leaving behind digital debris that includes multimedia communications that they consider "private" within their culturally and socially situated constructions of privacy. In other words, although users of social networks share a lot of information about themselves, not all communications that take place on social networks are considered public by them, irrespective of how users' cultural privacy definitions and technical privacy specifications overlap or conflict with those of legal precedents and/or online service providers' terms of services. Consider that many social networks such as Facebook provide messaging services or e-mail—like spaces where users believe they have greater privacy controls over their communications and, moreover, even in their apparently "public" postings or communications, there are important nuances in their level of "public-ness" according to the platform design and the user privacy controls it enables.

> Some messages that appear to be sent to the world—like Status updates—may in fact be part of a conversation with specific other users. Friendster users used Testimonials to carry out extended personal conversations, even though Friendster also had a private-messaging feature. Facebook's "Wall-to-Wall" feature, which displays the back-and-forth of Wall posts between two users, explicitly embeds this semi-public conversational mode in the site's interface design. The norms of social network sites encourage both relationships and public affirmation of them ([41], p. 1155).

There is a tension between the legal conceptions of privacy and the social and cultural deployment of varying privacy expectations within the scales of spatiality of networked communications, ranging, in some instances, from a high expectation of privacy in emails and what are considered "private" communications within user-generated and content-sharing platforms to lower expectations of privacy

in those spaces considered "semi-public" or "public". This tension becomes even murkier when we mix in the online service providers' understanding of privacy as per their terms of service or user agreements, raising a red banner for the need of legal regulation of online service providers to provide a technical architecture that enables clear choices concerning the level of privacy of the communications that take place and ensure that users understand the implications of the privacy choices they embed in their personalization of the technical design.

The issue is how to empower users' variable expectations of privacy or publicity relative to, or irrespective of, the legal infrastructure and the policies of online service providers.

> Instead of focusing on [social networks such as] Facebook—trying to dictate when, how, and with whom it shares personal information—we should focus on the users. It's their decisions to upload information about themselves that set the trouble in motion. The smaller we can make the gap between the privacy they expect and the privacy they get, the fewer bad calls they'll make ([41], p. 1195; [42]).

Given that "[n]ot everything posted on [social networks such as] Facebook is public, […u]sers shouldn't automatically lose their rights of privacy in information solely because it's been put on [social networks such as] Facebook somewhere" ([41], p. 1141).

Rather than simply adhering to the legal definitions of privacy, I believe that the archival interest in social network communications should focus on the normative empowerment of users relative to how they traced the private/public boundaries in their use of social networks and other user-generated platforms. Accordingly, as part of the theoretical experiment of this article and as further discussed ahead, whereas the first prong of the Networked Memory Project could subject "public" social network communications to the mandatory deposit requirement of the Library of Congress, the second prong concerning the archival of non-"public" communications, meaning all communications that fall below the bar of the "public" setting within the architecture of a social network like Facebook, including postings to a circle of "friends" irrespective of its size, could require an archival strategy that values the discretionary nature involved in sharing contents that are considered more private. In practice, this would mean that the Library of Congress could negotiate with social networks as part of offering people the possibility of donation upon death of a copy of all or some of their "private" communications, which would have to be anonymized, remain unavailable for a period of time and access controlled exclusively for research purposes. This strategy of voluntary donations of non-"public" communications, discussed in the final section, attempts to take into account the cultural ambiguity of how people negotiate the privacy boundaries of their communications and how it is impossible for the technical architectures of social networks to do justice to the intersubjective constitution of privacy.

Although archival efforts must always grapple with legal considerations surrounding privacy, the more difficult and culturally nuanced challenge is to decipher the social and cultural practices of selective visibility and "public privacy" and how they played out in the shifting spaces of network societies marked by ubiquitous computing. In order to further flesh out the implications of this for the theoretical exercise of the Networked Memory Project, it is necessary to discuss the debates surrounding digital death.

5. Digital Death: Legal Limbo for Archival?

Any proposal for archival of social networks for the purposes of historical research and scholarship must grapple with the novel phenomenon of digital death, which stands at the crossroads of the complex property and privacy claims of both corporate online service providers and the heirs of deceased account holders. The magnitude of the implications of digital death is starkly illustrated by the fact that on Facebook alone, Entrustet, a digital estate planning website, contends that approximately 408,000 Facebook users from the United States will die in the year 2011 [43].

The cultural anxiety surrounding the ambiguous status of digital remains left behind upon death, many of which are considered "private" by the heirs, has become increasingly visible on websites that attempt to provide practical assistance such as The Digital Beyond [44], The Death Reference Desk [45], and Death and Digital Legacy [46–48]. Of particular interest are repository services for the digital "legacy" of individuals like Legacy Locker [49], SecureSafe [50], and Swiss-owned DataInherit [51]. Legal thought emerging from the field of trusts and estates has focused on postmortem digital debris as "assets" in need of proper management [43,52,53]. The main thrust of the discussion is marked by a call for "on-line assets [to] be treated in the same way as brick-and-mortar assets" ([43], p. 36) given the relative absence of laws addressing the inheritance of digital remains.

The legal status of digital remains has hardly been addressed in the courts or in the legislative process and this ambiguity plagues the lives of those forced to confront these issues based exclusively on the terms of service of the company concerned. A poignant case in point is that of the family of Justin Ellsworth, a U.S. soldier killed in Iraq in 2004. Upon Justin Ellsworth's death, his father decided that he wanted to create a memorial using the emails his son had written and received while in Iraq ([54], p. 281). However, his family was denied access to his Yahoo! email account because under its terms of service Yahoo! could not disclose the private emails of its users. Specifically, Yahoo!'s terms of service has a section entitled "No Right of Survivorship and Non-Transferability" that states:

> You agree that your Yahoo! account is non-transferable and any rights to your Yahoo! ID or contents within your account terminate upon your death. Upon receipt of a copy of a death certificate, your account may be terminated and all contents therein permanently deleted ([55], s. 27).

In 2005, after the family filed suit against Yahoo!, a Michigan probate judge ordered the company to give the family a copy of the contents of the email account used by Justin Ellsworth [53]. Yahoo! complied unwillingly with the order, making clear that its compliance did not undermine its position over who has the legal title of the account nor its commitment to the privacy and confidentiality of user emails [53]. In this way, Yahoo!'s argument centered on the fact that a user agrees and consents to the terms of service and privacy policy when he creates an account.

The Ellsworth case clearly illustrates the legal limbo of digital remains wherein people assume that the digital contents left behind by the deceased is inheritable intangible property when in fact the "clickwrap" contractual agreement between users and online service providers, as interpreted by courts applying state law, governs by default who owns and inherits digital "assets" ([56], p. 381). The online companies that hold the digital contents of the deceased vary in terms of whether their terms of service include or not clauses pertaining to the fate of an account and its contents upon the death of a user and, more importantly, the on point clauses that do exist vary from one online service provider to another.

Let us turn to examine some of the relevant the terms of service of social networks.

Facebook allows family and friends to report when a person has passed away through an obituary or news article and gives the choice of taking down the profile or "memorializing" the page of the deceased where friends can continue to post on the "wall" or view the profile [57,58]. Facebook tries to factor in privacy concerns on memorialized pages by "set[ting] privacy so that only confirmed friends can see the profile or locate it in search" and by "removing sensitive information such as contact information and status updates" [57]. Although a person "owns" the content, according to Facebook's terms of service, the survivor's of a deceased Facebook account holder will not get a complete copy of the contents generated by the person, but rather can access the memorialized wall and place more posts. All the "private" messages and other content generated by the deceased user that are not contained on the memorialized "public" wall are simply not accessible and it is not clear whether it is "archived" somewhere or deleted. The contents sent by the decedent to his contacts will remain in their pages, but may also disappear upon the eventual death of said contacts.

Myspace's policy states that it "will only remove or preserve the profile of a deceased user at the request of the next of kin (mother, father, spouse, legally registered domestic partner, son, or daughter) or at the request of the executor of estate". Despite Myspace's contention that it "will not allow access or update the log in information for a profile for any circumstance to protect the privacy of the creator of the account", it indicates that "if you have access to the email account tied to the Myspace profile, you can retrieve the password by clicking here" [59]. This is a classic case of mixed signals concerning the alleged inviolability of the privacy of a deceased user. As in Facebook's policy, Myspace does not clarify what happens to all the contents of a deceased account holder, other than his or her profile, and whether the company keeps an archived copy of everything. In contrast, YouTube allows heirs to have access to a deceased user's account and its contents with a power of attorney [60].

According to Twitter's death policy, "[i]n the event of the death of a Twitter user, we can work with a person authorized to act on the behalf of the estate or with a verified immediate family member of the deceased to have an account deactivated" [61]. The privacy policy states that deactivation is said to lead to deletion after thirty days [62]. The policy, however, makes no mention of providing a copy of the contents of the account to heirs of the deceased account holder. Interestingly and to be discussed further ahead, since all public Tweets are being donated to the Library of Congress after a six-month period from emission, a permanent archive of public Tweets is being created, although with limited access for purposes of research. However, it is not clear what happens to the private Tweets upon death without deactivation of an account in terms of whether they are archived indefinitely by the company.

Other online service providers that are not social networks also have variable digital death policies. As we already saws, Yahoo!'s terms of service specifically establishes no rights of survivorship nor transferability of an email account and thus the rights of an account holder perish along with the person. If a family member sends Yahoo! a death certificate, the account may be terminated and its contents permanently deleted [55]. Yahoo!'s privileging of privacy seems to limit its conception of the property aspects of the contents to either one of non-inheritable private ownership by the account holder, unless forced by a court to hand over the contents to a decedent's family, or, alternatively, to one that infers that Yahoo! has de facto ownership over the contents. Another confusion is that the clause does not distinguish between the copyright to the work and the copy of the message. Instead of a transfer of copyright, the terms of service of Yahoo! that terminate rights to the content in an email

account could be interpreted as terminating rights to the copy itself rather than to the copyright ([51], p. 293). It is "somewhat unclear whether the legal status of the copyright is affected when the rights to the account contents are terminated" since "[n]ormally, a copyright owner's exclusive rights do not include preventing the destruction of a copy lawfully obtained [and, c]onversely, the destruction of the copy does not destroy the copyright in the work" ([51], p. 292).

