Regulating Electronic Identity Intermediaries: The "Soft eID" Conundrum

TAL Z. ZARSKY* & NORBERTO NUNO GOMES DE ANDRADE†

TABLE OF CONTENTS

* Associate Professor, University of Haifa, Faculty of Law.
† European Commission, Joint Research Centre, Institute for Prospective Technological Studies (IPTS).

The authors thank Michal Lavi, Eric Goldman, and James Grimmelmann for their thoughtful comments. The authors also thank Talya Ponchek for her assistance in research. The views expressed in this Article are purely those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission.

I. INTRODUCTION: THE RISE OF THE DIGITAL IDENTITY INTERMEDIARY

In late 2011, Salman Rushdie found himself in a unique and novel situation which was both surprising and annoying: he was required to prove that he indeed was Salman Rushdie, the famous author—a task he initially failed![1] This identity-based dispute began when Facebook suspected that the person behind the "Salman Rushdie" Facebook page was not the famous author.[2] Thus, it requested that the live persona operating the profile (indeed, Rushdie himself) provide proof of identity. Rushdie, however, was unable to prove that his first name was "Salman."[3] His first name, which he rarely uses, is "Ahmed" (Salman is his middle name).[4] Therefore, Facebook ordered that the Facebook page was

[1] Somini Sengupta, *Naming Names: Rushdie Wins Facebook Fight*, N.Y. TIMES, Nov. 15, 2011, at A1, *available at* http://www.nytimes.com/2011/11/15/technology/hiding-or-using-your-name-online-and-who-decides.html?pagewanted=all&_r=0.

[2] *Id.*

[3] *Id.*

[4] *Id.*

to be renamed "Ahmed Rushdie."[5] The infuriated Rushdie blasted Facebook via his Twitter account.[6] Two hours later, Facebook conceded. (Ahmed) Salman Rushdie was again controlling the "Salman Rushdie" Facebook profile.[7]

The former St. Louis Cardinals' Manager Tony LaRussa felt the sting of novel identity-related conflicts from a somewhat different angle. LaRussa learned of a Twitter account bearing his name and posting tasteless tweets.[8] He then moved to sue Twitter on several accounts (including trademark infringement, cybersquatting, and misappropriation).[9] The problematic profile was eventually removed and the case apparently settled (although the details of this settlement are disputed).[10] Similar stories regarding the hardship of individuals whose identities were manipulated or hijacked are often reported by the press.[11] Claims and suits against content platforms and dating services[12] which enabled these abuses were set forth, with limited success.

The rise of identity-based disputes should come as no surprise. Individuals are spending a great deal of time in online realms. They are engaging in commerce and participating in the social discourse.[13] This is all occurring in a variety of novel settings: through the use of social networking sites, virtual worlds, and peer-to-peer networks to name a few.[14] Users are carrying out these activities by using their desktop and laptop computers, tablets, and smartphones.

---

[5] *Id.*

[6] *Id.*

[7] Sengupta, *supra* note 1, at A1. When addressing similar issues, James Grimmelmann sums up these forms of situations while noting that "[t]hese victims thus find themselves trapped in the Kafkaesque position of being unable to prove that they really are themselves, to the satisfaction of a business that has already shown itself incapable of correctly telling who they are." James Grimmelmann, *Known and Unknown, Property and Contract: Comments on Hoofnagle and Moringiello*, 5 BROOK. J. CORP. FIN. & COM. L. 85, 88 (2010).

[8] LaRussa v. Twitter, Inc., DIGITAL MEDIA L. PROJECT (May 29, 2009), http://www.dmlp.org/threats/la-russa-v-twitter-inc#description.

[9] *Id.*

[10] *Id.*

[11] For a heartbreaking story featuring an author tormented by a fake profile, see Susan Arnout Smith, *The Fake Facebook Profile I Could Not Get Removed*, SALON (Feb. 1, 2011, 8:39 PM), http://www.salon.com/2011/02/02/my_fake_facebook_profile/. For an alarming story featuring the impersonation of a top NATO Commanding Officer (probably by Chinese hackers sponsored by the state), see David Meyer, *Top NATO Officer Impersonated on Facebook*, ZDNET (Mar. 12, 2012), http://www.zdnet.com/top-nato-officer-impersonated-on-facebook-4010025604/; *see also* Helen A.S. Popkin, *2 Girls, Ages 12 and 13, Face Felony for Fake Facebook Account*, NBC NEWS (July 30, 2012, 5:05 PM), http://www.nbcnews.com/technology/2-girls-ages-12-13-face-felony-fake-facebook-account-916555. For additional references to impostors of both celebrities (such as Prince William and Sarah Palin) and others, see Shannon N. Sterritt, Comment, *Applying the Common-Law Cause of Action Negligent Enablement of Imposter Fraud to Social Networking Sites*, 41 SETON HALL L. REV. 1695, 1698 (2011).