Google's Gmail has delineated a process through which family members might access the email contents of a deceased person, but Google also places emphasis on its concern for the protection of the privacy of users and how, ultimately, the decision will be discretionary [63,64]. It is important to signal that the contents of a Gmail account can be deleted by Google if it has been inactive for more than nine months [65]. In this way, contents can become inaccessible through deletion or a discretionary decision not to fulfill a family's request to acquire a copy of the decedent's emails, which would potentially and by default be deleted after 9 months of inactivity. Hotmail, on the other hand, has a policy whereby family members can acquire a CD with the contacts and email contents of a deceased person [66].

From Hotmail and YouTube that offer mechanisms to give complete access to the contents of the account of a deceased user to Yahoo! that privileges the privacy of the deceased over any other consideration, we see that the property and privacy of the contents created by departed users is contingent upon the variable dispositions of the online service providers with their users, sometimes explicitly contained in, or inferred from, their terms of service or other policy-related sections. The problem is that when corporate online service providers by default acquire ownership in the multimedia communications of account holders, even if it is under the rubric of privacy, they are operating without the proper checks and balances of the different public values that should come into play in such important matters as the privacy and ownership over the digital remains of the deceased and the cultural and social palimpsesting contained therein.

According to Darrow's discussion of emails, given that the "default ownership rules provided by statute or common law may in some cases be modified via private contract," the contractual provisions of the terms of service of online service providers "may potentially modify ownership both of the copyright in the e-mail messages and of the electronic copies of the messages stored by the service provider" ([54], p. 291). Although online service providers can argue that an account holder limited his rights in the copy or the copyrights, "it seems unlikely that either party would intend or expect a copyright transfer from the account holder to the e-mail service provider merely from the terms of use" given that for a copyright transfer to be valid:

> the writing required by 17 U.S.C. § 204(a) must do more than make a general statement that "rights and interests" in the work will be transferred. It is of course possible for the terms of use drafted by e-mail service providers to include language clearly indicating the intent to transfer copyright ownership. Absent such language, however, a court may be reluctant to read into a contract of adhesion the intent to transfer intellectual property rights where such intent is not clearly expressed ([54], p. 293).

The copyright in an email as a probate asset inheritable upon death is especially uncertain when the terms of service establish "No Right of Survivorship and Non-Transferability" such as Yahoo! ([54],

p. 292), However, given that federal law establishes that copyrights are inheritable by will or according to the applicable laws of intestate succession, if the provisions of the terms of service do not

> specifically address the transferability of an account upon death, then even a contract that declares itself not assignable by a party may be assigned to heirs at the death of a party "by operation of law". Assignment to heirs "by operation of law" will likely result unless language prohibiting assignment by operation of law appears in the contract. However, a "personal services contract" is canceled when the death of a party makes performance impossible ([56], p. 384).

As we can gather from the discussion above, emerging legacy services (Legacy Locker and Entrustet, mentioned above), which attempt to fill an as yet legally defined role of digital executor, may in fact violate an online service provider's terms of service such as that of Yahoo! when accessing a deceased user's account to fulfill their wishes.

> Unless the legacy service is working with the online asset providers, it may be a violation of the user's agreement to allow a third party to access an individual's account. Unlike an executor or personal representative recognized by a court or state statute, legacy services do not have legally recognized powers to control an individual's assets. Indeed, even their products are not legally binding because they do not satisfy the requisite will formalities [43].

Moreover, when an individual sets up an account on Facebook or web-based emails services, for instance, he is simply given a license to use the website. The fact that many accounts "are in the form of licenses rather than actual property" means that "these licenses generally expire upon death" [53]. Thus, "whoever receives the usernames and passwords has no legal right to use or access the information contained in the accounts" ([52], p. 306).

One solution proposed by Darrow to deal with the ambiguity of online service providers variable claims over the contents created on their sites has been to use the bailment relationship as a model. When a third party, meaning online service providers such as Yahoo! or Hotmail, is in possession of received or sent messages for safekeeping, "a bailment relationship is created by which the e-mail service provider acquires possession of the e-mail messages while the account holder retains ownership of those messages" ([54], p. 313; [67]). This is a useful suggestion that I believe should be legally required of online service providers not only of email services, but also of social networks. In this way, when a third party, meaning online service providers such as Facebook or Twitter are in possession of contents generated by users, a bailment relationship is created whereby the service provider acquires possession, and the user retains ownership and copyright, over the contents. This scheme would in turn ensure the inheritability of messages.

State legislation is recently emerging that tries to grapple with some of the legal limbo confronted by heirs relative to digital "assets" of a person who has passed away. Specifically, four states have thus far passed legislation: Indiana, Connecticut, Rhode Island and Oklahoma. The Indiana statute is the broadest in that it requires that a custodian or any person that stores a decedent's "documents or information" enable access or provide copies of said contents to the decedent's personal representative [68]. The Oklahoma law encompasses social networks, microblogging and email accounts:

> The executor or administrator of an estate shall have the power, where otherwise authorized, to take control of, conduct, continue, or terminate any accounts of a deceased person on any social networking website, any microblogging or short message service website or any e-mail service websites [69].

Given the qualification of "where otherwise authorized", the legislation would not "appear to grant executors any new powers not already conferred by the contract terms" ([56], p. 385). The Connecticut and Rhode Island legislation are more limited because they apply exclusively to email services [70,71]. A service provider will probably challenge the laws if it considers that it violates the terms of service or if it believes it must not be controlled by Oklahoma law [43]. Relative to service providers that claim ownership over the contents of an account as can be inferred from Yahoo!'s terms of service, it remains "unclear whether an online service provider may stake such an ownership claim in the contents of an online account in its terms of service, or whether account contents subject to such a claim can still be passed through probate" ([56], p. 385). Nonetheless, one position on the Oklahoma law contends that it assumes that an account and its contents are the property of the person who created the account ([52], p. 322). Although the law may conflict with a given online service provider's terms of service, "the real goal of the law is to make people think about the extent of their digital assets and how to properly plan for their disposition" ([52], p. 322). To the extent that the major online service providers have users dispersed throughout the United States, they will eventually tend to adopt terms compliant with the strictest state legislation, which might provide access to accounts and their content for heirs without resolving the ownership issue ([56], p. 386).

Nonetheless, this ambiguity creates a lot of anxiety for the immediate heirs. Building upon what has been discussed above, there could be property claims over the contents such as inheritable ownership and/or copyrights that directly conflict with the contractual terms of the online service providers. And there are privacy questions as to who should be the ultimate arbiter of a person's privacy when he dies without establishing his wishes concerning the deletion or not of his accounts and contents. Although clickwrap agreements have been upheld by the courts [43], they can still be couched as contracts of adhesion wherein the online service provider sets the terms and conditions and the user must accept the terms "as is" by clicking the "accept" button of the terms of service and cannot negotiate more favorable terms.

Upon clicking the clickwrap agreement, was the person consenting to disinheriting his heirs from their ownership and/or copyrights over the contents of his account? Was the person consenting to having the contents of his account deleted in the name of privacy? Were there other alternatives? Most people are not even aware of the terms of the contractual agreements they click their way into and death is an unlikely consideration when creating the many accounts through which people engage in web-based communications and sharing on a daily basis. This raises the question of whether users have actually consented to the online service providers' explicit or inferred terms or, in particular, other policies, not contained in the clickwrap agreement, concerning death. Maybe a person would rather have the online service provider protect his privacy than his nosy or vindictive heirs whom he spent his whole life avoiding. And maybe he would also much rather have had his social network communications or emails go up in digital smoke, some of which perhaps were literary masterpieces or politically or culturally relevant from the perspective of everyday forms of life contained therein, than let those same unworthy heirs have access to, or potentially reap financial benefits from, them. Or

maybe a person would have liked his heirs to have access to his accounts and ownership over their contents, trusting their capacity to protect his privacy or that of others implicated in his communications.

The importance of a staunch defense of the privacy of users such as that of Yahoo! cannot be underestimated. However, under the banner of protecting privacy corporations can embed a default situation that incidentally infers corporate ownership over the contents created by account holders. Are there other alternatives that can navigate the many converging interests without simply delegating the archival of "private" multimedia communications to corporations for whom archival is an incidental aspect of their technical architecture? Presuming to know what the person actually wanted is an ad hoc consideration in the name of the dead, who although may have clicked an agreement, did not necessarily nor effectively consent to all the terms of the agreement and much less to obscure inferences based upon the agreement. Would the person have made other provisions rather than delegate it to the default scenario of a clause in a clickwrap agreement? I believe that a person who wants to delete what he considers are his "private" communications should have the prerogative to do so, be it in life or upon his death. The problem is that under the current legal and technical infrastructure, the boundary between what people are consciously consenting to and what remains beyond the scope of that consent is a problematic and contentious gray area that needs to be clarified in order to empower people to have a say on the fate of what they consider their "private" digital contents.

The preceding discussion of the terms of service of online service providers is a clear example of the Lessig categorizes as code displacing law. Lessig makes an important criticism of the assumption that in cyberspace contract rather than law will regulate people's conduct [72]. For Lessig contracts have a "structural safety check" that courts can calibrate with the "collection of tools that contract law has developed to modify, or soften, the obligations that contract law might otherwise enforce" contrary to cyberspace that has "no equivalent toolbox" and is simply subject to the conditions embedded in the code, which ultimately serve the private interests of the code writer or, in terms of the discussion above, the interests of private corporations such as Google, Yahoo! and Facebook ([6], p. 531). Thus, the obligations of cyberspace are not "conditioned by the public values that contract law embraces" and its encoded values undermine contract law as a "public value" when it entrenches an oxymoronic "private public law" ([6], p. 531). When corporate online service providers by default acquire ownership in the multimedia communications of account holders, even if it is under the rubric of privacy, they are part of the unregulated dynamics of cyberspace that operate without the proper calibrations of the different public values that come into play in the contractual toolbox.

As online service providers automatically and invisibly amass huge amounts of information and multimedia communications, "private" and otherwise, they become an obstacle to the empowerment of people's choices from the bottom up [73]. In order to avoid the collection of information without the users' consent, Lessig proposes that the state clarify the issue of property ownership. He calls for a shift of the legal entitlements wherein people have a property right to the data pertaining to them ([6], p. 520). Yet the legal change will only be useful if it leads to:

> a change in the architecture of the space, and not just in the laws that govern that space. This change in the architecture would aim to reduce the costs of choice, to make it easy for individuals to express their preferences about the use of personal data, and easy for negotiations to occur about that data. Property regimes make little sense unless transactions

> involving that property are easy. And one problem with the existing architectures, again, is that it is hard for individuals to exercise choice about their property ([6], pp. 520–21).

One of the limitations of the emerging state legislations discussed above is that they do not clarify the issue of the property over the information and contents of deceased users in the platforms of online service providers. In general, the state legislations address the issue of access and acquiring copies of the contents accumulated in accounts; which could be used to infer a property right; but inferences are not stable grounds for broader policy concerns surrounding the empowerment of people relative to much more powerful corporate structures.

One approach that has been put forward is to use the legal treatment of private letters as an analogy to explore the property and privacy claims in emails, which can also be extended to forms of communication that take place on social networks or user-generated/content sharing platforms such as "private" messages or "semi-public" postings. Specifically, in his discussion of emails, Darrow proposes that, "[a]s a general rule, the author's rights in her e-mail should be equivalent to her rights in her private letters" ([54], p. 313). This means that upon the death of an intestate author of a letter, that is, a letter left behind without specific instructions as to the disposition of its copyright, the copyright goes to the estate of the deceased author although the letter itself continues to be the property of the recipient ([54], pp. 287, 313). This is because copyright law distinguishes between owning a right to the creative contents of a work and owning a copy of the work [74]. Thus, Darrow proposes that the inheritability of e-mails should be analogous to those of private letters ([54], p. 294).

If the author does not retain a copy of the communication after it has been sent, he "cannot compel the recipient to return them, except possibly on a temporary basis for the purpose of publication. The author retains the "right to publish if he keeps or can procure a copy. But the recipient is not bound to keep the original for his transcription, inspection, or other use" ([54], p. 294). In practical terms, this means that if a person is the recipient of a communication and retains a copy of it, he has ownership over the copy of the communication, irrespective of whether the author deletes his copy or requests that it be deleted upon his death.

From the perspective of the historical archiving of the digital remains left behind by the deceased, the lack of uniformity among the state legislation that is emerging, the variable terms of service of online service providers, the dubious status of ownership and access to the contents left in accounts as well as the highly contentious privacy concerns surrounding the contents, operate to undermine the possibility of acquiring a comprehensive record of the past when it comes to "private" communications taking place through web-based email and social networking or user generated platforms. Moreover, the legislation discussed in the this section is designed to facilitate the process of heirs upon the death of an account holder and does not even remotely consider the broader historical and cultural dimensions of the digital archive being amassed in the hands of private corporations, snippets of which are sometimes handed over to heirs in a piecemeal fashion.

This situation highlights the need for a public policy that not only uses the bailment model, suggested by Darrow, but also requires social networks to include death-related policies in the terms of service to which people would have to acquiesce separately and specifically, indicating whether they would like their contents to be deleted upon death or to be passed on to their heirs. In this way, after the death of an account holder, the corporations would have to make the contents of the account available to the heirs if the account holder did not request deletion upon death. If the heirs do not

request the contents within a certain timeframe, the non-"public" contents would have to be deleted and remain unrecoverable. However, if inherited, the heirs would be able to exercise all their rights over the contents, including ownership of the copy, copyright, privacy.

Nonetheless, even if these steps are taken, important questions remain concerning the historical archiving of social networks such as: When should the empowerment of people over their more "private" multimedia communications give way to an empowerment of a society to have access to the palimpsesting of everyday life that occurs through social networks or other user-generated platforms? When can the "private", "semi-public" or "public" communications belong to the imaginary commons of the cultural and historical memories to which society should have unlimited access and when should they remain within the sphere of the user's understandings of privacy as selective visibility? Should there be a different archival strategy to access the more "public" as opposed to the more "private" digital palimpsesting of daily life taking place? When do multimedia communications cross the line into the "public" sphere, be it because the communication was directed at the world or because the circle of visibility was wide enough to warrant an expectation that the world at large could access the communication and clearly not because the techno-legal regime was faulty? How to draw the line if the very notions of privacy are culturally constructed through intersubjective relations that constantly renegotiate potentially ambiguous boundaries?

The thought experiment I propose to test the limits of the above concerns, which I have discussed briefly in the preceding sections and I develop further in the succeeding sections, is premised upon a hybrid two-pronged strategy for the Networked Memory Project at the Library of Congress wherein: (a) all communications on social networks that are posted under a "Public" setting, meaning that they are visible to all the members of the social network, could be archived through the mandatory deposit requirement, subject to privacy-protection measures; and, (b) all communications that fall below the bar of the "Public" setting, including postings to a circle of "Friends" irrespective of its size, could require another archival strategy that envisions the discretionary nature involved in sharing contents that are considered more private.

6. Copyright Hurdles to the Archiving of Facebook: How to Reconfigure the Mandatory Deposit Requirement?

In this section I discuss the copyright hurdles to the digital archiving of social networks by the Library of Congress, including an analysis of the limitations of the current framework of the deposit requirement, the library exception and the fair use doctrine. Copyright law is at the center of digital conservation concerns given that by definition it requires making copies, distributing and publicly displaying said copies, all of which are exclusive rights of the copyright holder [75]. Thus, the archival of social networks that contain original textual, visual and other materials necessarily implicates copyright law.

Facebook provoked a heated debate with users when the company tried to revise its policies to claim ownership over the contents uploaded by account holders to the site [76]. As a result of the successful opposition of users, Facebook was forced to revise its terms of service once again and they now state that "[y]ou own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings" [77]. Yet said ownership is subject to a non-exclusive, transferable, sub-licensable, royalty-free and worldwide license to use any

intellectual property content a user posts "subject to your privacy and application settings" [77]. The intellectual property license is understood to end "when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it" [77,78]. Thus, the terms of service of Facebook currently establishes that users own the content they generate on the social network, and consequently users also own the copyright over said content, but subject to certain limitations [79,80]. Let us examine the implications of Facebook's terms of service relative to the deposit requirement.

The existing contours of the deposit requirement make an important distinction concerning the deposit requirement of works in the Library of Congress based upon whether the work is considered published or unpublished. As a result, I first put forward the definition of publication, the statutory definition of which was first provided in the 1976 Copyright Act:

> "Publication" is the distribution of copies or phonorecords of a work to the public by sale or other transfer of ownership, or by rental, lease, or lending. The offering to distribute copies or phonorecords to a group of persons for purposes of further distribution, public performance, or public display, constitutes publication. A public performance or display of a work does not of itself constitute publication [81,82].

Relative to published works, the deposit requirement states that the owner of the copyright (or of the exclusive right of publication) in a work published in the United States must deposit a copy or phonorecord (in the case of sound recording) within three months after the date of such publication [19]. The required deposit, however, is not a condition for copyright protection. More provisions were incorporated to the Code of Federal Regulations to address electronic works and their status relative to the deposit requirement [83,84]. The Code of Federal Regulations specifies that electronic works published in the United States and available only online are exempt from the deposit requirement [85]. Said exemption includes "electronic serials" such as periodicals, newspapers, annuals, and the journals, proceedings, transactions, and other publications of societies that are "issued on an established schedule in successive parts bearing numerical or chronological designations, without subsequent alterations, and intended to be continued indefinitely" [86]. However, the language of the Code of Federal regulations is ambiguous given that the exemption of electronic works from the deposit requirement is said to last "until such time as a demand is issued by the Copyright Office" [85], which clearly is leaving the door open to future legislation or regulations that could require the deposit of electronic works in the Library of Congress.

Although electronic works are currently exempt from the mandatory deposit requirement, section 202.24 of the Code of Regulations states that at anytime after publication the "Register of Copyrights may make written demand to deposit one complete copy or a phonorecord of an electronic work published in the United States and available only online upon the owner of copyright or of the exclusive right of publication" subject to the conditions that: (1) the demand for electronic works be for categories identified as electronic serials, previously defined; and, (2) the demand is for works published on or after 24 February 2010 [87].

Section 407(e) of the law that regulates deposits in the Library of Congress addresses the deposit of unpublished audiovisual and radio programs. Specifically, relative to transmission of audiovisual and radio programs that have been fixed and transmitted to the public in the United States but have not

been published, the library of Congress is permitted to either: (1) make a fixation of a transmission program directly from a transmission to the public, and to reproduce one copy or phonorecord from such fixation for archival purposes; or, alternatively; (2) make a written demand, upon the owner of the right of transmission in the United States, for the deposit of a copy or phonorecord of a specific transmission program [88]. Furthermore, the Code of Federal Regulations that interprets section 407(e) states that "[a]dditionally, the Library will record a selected portion of unpublished Internet, cable and satellite programming transmitted to the public in the United States" [89].

In sum, the current state of the law and regulations concerning the deposit of electronic works and internet programming in the library of Congress is: (1) electronic works that are considered to be published are exempt from the mandatory deposit requirement, but can nevertheless be subject to a discretionary written demand for the deposit of a copy; and, (2) a selected portion of internet audiovisual and radio programming that is considered to be unpublished will be recorded.