[12] *See, e.g.*, Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1122, 1125 (9th Cir. 2003).

[13] Sengupta, *supra* note 1, at A1.

[14] *Id.* at A3.

Moreover, they will soon be able to do so with their glasses![15] Therefore, users are creating and investing a great deal of social capital in their online identities. Given this massive investment, many users hold their online identity as dear to them, both financially and emotionally. For them, the implications of losing control over, harming, or wrongfully assuming their online identity are dire. Such loss of control carries with it overall negative social implications as well. While both technology and market forces provide responses to these emerging problems,[16] the law is destined to play an important role in resolving these novel forms of disputes. Such disputes are making their way to the courts and the regulator's attention,[17] and even generating novel terms of art, such as "e-personation" and "catfishing."[18] This Article strives to introduce and map out some initial strategies for addressing these novel legal matters.[19]

While the problems and tensions noted address a variety of plaintiffs, defendants, and victims, they often involve the actions of a handful of *identity intermediaries*.[20] Indeed, as a greater portion of our lives migrates to the digital realm, many of our interactions are made possible by powerful intermediaries.[21] The digital realm has led to the emergence of several powerful platforms which enable the publication, sharing, and distribution of content, as well as facilitate

---

[15] *See How It Feels*, GOOGLE GLASS, http://www.google.com/glass/start/how-it-feels/ (last visited July 12, 2013).

[16] Sengupta, *supra* note 1, at A3.

[17] *Carafano*, 339 F.3d at 1121, 1125.

[18] Zimmerman v. Bd. of Trs. of Ball State Univ., No. 1:12-cv-01475-JMS-DML, 2013 WL 1619532, at *14 (S.D. Ind. Apr. 15, 2013).

[19] The discussion noted in the text is closely linked to a recent doctrinarian movement of legal "revitalization" of the right to identity in the EU. *See* CLARE SULLIVAN, DIGITAL IDENTITY 19–39 (2011); Norberto Nuno Gomes de Andrade, *Right to Personal Identity: The Challenges of Ambient Intelligence and the Need for a New Legal Conceptualization*, *in* COMPUTERS, PRIVACY AND DATA PROTECTION: AN ELEMENT OF CHOICE 65, 66–69, 94 (Serge Gutwirth et al. eds., 2011); Roger Brownsword, *Friends, Romans, Countrymen: Is There a Universal Right to Identity?*, 2 L. INNOVATION & TECH. 223, 224–26 (2009); Giorgio Pino, *The Right to Personal Identity in Italian Private Law: Constitutional Interpretation and Judge-Made Rights*, *in* THE HARMONISATION OF EUROPEAN PRIVATE LAW 225, 225–26, 233–37 (Mark Van Hoecke & François Ost eds., 2000); Elad Oreg, Right to Information Identity 4–24 (Oct. 2011) (unpublished manuscript), *available at* http://works.bepress.com/elad_oreg/1; Paul De Hert, *A Right to Identity To Face the Internet of Things*, UNESCO 5–10, http://portal.unesco.org/ci/fr/files/25857/12021328273de_Hert-Paul.pdf/de%2BHert-Paul.pdf (last visited July 17, 2013). For a very recent argument in favor of recognizing the right to identity in the United States, see Clare Sullivan, *Digital Identity, Privacy and the Right to Identity in the United States of America*, 29 COMPUTER L. & SECURITY REV. 348, 349 (2013).

[20] It appears this term was coined by Chris Hoofnagle, as mentioned in Sengupta, *supra* note 1, at A3.

[21] Oreg, *supra* note 19, at 10–11 ("With the evolving of the Web the range of intermediaries has become more sophisticated, partisan, and interest motivated, including: access providers, search and filter services, name managers, content hosts, communities' administrators, database operators and others. They can all determine what information—including identity-related information—will be kept, verified, accessed and disseminated.").

and even control the rich public discussions and discourses that are unfolding. Yet the examples mentioned illustrate the rise of the new role of identity intermediation, i.e., the process of creating, authenticating, verifying, and guiding stable identities through which we interact, send, and receive information online, as well as structure our identity and persona. With this new social and technological role, duties and responsibilities for these new intermediaries are sure to follow—and with that, legal liability. This Article focuses its attention on the role law must play in shaping the conduct and behavior of these identity intermediaries.