How does a social network like Facebook fit within the existing framework of the deposit requirement? From a strictly legal standpoint, the main question is if the contents produced by users on social networks qualify to be considered as electronic works. Even if the deposit of published electronic works were mandatory, there are important drawbacks to the Library of Congress' definition of electronic works that would limit its archival capacity for social networks. In particular, "electronic serials" (e.g., periodicals, newspapers, annuals and journals) that may be subject to discretionary written demands for deposit must be "issued on an established schedule in successive parts bearing numerical or chronological designations, without subsequent alterations, and intended to be continued indefinitely" [86]. This definition of electronic works replicates the brick and mortar model of fixed and final print publications that are published on a regular schedule. To the extent that "new forms of non-fixed informational materials such as websites" ([25], n. 210) are excluded from the definition of electronic works, a broad swath of internet production will remain outside the purview of potential archival, including user-generated contents on social networks [90].

Part of the challenge to the definition of electronic works lies in that, despite the fact that users on Facebook own the contents they produce, the interactions occurring on social networks speak of a process of collective non-linear authorship. This implies that the contextual space of how each individual's postings are inscripted in a broader dialogue is lost from the legal perspective of individual authorship and ownership. The cultural mapping of their postings loses much of its value in the absence of the dialogic space through which meaning is constructed and negotiated. From the perspective of the integrity of the archival record, the isolated and piecemeal recovery of decontextualized individual postings undermines the possibility of acquiring a comprehensive record of the palimpsesting of everyday life taking place on social networks.

If the archiving of social networks cannot be achieved through the mandatory deposit requirement (nor the library exception nor fair use, discussed ahead), there would be very high transaction costs involved in archiving the digital remains of networked societies given the chaotic licensing scheme that would have to be devised to keep the dialogic integrity of the user-generated communications on social networks. Even if we extend Darrow's analysis of emails to social networks, the transaction costs for digital archiving would still be insurmountable. As already discussed, Darrow uses the legal treatment of private letters as an analogy to explore the property claims in emails. The copyright of a letter belongs to the author, but the letter itself becomes the property of the recipient ([54], p. 313).

Applying this proposition to social networks, users would be the owners and copyright holders of their posts, but also owners of their "copy" of the postings and messages they receive from others. The dialogic integrity of the interactions could hypothetically thus be preserved, although with several drawbacks. The individual user would be able to license or donate the contents over which s/he has copyright and sell or donate her/his "copy" of the contents received from others, which does not resolve the potential licensing and purchase costs and which also has different implications in terms of the accessibility to the public given that the contents of which the user merely owns a "copy" would still be subject to the copyright of the original author. On the other hand, waiting for materials generated on social networks to enter the public domain is also problematic and highly ineffective as an archival strategy. Upon hypothetically entering the public domain, most of the digital archive of a given period would probably already be lost in the wake of the contentious interplay of the property and privacy claims of corporate online service providers and the heirs of deceased account holders.

Although social networks do not fit into the current definition of electronic works for purposes of the deposit requirement, let us assume that they could fit if the requirement is redefined and move to a consideration of whether the contents produced by users on social networks qualify to be considered a publication. According to the definition of publication cited above, this is not the case given that there is no transfer of ownership or possession of the contents to the public and, as a result, neither the social networks nor its users could be subject to the deposit requirement for published works. Part of the problem lies in the legal definition of publication for purposes of the deposit of published works as it is applied to electronic publications. When is an electronic work considered published? When does the public display of a website become a publication? Websites, including social networks and blogs, are distributed to the public when displayed on the internet, but does said distribution occur "by sale or other transfer of ownership, or by rental, lease, or lending" [81,82]. According to the definition of publication provided above, in and of itself, a public display, without the sale or other transfer of possession of a copy, does not constitute publication. This definition of publication is incapable of encompassing the vast and constantly shifting forms of internet communication to which the public can have unlimited access without the transfer of ownership or possession of any tangible copies. To the extent that the free display of informational materials on the internet does not transfer ownership or possession to the viewers, said digital works would not be considered publications subject to the deposit requirement.

It is not even clear if the "electronic serials", currently subject to discretionary deposit demands as published electronic works, would all actually comply with the legal rubric of a publication if there has not been an actual transfer of ownership or possession of said electronic works. In the case of a copy of an electronic work that is given freely as a gift, there would be a transfer of ownership in that copy, which would amount to a publication. Yet, in some instances at the very least, the Library of Congress may be stretching its understanding of publication in order to encompass certain electronic works defined as "electronic serials" that resemble closely the physical publications it has historically subject to the deposit requirement.

One possible strategy to broaden the scope of the deposit requirement to encompass social networks is to interpret more generously the second sentence of the statutory definition of publication: "The offering to distribute copies or phonorecords to a group of persons for purposes of further distribution, public performance, or public display, constitutes publication" [81]. The Committee Reports specify

that the purpose of the second sentence is to make "clear that when copies or phonorecords are offered to a group of wholesalers, broadcasters, motion pictures, *etc.*, publication takes place if the purpose is "further distribution, public performance, or public display" [91,92]. New technologies have enabled everyday users of the internet to inadvertently fulfill the role of "further distribution, public performance, or public display" when they constantly post links to, or embed, the informational materials available on the internet in blogs, social networks and other digital platforms. Distribution on the internet is not inevitably linked to traditional intermediaries (e.g., wholesalers and broadcasters) for further distribution. Based on the unprecedented agency of internet navigators to further distribute informational contents, the public display of freely available websites and other informational contents and spaces on the internet could fulfill the publication requirement for deposit. By limiting this broad interpretation of publication to the display of freely available informational materials on the internet, contents that are available for a price such as through sale or rental would remain subject to the traditional definition of publication.

It could also be argued that posting contents on social networks constitutes publication by way of transfer of ownership of a copy of the contents to the public. Whereas in the context of a letter or email addressed to one person, there can be no claim to publication, the complexity of the technical architecture of social networks makes feasible a publication claim. Facebook enables varying levels of visibility of contents posted by users according to the privacy settings they deploy, namely: (1) When a user posts content to the "Public" in Facebook (hereinafter referred to as the "Public setting" or "Public"), said post is visible to anyone on the network; (2) If content is posted to "Friends" in Facebook (hereinafter referred to as the "Friends setting" or "Friends"), the materials posted are only visible to the list of friends of the account holder. Pushing even further Darrow's analogy of letters to emails [54], the argument would be that on social networks both instances, that is, posting contents to the "Public" and "Friends" settings, constitute publication by way of transfer of ownership of a copy of the contents to the public.

However, privacy concerns raise big red flags here. As already discussed, the inability of the existing legal scheme of privacy to grapple adequately with the nuances of the culturally negotiated boundaries between public and private, should not hinder the ability of an archival strategy of social networks to take into account the forms of privacy in public (or "public privacy") that are symptomatic of how people interact within the technical architectures of a social networks. Thus, in order to be respectful of the practices of "public privacy" deployed by many users who post under the "Friends" setting, the presumption of publication on social networks such as Facebook could be limited exclusively to the "Public" spaces and postings for the purposes of the mandatory deposit requirement.

If users of social networks are the copyright owners of their postings and we assume, extending Darrow's analysis of emails to social networks [54], that there is a collective and mutual transfer of ownership in the copies of all postings sent via the Public setting, the landscaping of everyday life that occurs on the Public spaces of social networks could be subject to the deposit requirement of the Library of Congress. This would enable the archiving of a broad part of the communications taking place on social networks without infringing unduly on those communications that users may consider as more private such as those posted to their circle of "Friends" or the messages sent within messaging or e-mail-like services of social networks.

Another strategy for the archiving of social networks under the deposit requirement is simply not to require publication for the deposit of publicly displayed and freely available informational materials on the internet, including social networks, similar to Section 407(e) that regulates deposits of unpublished audiovisual and radio programs, under which the Library can make a fixation or, alternatively, request that the owner deposit a copy [88]. Nonetheless, irrespective of which strategy is pursued to broaden the deposit requirement in this article's thought experiment, all communications that fall below the bar of the "Public" setting should not be subject to the mandatory deposit requirement and should instead require another archival strategy that envisions the discretionary nature involved in sharing contents that are considered as more private.

In the case of Facebook, as already discussed, the terms of service establish that users own the copyright to the content they generate and the social network has a non-exclusive license to use the contents posted subject to the privacy settings of an account holder. The users as owners of the copyright over their contents would be subject to the deposit requirement whereas the social network would not since it was not granted an exclusive right of publication, but rather a non-exclusive license. However, contrary to this disposition, the dilemma arises as to who should carry the onus of complying with the mandatory deposit requirement of the "Public" spaces and postings of a social network such as Facebook. Should it be placed on the company rather than the individual account holders? I believe that Facebook is more efficiently situated to comply with the technical complexities of fulfilling the deposit requirement given the collective and multimedia nature of the communications taking place on Facebook.

In the absence of a deposit requirement for the archival social networks under the existing copyright framework, I briefly turn to an analysis of the library exception and the fair use doctrine. For purposes of the archival of social networks, the current statutory library exception to copyright holders' exclusive rights neither covers digital archiving nor contemplates the "nature" of a social network as constituting a "work" subject to the exception. Section 108 for libraries [93], concerned with outlining limited exceptions that allow copying for preservation purposes that would not substitute the commercial sale of works, only applies to materials owned by the library and only allows the use of digital copies within the library premises. Thus, the archival interest in social networks clearly falls beyond the scope of the Library exception.

The library exception also establishes that if a library's activities do not qualify for the section 108 exemption, they may still qualify as fair use [93]. The doctrine of fair use allows the use of copyrighted materials without requesting permission for certain purposes considered crucial to free speech such as news reporting, criticism, teaching, scholarship or research. Congress has put forward four non-exclusive factors for the determination of whether a use is fair or not, namely, the purpose and character of the use (e.g., commercial/nonprofit educational use, transformative use or not); the nature of the copyrighted work (e.g., fictional or not; published or unpublished); the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and, the effect of the use on the potential market of the copyrighted work [94]. The problem lies in the uncertainty of whether the fair use doctrine would serve as a reliable defense to copyright infringement claims against the digital archiving of social networks given the unpredictable outcomes of the fact-specific court opinions on fair use. Nonetheless, we can tentatively predict that an archive of social networks at the Library of Congress that, one the one hand, has a non-profit educational purpose and does not

impact the market of the copyrighted works by limiting access for purposes of historical academic research would favor a fair use defense whereas, on the other hand, is either a complete copy or a substantially large copy of the social network as a whole (e.g., only encompassing the public portion of contents posted to the network) and includes a considerable amount of unpublished and fictional materials of many authors would definitely undermine a fair use defense.