The law can respond to the rise of these intermediaries and the disputes they generate in several ways. One dominant strategy is that of limited responses—sitting on the sidelines and allowing social, economic, and technological forces to guide the identity intermediaries and their users toward optimal and socially acceptable outcomes. Such a strategy indeed might make sense in an innovative and ever-changing environment. To a great extent, that is the path currently taken by U.S. law. This path is enabled by a strategy of deference to the one-sided standard form contracts set forth by the intermediary. It is further supplemented by the blanket immunity provided by Section 230 of the Communications Decency Act (CDA) to the intermediaries' role as publishers, which can be applied to the identity intermediation context.[22] Indeed some of the most (in)famous Section 230 cases involved impersonation and abuse of identity intermediation. Here, the court upheld the broad protection the CDA provides content providers in their capacity as identity intermediaries and limited their exposure to the users'/plaintiffs' claims.[23] In short, current U.S. law mostly takes a non-intervening approach which merely protects the contractual and property rights of the intermediaries and allows them to voluntarily govern these virtual realms.[24] The first two examples noted above (as well as many others) demonstrate how identity intermediaries are doing so, with relative success.[25]

The United States' immunity-based strategy for regulating digital intermediaries has been the subject of endless debates.[26] Academics have discussed the pros and cons of the overall immunity Section 230 provides, while noting its vast benefits to both free speech and innovation policy.[27] The global dominance of various U.S.-based online ventures (and the paucity of notable

---

[22] Communications Decency Act, 47 U.S.C. § 230 (1996).

[23] *See* discussion of *Carafano infra* notes 186–189.

[24] *See* discussion *infra* notes 186–189.

[25] Sengupta, *supra* note 1, at A1.

[26] DAWN C. NUNZIATO, VIRTUAL FREEDOM: NET NEUTRALITY AND FREE SPEECH IN THE INTERNET AGE 11–87, 135–51 (2009); DANIEL J. SOLOVE, THE FUTURE OF REPUTATION 105–88 (2007); JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 101–26, 175–234 (2008); Felix T. Wu, *Collateral Censorship and the Limits of Intermediary Immunity*, 87 NOTRE DAME L. REV. 293, 295–97, 328–49 (2011).

[27] NUNZIATO, *supra* note 26.

online ventures from other parts of the world)[28] might perhaps indicate the successful outcome of opting for this legal strategy. On the other hand, the current legal setting provides limited protection of users' identity, privacy, and autonomy interests.[29] Such users, when harmed by speech-related torts generated in the digital realm, can only pursue the primary tortfeasor (who is often cloaked in anonymity) or rely upon the good graces of the relevant intermediary to limit their damages or even punish wrongdoers.[30] A discussion as to the proper regulation of identity intermediaries must clearly echo the arguments set forth within this broader discussion. However, this Article finds that the context of identity intermediation calls for a specific set of considerations, balances, and possibly legal rules. For that reason, it proposes an innovative legal taxonomy for addressing the process of identity intermediation. In addition, it moves to inquire whether courts and regulators must take a more proactive stand in resolving these novel disputes and defining the role of these powerful identity players.

Given the fact that the U.S. legal response to regulating identity intermediaries is relatively clear (though possibly wrong),[31] the Article looks to existing and possibly future EU legislative efforts aimed at regulating identity intermediaries on several dimensions as possible points of inspiration. In Europe, identity intermediaries of a different form are regulated by the E-Signature ("eSig") Directive, which is currently going through a major revision process.[32] EU policymakers are further considering expanding these rules to a broader set of identity intermediaries.[33] This Article will examine the eSig Directive's unique features, as well as its unimpressive track record, and the reasons and implications of its relative failures. Understanding these failures will assist us in understanding the limits of such a regulatory framework, should we choose to expand it to all identity intermediaries—including social networking sites and micro-blogging platforms.

Although this aspect of our study might seem Euro-centric, this analytical inquiry should be of great interest to U.S. readers. As with other recent U.S.-originated academic projects examining the intricacies of recent EU initiatives, this study will inquire what U.S. regulators and market participants can learn

---

[28] European Commission JRC Technical Reports, *Comparing Innovation Performance in the EU and the USA: Lessons from Three ICT Sub-Sectors*, 3, JRC 81448 (2013) (Simon Forge et al.), *available at* ftp://ftp.jrc.es/pub/EURdoc/EURdoc/JRC81448.pdf.

[29] Wu, *supra* note 26, at 294–95. *See generally* Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO ST. L.J. 1217 (2013).

[30] SOLOVE, *supra* note 26, at 186–87.

[31] NUNZIATO, *supra* note 26; Wu, *supra* note 26, at 295–97, 328–49.

[32] *Proposal for a Regulation of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market*, at 2, COM (2012) 238 final (Apr. 6, 2012).

[33] *Id.*

from the EU's experience.[34] Indeed the U.S. Government is contemplating a number of novel steps which greatly resemble those discussed across the pond.[35] Thus, learning of the EU experiences and discussions will surely prove helpful in this limited context, as well as when contemplating the proper form of identity intermediary regulation.