In sum, neither the deposit requirement, the library exception, nor the fair use doctrine provide stable legal grounds for the protection from copyright infringement claims aimed at the archival of social networks. As a result, there is a gaping absence in the archival work of the Library of Congress given how new technologies have revolutionized communications in every field and online forms of expression are born and remain exclusively digital.

7. Alternative Internet Archiving Efforts at the Library of Congress

In this section I explore alternative internet archiving efforts currently underway in the Library of Congress that do not fall under the umbrella of the mandatory deposit requirement, the library exception, nor fair use. A pilot web archiving project of the Library of Congress began in the 2000 presidential election and eventually became a "permanent fixture of our national archives" with five full-time staff members that use an open-source web crawler called Heretix to capture portions of the internet for the benefit of future generations [95]. Part of the challenge is the selections process of what to archive, particularly given that there is no clearly bounded space that can be identified as the "U.S. web" [95]. Thus far, the selection process has focused on five areas of internet archival:

(1) Twitter feeds—After the Library of Congress expressed to Twitter its interest in preserving public Tweets, Twitter decided to "donate access to the entire archive of public Tweets to the Library of Congress for preservation and research" [96,97] The tiny percentage of Tweets that are protected will not be available as part of the donation to the Library [96]. Part of the dilemma was the manner of access to be given to the public Tweets such as a "more of a researcher, data mining-type access to it" [95,98]. According to the Twitter blog, the arrangement establishes that only after a six-month delay can the tweets "be used for internal library use, for non-commercial research, public display by the library itself, and preservation" [95,96]. In an official audio communication of the Library of Congress, the exact nature of access to be given to the Twitter collection is seen in terms of data-mining and algorithms for the purpose of research rather than giving general access to the tweets of a specific individual [99]. For instance, the Twitter archive can be of sociological and historical value to determine the mood of people in reaction to major news events and, as such, access could be given based on a block of time relative to a specific event [99].

(2) Selection of a few Facebook pages—The Library has asked political figures such as candidates or congress people for permission to archive their Facebook pages because the content of the Facebook page is "actually owned by the site owner who put it up there" [95]. Thus, contrary to Twitter with whom the Library has achieved a deal to have the public Tweets donated to the Library of Congress, the archival of selective Facebook pages is at the discretion of the political figures approached. Although I was unable to access more specific information on the manner of accessing the archived Facebook pages (*i.e.*, whether it would be accessed by the

public in general or for research purposes alone), according to Kessler, "unless you're a national election candidate who has given permission, you probably don't have to worry about your grandchild stumbling across an embarrassing Facebook photo while doing archival research for his or her college thesis" [95]. This would seem to imply that access to the archived Facebook pages would be limited to research purposes.

(3) Internet presence of national election candidates—The archives of the internet presence of national election candidates includes presidential, congressional and certain overseas elections [95].
(4) Websites on notable historical events—The Library has archived websites on notable events such as September 11, Iraq war and hurricane Katrina [100].
(5) News sites and blogs that give permission—Since the library of Congress does not have a legal mandate to preserve the web, it must acquire permission to archive news sites and blogs that make a profit off of their content [95].

The Library of Congress's archival of Twitter's public Tweets and select Facebook pages of political figures raise several privacy questions concerning the archival of contents generated on social networks.

First, upon archival at the Library of Congress, are and should steps be taken to protect the identities of Tweet "Followers" and Facebook "Friends" that may appear or can be deduced from the archived materials? In terms of the archival of public Tweets, will the data pertaining to "Followers", meaning users who subscribe to other user's Tweets, be available and how it will be available to researchers [101,102]? But even if the information of "Followers" is not available, a "Follower" who responds to a Tweet without the proper privacy controls could potentially be identified [103,104].

An examination of different Facebook pages of politicians and the instructions concerning their creation in Facebook [105] revealed that the pages vary in terms of the features used in their design; for instance, some pages allow people to become "Friends" [106] and post comments whereas others just allow people to subscribe or indicate that they like a page, without becoming "Friends". Each of these instances raises privacy concerns in terms of the scope of the archival of the Facebook pages at the Library of Congress. Does the archival include, make visible and available for research the identity of the "Friends", subscribers or likers of the archived page? In the case of "Friends" who posted comments to the Facebook page, do they appear on the archived page irrespective of the privacy settings of the post, namely, if it was posted just to the circle "Friends" or to "Public"? Will the public posts of Friends of the political figure's Facebook page be anonymized? Does it make sense to speak of Friends being politically "outed" by revealing their public posts in an archival setting? Does the fact that they were "Public" posts within the confines of Facebook's privacy settings make them unworthy of privacy measures to protect the identity of the person who posted? If the privacy setting of the posts to a public figures' Facebook page was "Friends", does this signal a greater concern by the user to protect the privacy of his or her posts? Should the archival of Facebook anonymize posts on archived pages, irrespective of whether the privacy settings of the posts were "Public" of "Friends"?

The Library of Congress' archival of public Tweets can be from people who are or are not public figures whereas the archival of public Facebook pages is of people who are thus far public figures. Beyond the privacy consideration of "Followers", should Tweeters that are not public figures be anonymized in the archive in order that the protection of privacy to be the default social value undergirding the design of the archive? Part of the challenge is defining the scope of what constitutes a public figure, particularly given how new technologies have altered the scope of visibility of people

who in the past would not have been considered public figures. Nonetheless, given that the research usefulness of the archived social network materials is seen in terms of data-mining and algorithms rather than the identification of specific individuals [99], anonymization, with the exception of public figures, of the archived materials of social networks would be consonant with this approach and could operate as a normative principle that undergirds archival.

In both the Twitter and Facebook instances the communications to be archived were available to members of the public before archival, but that public must be delineated more clearly in each case. The Facebook materials of the political figures archived at the Library of Congress are pages, distinct from personal profiles (timelines) and groups [107]. Pages "allow real organizations, businesses, celebrities and brands to communicate broadly with people who like them" and "[p]age information and posts are public and generally available to everyone on Facebook" [107]. In the case of Twitter the public Tweets were also available to all the members of Twitter and not just "Followers" of specific Twitter feeds [103]. The Twitter website explains that Tweets are "public by default".

> If your Tweets are public, anyone who runs a search for a keyword in your Tweet may be able to see that message. Your Tweets are public by default; if you're hesitant to have strangers read your updates, protect your Tweets to approve followers and keep your updates out of search.

However, there is a free online Twitter archive search service called Topsy that allows anyone on the web to search public Tweets up to May 2008 [108,109]. Thus, despite the non-commercial research-based limitations to access Tweets at the Library of Congress, the Topsy service is open to all. Whereas an account holder concerned about privacy must delete public Tweets before the six-month period after emission to avoid their archival at the Library of Congress, it is unclear if the same applies to Topsy.

Second, who will have access to the archived materials of social networks? In the case of Tweets, it is clear that the donation by Twitter is conditioned upon a model of limited access for non-commercial research purposes, but, as just mentioned, the public Tweets are actually accessible online by anyone through the search service Topsy [110]. In the case of Facebook pages that are archived based on individual negotiations with the account holder, it is not clear what the terms of access are and if they are variable, despite the indication that it would appear to be for research purposes. In general, the current scheme of the Library of Congress lacks clarity concerning the availability and accessibility to the electronic works that are deposited in the Library [111,112].

Third, how long should the social media materials archived by the Library of Congress remain unavailable or what some have termed as dark? In the case of Tweets, the Tweets will not be accessible at the library of Congress until after a period of six-months. Relative to Facebook pages, it is not clear if there is a time lapse in terms of their availability for research. Despite the public nature of the Facebook pages archived, a period of darkness of the social media materials can be instrumental in allaying certain angles of privacy concerns such as a guaranteeing sufficient time to ensure proper anonymization of "Friends" who posted contents on the archived page, irrespective of their specific privacy settings on the social network and the limited legal scope of privacy protection.

Fourth, whereas the Facebook pages archived are based on individual arrangements with the political figures involved, the public Tweets archived were the result of the Library of Congress's

negotiation with the Twitter company that decided to make an ongoing donation to the Library. This raises the issue of the scope of the consent given by Twitter users to Twitter upon becoming account holders and consenting to the terms of service. It can be argued that eternal archival goes beyond the scope of consent.

Fifth, conflicting privacy legal regimes come into play in the context of social networks such as Facebook and Twitter given the transnational nature of their use ([102], p. 166). The archival of these social networks at the Library of Congress in the U.S. must take into account that it includes Tweets generated by people from other countries or regions, including for instance, the European Union and Canada, which have more stringent privacy controls than the U.S. The official information on the agreement between Twitter and the Library of Congress simply mentioned the archival of all public Tweets without making any reference to the exclusion of non-U.S. Tweets.

The existing scheme for the archival of social networks at the Library of Congress is thus problematic at many levels and the issues raised by these initial efforts are relevant to the discussion of a broader archiving strategy for social networks such as Facebook, namely, beyond the archival of public Facebook pages of political figures.

8. Networked Memory Project: A Thought Experiment

In this section I explore the thought experiment of forming the Networked Memory Project at the Library of Congress, through a hybrid two-pronged strategy, wherein: (a) all communications on social networks that are posted under a "Public" setting, meaning that they are visible to all the members of the social network, could be archived through the mandatory deposit requirement, subject to privacy-protection measures; and, (b) all communications that fall below the bar of the "Public" setting, including postings to a circle of "Friends" irrespective of its size, could require another archival strategy that envisions the discretionary nature involved in sharing contents that are considered more private.

In order to set the stage for the discussion of the Networked Memory Project thought experiment, I will give a brief recap of what could be legally required of, and technically embedded by, social networks as discussed in, and derived from, the preceding sections:

First, it could be legally required for online service providers to provide a technical architecture that enables clear choices concerning the level of privacy of the communications that take place and ensure that users understand the implications of the privacy choices they embed in their personalization of the technical design.

Second, as per Darrow's suggested solution to the ambiguity of online service providers' variable claims over the contents created on their sites, the bailment relationship could be used as a model. When a third party, meaning online service providers such as Facebook or Twitter are in possession of contents generated by users, a bailment relationship is created whereby the service provider acquires possession, and the user retains ownership and copyright, over the contents ([54], p. 313; [113]).

Third, social networks could include death-related policies in the terms of service to which people would have to acquiesce separately and specifically, indicating whether they would like their contents to be deleted upon death or to be passed on to their heirs. This would be analogous to a living digital will.

Fourth, after the death of an account holder, the corporations would have to make the contents of the account available to the heirs if the account holder did not request deletion upon death. If the heirs

do not request the contents within a certain timeframe, the non-"Public" contents would have to be deleted and remain unrecoverable. However, if inherited, the heirs would be able to exercise all their rights over the contents (e.g., ownership of the copy, copyright, privacy).

Fifth, online service providers of social networks would be prohibited from incidental and indefinite archiving of, and acquiring default ownership over, the communications generated on their platforms, except for the limited purposes of technical functionality.

Now I can turn to a discussion of some of the specific contours of the Networked Memory Project thought experiment.

8.1. First Prong: Mandatory Deposit of "Public" Communications

The first prong of the Networked Memory Project at the Library of Congress could explore redefining the scope of the deposit requirement to encompass the cultural palimpsesting that is taking place on social networks as a central element of the U.S. experience worthy of preservation for future generations. Here are certain aspects of how the deposit requirement might work.

- The deposit requirement would only apply to the communications on social networks that are posted under a "Public" setting, meaning that they are visible to all the members of the social network as in Facebook.
- In consideration of conflicting transnational privacy regimes, the mandatory deposit would only apply to contents generated within the U.S. Despite the "Public" character of the contents generated, there would also be several additional privacy protection measures, exceptions or loopholes to give flexibility to the mandatory deposit requirement as applied to contents generated in the U.S.
- There should be an opt-out option for people that did not understand the privacy implications of posting under the "Public" setting (e.g., when an account holder had his or her default privacy setting to "Public" rather than "Friends"). Despite the fact the an optout "solution" is generally considered to be a weak form of privacy protection, this strategy can provide some minimal protection in the context of opaque privacy architectures of social networks with changing default settings that may confuse users as to the actual level of visibility of their communications on social networks. However, creeping public defaults wherein, for instance, content that may have been originally private becomes public without the knowledge of users should be excluded from the deposit requirement.
- Although complete anonymization will be very difficult with this kind of social data, all the "Public" archive should nevertheless be anonymized and remain invisible or dark for a period of time, with the exception of public figures.
- Precisely given the difficulty of ensuring an effective anonymization and the possibility of unwitting "Public" postings for which users may not have requested the opt-out option, the access to the archive should be limited to research purposes and not be open to the public in general.
- Example of the archival of an exchange between two account holders who are contacts in a social network, one of whom has his privacy setting as "Friends" and the other as "Public": Only the "Public" sections of the exchange would remain visible within the archive. Here the privileging of the privacy choices of the users trumps the completeness of the "Public" archive.

- The onus of complying with the mandatory deposit requirement of the "Public" communications on a social network would be placed on the company rather than the individual account holders. Facebook, for instance, is more efficiently situated to comply with the technical complexities of fulfilling the deposit requirement given the collective and multimedia nature of the communications taking place on Facebook.

This scheme of the first prong of the thought experiment attempts to preclude default corporate ownership over the broad cultural landscaping occurring through social networks or other or user-generated platforms while simultaneously empowering the privacy choices made by users and enabling archiving efforts that have a non-profit public-interest approach. Thus, normative values concerning privacy necessarily call for enabling a techno-legal architecture of loss and the consequent incompleteness of the social networks' archive amassed.

8.2. Second Prong: Voluntary Donations of Non-"Public" Communications

Given the inevitable indeterminacy of how people cross-culturally and diachronically negotiate the boundaries around their communications and try to deploy "contained" spaces or nodes of communication, it is impossible for the technical architecture of social networks and other user-generated platforms to do justice or even remotely resemble the shifting, contradictory and multiple character of the selective strategies of visibility of peoples' privacy practices. This cultural ambiguity calls for an archival strategy that errs on the side recognizing forms of "public privacy" and explains why the proposed second prong of the thought experiment for the archival of social networks at the Library of Congress could explore requiring a different archival strategy that envisions the discretionary nature involved in sharing contents that are considered potentially more private, namely, all communications that fall below the bar of the "Public" setting, including postings to a circle of "Friends" irrespective of its size.

In this context, the Library of Congress could negotiate with social networks to enable users, as part of the death policy agreements, to be given additional choices regarding the possibility of donation upon death of a copy of all or some of their communications that fell below the bar of "Public". The individual "Private" archive should be anonymized and remain dark for a period of time that would be more extensive when compared to the "Public" archive. Alternatively, in the case of social network communications that form part of the estate of the deceased without the arrangement of a prior donation to the Library of Congress, the archiving strategy would have to be the same as those utilized before the digital turn of society, namely, requesting donations from, and/or making contractual arrangements with, the heirs of the deceased. Similar to the "Public" archive and given the sensitive nature of the "Private" archive, access would have to be limited to research purposes.

All the materials donated under this discretionary scheme of archival should be subject to the protocols for protecting privacy developed by the archiving profession. Archivists are in tune with the sensitive nature of "private" materials, particularly given how heirs and executors have burnt, destroyed and controlled access to private letters and papers as part of their attempt at "engineering history" [114]. Archivists thus "fear the smell of burnt letters" ([115], p. 313, n. 176) and are in a privileged position to understand the stakes involved in trying to rescue for future generations the "private" digital landscaping that is taking place on a daily basis.

Section VII of the Code of Ethics of the Society of American Archivists' specifically states that

> Archivists recognize that privacy is sanctioned by law. They establish procedures and policies to protect the interests of the donors, individuals, groups, and institutions whose public and private lives and activities are recorded in their holdings. As appropriate, archivists place access restrictions on collections to ensure that privacy and confidentiality are maintained, particularly for individuals and groups who have no voice or role in collections' creation, retention, or public use. Archivists promote the respectful use of culturally sensitive materials in their care by encouraging researchers to consult with communities of origin, recognizing that privacy has both legal and cultural dimensions ([116], s. 7).

Archival interest in "private" multimedia communications of social networks can focus on the normative empowerment of users relative to how they traced the private/public boundaries in their use of web-based emails, social networks and other user-generated platforms while simultaneously weighing in the public interest in preserving the digital remains. In this way, archivists can go beyond legal considerations and technical design inadequacies surrounding privacy in order to grapple with the difficult and culturally nuanced challenge of deciphering the social practices of "public privacy" and how they played out in the shifting spaces of network societies marked by ubiquitous computing. Moreover, they can carefully gauge the obsolescence of privacy considerations with the passage of time, taking into consideration, for instance, the death of all the people involved in the digital remains.

This article shows that U.S. copyright laws are much more effective than privacy laws at blocking archiving efforts of the digital palimpsests left behind by the deceased [117]. The existing technical architectures replicate this hierarchy of protection of copyright over privacy given, for instance, the contrast between the extensive deployment of DRMs to protect copyrights as opposed to the broad incidental and unquestioned archiving of "private" multimedia communications on social networks by corporations. As a result, whereas copyright law is particularly anachronistic and inhibitory to archiving projects, the legal privacy framework of privacy is not sufficiently nuanced to accommodate the complex scales of visibility deployed by people on social networks. This state of affairs poses huge challenges for a non-profit public-interest archiving project such as that of the Library of Congress to have, on the one hand, easy access to copyrighted materials while, on the other hand, affirmatively defending an architecture of partial loss that empowers people's intersubjectively constituted privacy boundaries. The theoretical experiment of the Networked Memory Project for the archival of social networks by the Library of Congress is thus premised upon a techno-legal architecture of loss and, ultimately, only the possibility of partial recovery, through archival efforts that build upon a two-pronged strategy for the mandatory deposit of the "Public" communications and voluntary donations of non-"Public" communications. Although this theoretical exercise may have raised more questions than it answered, the proposed strategy attempts to push forward the discussion of some of the salient questions of an archival project of this nature in a way that could potentially be more comprehensive in scope and more protective of privacy than the existing scheme of archiving social networks at the Library of Congress.

Conflicts of Interest

The author declares no conflict of interest.

References and Notes

1. Danah M. Boyd, and Nicole B. Ellison. "Social Network Sites: Definition, History, and Scholarship." *Journal of Computer-Mediated Communication* 13 (2007): 210–30. Available online: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html (accessed on 23 July 2014).
2. Social networks are "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system; (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system" [1].
3. Andrew Lipsman. "State of the U.S. Social Networking Market: Facebook Maintains Leadership Position, but Upstarts Gaining Traction." *comScore* (blog), 28 December 2011. Available online: http://blog.comscore.com/2011/12/state_of_the_us_social_network.html (accessed on 23 July 2014).
4. This study showed that Twitter was in the second position with 35.4 million unique visitors and Linkedin in third place with 35 million. In addition, the study showed how the use of Myspace had been steadily decreasing and only had 24,969 million users as opposed to Facebook that had 166,007 million users as of November 2011. As a result, Facebook is the focal test case of the article because no other social network can currently compete with it in the U.S. Nonetheless, the analysis of Facebook as a worthy object of archiving efforts applies equally to Myspace, particularly given the obsolescence of Myspace relative to Facebook and the potential loss of the record of networked memories contained therein [4].
5. By multimedia communications I mean the combination of texts, photos, images, videos, links and other formats that come into play in the spontaneous daily emails, messages and postings on social networks or user-generated platforms in societies marked by the pervasive use of webbed digital technologies.
6. Lawrence Lessig. "The Law of the Horse: What Cyberlaw Might Teach." *Harvard Law Review* 113 (1999): 501–46.
7. Lawrence Lessig. *Code: Version 2.0*. New York: Basic Books, 2006.
8. All the points raised in this section concerning the project of archiving social networks are discussed in further detail in the succeeding sections.
9. *See* section 3.2 for discussion.
10. *See* section 4 for discussion.
11. *See* sections 4 and 6 for discussion.
12. *See* section 5 for discussion.
13. *See* section 3.3 for discussion.
14. Library of Congress. "About the Library." Available online: http://www.loc.gov/about/ (accessed on 23 July 2014).
15. Library of Congress. "25 Most Frequently Asked Questions by Visitors." Available online: http://www.loc.gov/about/faqs.html (accessed on 23 July 2014).
16. American Library Association. *Policy Manual*. Chicago: American Library Association, 2013.

Available online: http://www.ala.org/aboutala/governance/policymanual/updatedpolicymanual/section1/1mission (accessed on 23 July 2014).
17. Peter S. Menell. "Knowledge Accessibility and Preservation Policy for the Digital Age." *Houston Law Review* 44 (2007): 1013–72.
18. U.S. Const. art I, § 8.
19. 17 U.S. Code § 407(a).
20. In addition to the mandatory deposit requirement, the collections of the Library of Congress are also comprised of materials that are donated or purchased.
21. Citing Charles Jewett, the first librarian of the Smithsonian Institution, who praised the preservation, access, and scholarly virtues of copyright deposit in 1850.
22. Ekaterina Haskins. "Between Archive and Participation: Public Memory in a Digital Age." *Rhetoric Society Quarterly* 37 (2007): 401–22.
23. Contrary to hegemonic forms of memorialization, vernacular forms of remembrance have generally assumed "ephemeral forms such as parades, performances, and temporary interventions [and have employed] non-hierarchical, sometimes subversive symbolism and stress egalitarian interaction and participation" [22].
24. Discussing of the September 11 Digital Archive, which incorporated a varied and polyphonic account using different types of media rather than a "univocal, self-aggrandizing narrative".
25. Guy Pessach. "[Networked] Memory Institutions: Social Remembering, Privatization and its Discontents." *Cardozo Arts and Entertainment Law Journal* 26 (2008): 71–149.
26. Jeffrey Schnapp. "Animating the Archive." *First Monday*, 4 August 2008. Available online: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2218/2020 (accessed on 23 July 2014).
27. Belinda Barnet. "Pack-Rat or Amnesiac? Memory, the Archive and the Internet." *Continuum: Journal of Media & Cultural Studies* 15 (2001): 217–31.
28. Emil Protalinski. "Facebook has over 845 million users." *ZDNet* (blog), 1 February 2012. Available online: http://www.zdnet.com/blog/facebook/facebook-has-over-845-million-users/8332?tag=mantle_skin;content (accessed on 23 July 2014).
29. Dino Grandoni. "Facebook Has 10,000 Times the Photos the Library of Congress Does." *The Atlantic Wire*, 16 September 2011. Available online: http://www.theatlanticwire.com/technology/2011/09/facebook-has-10000-times-photos-library-congress-does/42605/ (accessed on 23 July 2014).
30. This is discussed in further detail in section 5.
31. Valerie Steeves. "Reclaiming the Social Value of Privacy." In *Privacy, Identity and Anonymity in a Network World: Lessons from the Identity Trail*. Edited by Ian Kerr, Valerie Steeves and Carole Lucock. Oxford: Oxford University Press, 2009, pp. 191–208.
32. Alan Westin. *Privacy and Freedom*. New York: Atheneum, 1967.
33. Colin J. Bennett, and Charles Raab. *The Governance of Privacy: Policy Instruments in Global Perspective.* Cambridge, MA: Massachusetts Institute of Technology Press, 2006.
34. David Phillips. "Ubiquitous Computing, Spatiality, and the Construction of Identity: Directions for Policy Response." In *Privacy, Identity and Anonymity in a Network World: Lessons from the Identity Trail*. Edited by Ian Kerr, Valerie Steeves and Carole Lucock. Oxford: Oxford University Press, 2009, pp. 303–18.

35. Patricia Regan. *Legislating Privacy: Technology, Social Values, and Public Policy*. Chapel Hill: University of North Carolina Press, 1995.
36. Manuel Castells. *The Rise of the Network Society*. Boston: Blackwell Publishers, 1996.
37. Restatement of the Law, Second, Torts. § 652. Comment b (2011).
38. Lior Jacob Strahilevitz. "A Social Networks Theory of Privacy." *University of Chicago Law Review* 72 (2005): 919–88.
39. Elizabeth Paton-Simpson. "Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places." *University of Toronto Law Journal* 50 (2000): 305–46.
40. Lauren Gelman. "Privacy, Free Speech, and 'Blurry-Edged' Social Networks." *Boston College Law Review* 50 (2009): 1315–44.
41. James Grimmelmann. "Saving Facebook." *Iowa Law Review* 94 (2009): 1137–206.
42. He also states that "[w]hile the privacy settings chosen by the original user shouldn't be conclusive, they're good evidence of how the plaintiff thought about the information at issue, and of how broadly it was known and knowable before the defendant spread it around" ([41], p. 1196).
43. Naomi Cahn. "Postmortem Life Online." *Probate & Property* 36 (2011): 36–39.
44. The Digital Beyond. Available online: www.thedigitalbeyond.com (accessed on 23 July 2014).
45. The Death Reference Desk. Available online: http://deathreferencedesk.org/ (accessed on 23 July 2014).
46. Death and Digital Legacy. Available online: http://www.deathanddigitallegacy.com/ (accessed on 23 July 2014).
47. John Romano, and Evan Carroll. *Your Digital Afterlife: When Facebook, Flickr and Twitter are Your Estate, What's Your Legacy?* San Francisco: New Riders, 2009.
48. Also, see a recent book that offers practical guidance on how to handle digital "assets" upon death [47].
49. Legacy Locker. Available online: http://legacylocker.com/ (accessed on 23 July 2014).
50. SecureSafe. Available online: http://www.securesafe.com/en / (accessed on 23 July 2014).
51. DataInherit. Available online: http://www.datainherit.com/en/home.html (accessed on 23 July 2014).
52. John Conner. "Life After Death: The Issue of Planning for a Person's Digital Assets after Death." *Estate Planning & Community Propery Law Journal* 3 (2011): 301–22.
53. Michael Walker, and Victoria Blachly. "Virtual Assets." *Tax Management, Estates, Gifts, and Trusts Journal* 36 (2011): 253–60.
54. Jonathan L. Darrow. "Who Owns a Decedent's E-mails: Inheritable Probate Assets or Property of the Network?" *New York University Journal of Legislation & Public Policy* 10 (2006): 281–320.
55. Yahoo! "Yahoo! Terms of Service." Available online: http://info.yahoo.com/legal/us/yahoo/utos/utos-173.html (accessed on 23 July 2014).
56. Michael D. Roy. "Beyond the Digital Asset Dilemma: Will Online Services Revolutionize Estate Planning?" *Quinnipiac Probate Law Journal* 24 (2011): 376–417.
57. Facebook. "Report a Deceased Person's Profile." Available online: https://www.facebook.com/help/contact/305593649477238 (accessed on 23 July 2014).
58. Max Kelly. "Memories of Friends Departed Endure on Facebook." *Facebook Blog*, 26 October 2009. Available online: http://blog.facebook.com/blog.php?post=163091042130 (accessed on 23 July 2014).

59. Myspace. "What If My Friend/Loved One Passed Away?" Available online: http://www.myspace.com/help?pm_cmp=ed_footer (accessed on 23 July 2014).
60. Youtube. "I Need Access to the Account of a Deceased YouTube Member." Available online: http://www.google.com/support/youtube/bin/answer.py?hl=en&answer=94458 (accessed on 23 July 2014).
61. Twitter Help Center. "How to Contact Twitter About a Deceased User." Available online: http://support.twitter.com/groups/33-report-a-violation/topics/148-policy-information/articles/87894-how-to-contact-twitter-about-a-deceased-user (accessed on 23 July 2014).
62. Twitter. "Privacy Policy." Available online: http://twitter.com/privacy (accessed on 23 July 2014).
63. Google Gmail. "Accessing a Deceased Person's Mail." Available online: http://mail.google.com/support/bin/answer.py?hl=en&answer=14300 (accessed on 23 July 2014).
64. Stating that "[a]t Google, we're keenly aware of the trust users place in us, and we take our responsibility to protect the privacy of people who use Google services very seriously. Any decision to provide the contents of a deceased user's email will be made only after a careful review, and the application to obtain email content is a lengthy process" [63].
65. Google Groups. "Inactive Gmail Account." Available online: http://www.google.com/support/forum/p/gmail/thread?tid=333f7e4e37f05936&hl=en (accessed on 23 July 2014).
66. Microsoft Community. "Microsoft Next of Kin Process: What to do in the event of the death or incapacitation of a loved one with a Outlook.com account." Available online: http://answers.microsoft.com/en-us/outlook_com/forum/oaccount-omyinfo/my-family-member-died-recently-is-in-coma-what-do/308cedce-5444-4185-82e8-0623ecc1d3d6 (accessed 23 July 2014).
67. Darrow developed this proposal in relation to email service providers.
68. Ind. Code § 29-1-13-1.1 (2010).
69. Okla. Stat. tit. 58, § 269 (2011).
70. Conn. Gen. Stat. § 45a-334a (2010);
71. R.I. Gen. Laws § 33-27-3 (2007).
72. According to Lessig, "[t]he dissimilarity is this: with every enforced contract—with every agreement that subsequently calls upon an enforcer to carry out the terms of that agreement—there is a judgment made by the enforcer about whether this obligation should be enforced. In the main, these judgments are made by a court. And when a court makes such judgments, the court considers not just the private orderings constituted in the agreement before it, but also issues of public policy, which can, in some contexts, override these private orderings. When a court enforces the agreement, it decides how far the power of the court can be used to carry out the agreement. Sometimes the agreement will be carried out in full; but often, the agreements cannot be fully effected. Doctrines such as impossibility or mistake will discharge certain obligations. Rules about remedy will limit the remedies the parties can seek. Public policy exceptions will condition the kinds of agreements that can be enforced. "Contracts" incorporate all these doctrines, and it is the mix of this set of public values, and private obligations, that together produce what we call "a contract" ([6], p. 530).
73. Lessig states that "[a]rchitectures can enable or disable individual choice by providing (or failing to provide) individuals both with the information they need to make a decision and with the option

of executing that decision. […] Self-regulation, like state-regulation, depends upon architectures of control. Without those architectures, neither form of regulation is possible" ([6], p. 519).

74. 17 U.S.C. § 202 (2011).
75. 17 U.S.C. § 106.
76. Chris Walters. "Facebook's New Terms of Service: 'We Can Do Anything We Want with Your Content, Forever.'" *The Consumerist*, 15 February 2009. Available online: http://consumerist.com/2009/02/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever.html (accessed on 23 July 2014).
77. Facebook. "Statement of Rights and Responsibilities." Available online: http://www.facebook.com/terms.php?ref=pf (accessed on 23 July 2014).
78. In terms of Myspace, the terms of service imply that the profile of a user disappears with his or her death.
79. Myspace. "Myspace.com Terms of Use Agreement." Available online: http://www.Myspace.com/Help/Terms (accessed on 23 July 2014).
80. Similarly, Myspace recognizes that users retain ownership, including the copyright, over the contents they post, subject to a non-exclusive, fully-paid and royalty-free, sublicensable and worldwide limited license "to use, modify, delete from, add to, publicly perform, publicly display, reproduce, and distribute such Content solely on, through or in connection with the Myspace Services […] except that Content marked 'private' will not be distributed by Myspace outside the Myspace Services and Linked Services". Additionally, Myspace states that "[t]his limited license does not grant Myspace the right to sell or otherwise distribute your Content outside of the Myspace Services or Linked Services." Upon a user's removal of content from Myspace, the network will "cease distribution as soon as practicable, and at such time when distribution ceases, the license will terminate" [79]. In general, we see that the terms of service of Facebook and Myspace share certain characteristics such as the recognition of user ownership of content posted and the grant of a non-exclusive license of use to the social network subject to the user's privacy setting. However, whereas Myspace specifies certain limits of its license in that it does not grant Myspace the right to sell or otherwise distribute users' content outside of the Myspace Services or Linked Services, Facebook remains more obscure in terms of the contours of its limited license.
81. 17 U.S.C.A. § 101.
82. Definition of "publication".
83. 37 C.F.R. § 202.19.
84. Latest version effective 13 May 2011.
85. 37 C.F.R. § 202.19 (c) (5).
86. 37 C.F.R. § 202.19 (b) (4).
87. 37 C.F.R. § 202.24 (a).
88. 17 U.S.C. § 407(e).
89. 37 C. F. R. § 202.22 (c) (1).
90. The absence of news and critical social commentary blogs is a particularly glaring omission given the explicit inclusion of periodicals and newspapers in the definition of electronic works and signals the deposit requirement's inability to grapple with how the internet has

undermined traditional outlets of news and enabled a broad following of alternative sources of information and analysis.

91. H.R. Rep. No. 1476, 94th Cong., 2d Sess. 138 (1976).
92. S. Rep. No. 473, 94th Cong., 1st Sess. 121 (1975).
93. 17 U.S.C. § 108.
94. 17 U.S.C. § 107.
95. Sarah Kessler. "5 Things the Library of Congress is Archiving Online." *Mashable*, 30 May 2010. Available online: http://mashable.com/2010/05/30/library-of-congress-web-archive/ (accessed on 23 July 2014).
96. Biz Stone. "Tweet Preservation." *Twitter Blog,* 14 April 2010. Available online: http://blog.twitter.com/2010/04/tweet-preservation.html (accessed on 23 July 2014).
97. Jennifer Van Grove. "Library of Congress to Preserve Tweets for Eternity." *Mashable*, 14 April 2010. Available online: http://mashable.com/2010/04/14/twitter-library-of-congress/ (accessed on 23 July 2014).
98. Matt Raymond. "How Tweet It Is!: Library Acquires Entire Twitter Archive." *Library of Congress Blog*, 14 April 2010. Available online: http://blogs.loc.gov/loc/2010/04/how-tweet-it-is-library-acquires-entire-twitter-archive/ (accessed on 23 July 2014).
99. Tom Temin, and Amy Morris. "Library of Congress to Receive Entire Twitter Archive: An Interview with Digital Initiatives Program Manager, Bill Lefurgy." 6 December 2011. Available online: http://media.dev-cms.com/wtop/23/2320/232030.MP3 (accessed on 23 July 2014).
100. Library of Congress Web Archives. Available online: http://lcweb2.loc.gov/diglib/lcwa/html/lcwa-home.html (accessed on 23 July 2014).
101. Marshall Kirkpatrick. "Twitter's Entire Archive Headed to the Library of Congress." *ReadWriteWeb*, 14 April 2010. Available online: http://www.readwriteweb.com/archives/twitters_entire_archive_headed_to_the_library_of_c.php (accessed on 23 July 2014).
102. Amar Toor. "Library of Congress to Store Entire Twitter Archive." *Switched*, 14 April 2010. Available online: http://www.switched.com/2010/04/14/library-of-congress-to-store-entire-twitter-archive/ (accessed on 23 July 2014).
103. Twitter. "Get to Know Twitter: New User FAQ." Available online: http://support.twitter.com/articles/13920-frequently-asked-questions (accessed on 23 July 2014).
104. Consider the distinction between a "reply" and a "direct message," explained in the FAQ section of Twitter [103]:

    What are @replies?
    If a message begins with @username, meaning it was directed to another user, it is an @reply. Click the Reply button on another person's Tweet to reply to it. Please note that if your Tweets are protected, users who are not following you will not see your @replies or mentions. Read more here.

    What are direct messages?
    Direct messages are personal messages sent from one Twitter person to another; they do not appear in public for anyone else to read. You can only send a direct message to a person who follows you. Read more here.

What is the difference between an @reply and a direct message?
An @reply is a public message sent regardless of follow-ship that anyone can view (if your Tweets are public). A direct message can only be sent by someone you follow, and can only be seen by the sender and intended recipient.

105. Facebook. "Managing a Page." Available online: http://www.facebook.com/help/?page=203955942973503 (accessed on 23 July 2014).
106. "Friends" refers to people who are confirmed friends of another Facebook account holder. This is distinct from the "Friends" privacy setting, which allows users to post content just to their circle of friends rather than all the members of Facebook, that is, the "Public" privacy setting.
107. Facebook. "About Facebook Pages." Available online: http://www.facebook.com/help/?faq=217671661585622&ref_query=facebook+page (accessed on 23 July 2014).
108. Danny Sullivan. "Google Realtime Search & the Aftermath of the Google-Twitter Split." *Search Engine Land*, 7 July 2011. Available online: http://searchengineland.com/google-realtime-search-the-aftermath-of-the-google-twitter-split-84794 (accessed on 23 July 2014).
109. Google also had a service to search Tweets called Google Realtime Search that was discontinued.
110. Topsy. Available online: http://topsy.com/ (accessed 23 July 2014).
111. 37 C. F. R. § 202.22 (e) (2).
112. For instance, there is no mention in the law nor regulations of the availability and accessibility of digital works, either published electronic works or unpublished internet programming transmitted to the public. The only direct and specific discussion on access is when the Code of Federal Regulations addresses the acquisition and deposit of unpublished audio and audiovisual transmission programs.

> All copies and phonorecords acquired or made under this section, except copies and phonorecords of transmission programs consisting of a regularly scheduled newscast or on-the-spot coverage of news events, shall be subject to the following restrictions concerning copying and access: in the case of television or other audiovisual transmission programs, copying and access are governed by Library of Congress Regulation 818–17, Policies Governing the Use and Availability of Motion Pictures and Other Audiovisual Works in the Collections of the Library of Congress, or its successors; in the case of audio transmission programs, copying and access are governed by Library of Congress Regulation 818–18.1, Recorded Sound Listening and Duplication Services, or its successors. Transmission programs consisting of regularly scheduled newscasts or on-the-spot coverage of news events are subject to the provisions of the "American Television and Radio Archives Act", 2 U.S.C. 170, and such regulations as the Librarian of Congress shall prescribe [111].

Copying and access varies according to whether it is a newscast or on-the-spot coverage of news events, audiovisual transmission programs or audio transmission programs. Unfortunately, I was unable to locate copies of the policies mentioned in the above quote to gauge the nature of the variability of copying and accessibility and to determine if there are specific protocols that differentiate the copying and accessibility to published electronic works or unpublished internet programming.

113. As already discussed, Darrow developed this proposal in relation to email service providers.
114. Joseph L. Sax. *Playing Darts with a Rembrandt: Public and Private Rights in Cultural Treasures.* Ann Arbor: University of Michigan Press, 1999.
115. Mary Sarah Bilder. "The Shrinking Back: The Law of Biography." *Stanford Law Review* 43 (1992): 299–360.
116. Society of American Archivists. *SAA Core Values Statement and Code of Ethics*. Chicago: Society of American Archivists, 2011. Available online: http://www2.archivists.org/statements/saa-core-values-statement-and-code-of-ethics (accessed on 23 July 2014).
117. Consider the following quote: "The laws that protect privacy are far narrower than copyright law. Individuals are less likely to have lawyers on retainer to protect their interest. And more importantly, there is no inherent monetary value in most private information that can be recouped when it is disclosed. So although copyright owners have strong legal protections, with a robust statutory damages regime to weigh in determining whether to protect the value of the copyrighted work against a purported infringer, individuals have weak laws and uncertain economic value to weigh when determining whether to pursue an action against someone who revealed private information about them ([40], p. 1334)".