The Article proceeds as follows. Following this introduction (Part I), Part II provides the background and terminology for understanding the role of identity intermediaries in the digital age. It maps out the various forms of identity intermediation—from the state, through the creation of electronic IDs ("eIDs"), until the recent rise of "soft eID" intermediaries. These are defined as entities which provide for identity intermediation online, yet do so incidentally, remotely, and in a lightly regulated environment. Part III moves to further address the specific traits of soft eID intermediation. It notes intermediation which generates either ipse or idem identities. The former ("ipse") refers to a digital identity initiated by the relevant individual.[36] The latter ("idem") addresses instances in which others collect and rely upon information pertaining to an individual.[37] This Article chooses to focus on the former category. Thereafter, the Article distinguishes between intermediations which rely upon the use of "Real Names" and "Stable Pseudonyms"—each category employing a different set of technologies and verification methods, and generating unique benefits and concerns.

In Part IV, we explore the benefits and risks of soft eID intermediation. Identity intermediation promotes economic interests, as well as those related to personality and identity. It also enhances autonomy and promotes free speech.[38] However, such intermediaries might generate serious concerns. The integrity of soft eIDs might be compromised.[39] They might be hacked, used for impersonation or identity misrepresentation.[40] In addition, the intermediaries might use the power they are vested with excessively, by terminating accounts, or limiting their interoperability and mobility.[41] The analysis notes the parties affected, while drawing from recent events addressed by courts and the press. This Part ends by addressing possible legal responses, while noting the option

---

[34] *See, e.g.*, Paul M. Schwartz, *The EU–U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1976 (2013).

[35] *See* THE WHITE HOUSE, NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE 1 (Apr. 2011) [hereinafter NSTIC REPORT], *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

[36] Mireille Hildebrandt, *Profiling and the Identity of the European Citizen*, *in* PROFILING THE EUROPEAN CITIZEN 303, 312–13 (Mireille Hildebrandt & Serge Gutwirth eds., 2008).

[37] *Id.*

[38] SOLOVE, *supra* note 26, at 125–60.

[39] Paul Bernal, The Right to Online Identity 13 (Sept. 7, 2012) (unpublished manuscript), *available at* http://ssrn.com/abstract=2143138.

[40] *Id.*

[41] *See, e.g.*, *Statement of Rights and Responsibilities*, FACEBOOK, §§ 5, 9, https://www.facebook.com/legal/terms (last visited July 16, 2013).

of a limited, responsive, and strategic role for law. Seeking the proper role of law, Part V introduces readers to several related regulatory frameworks, namely the EU eSig Directive. This Directive made use of both the regulatory and strategic responses.[42] We then examine two novel governmental steps in the United States and the EU, which closely coincide with some of the eSig Directive general themes. These legal frameworks provide important insights when considering the proper legal regime to be used to regulate soft eID intermediaries.

On the basis of these interesting insights, Part VI provides recommendations for legal responses. Here, the Article examines a variety of policy moves which pertain to soft eID intermediaries, such as requiring mandatory approval, setting up a voluntary accreditation system, and assigning tort liability. The Article generally rejects the first two options, and thereafter closely examines whether and how tort liability should normatively be assigned to these powerful intermediaries. It does so while distinguishing among different methods of intermediation (Real Names vs. Stable Pseudonyms) as well as the different concerns noted in Part IV (ID hijacking, impersonation, and identity misrepresentation). The analysis thus generates a two-by-three liability matrix. Finally, this Part examines the role law should take in curbing the intermediaries' excessive ability to impede on the individual's identity interests. It addresses the optimal ways law should encourage mobility and interoperability, as well as other educational roles which will prove constructive in this context. We provide several concluding remarks regarding future research and broader legal questions in Part VII.

II. IDENTITY INTERMEDIATION: "HARD" EIDS/"SOFT" EIDS

A. *From IDs to eIDs*

How can I prove I am who I say I am? In the olden days, when individuals lived in small communities and stayed put for most of their lives, meeting this task was trivial. Members of society recognized each other while relying on various physical traits, as they interacted with almost the same people throughout the course of their lives. But as society moved toward urbanization, greater mobility, and overall complexity, identification[43] became a greater

---

[42] *See generally* Directive 1999/93/EC, of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures, 1999 O.J. (L 13) 12 [hereinafter Directive 1999/93/EC].

[43] The term "identity" is quite difficult to define. James Fearon notes fourteen (!) different definitions for this term. James D. Fearon, What Is Identity (as We Now Use the Word)? 4–5, 7 (Nov. 3, 1999) (unpublished manuscript), *available at* http://www.stanford.edu/~jfearon/papers/iden1v2.pdf. Generally, the word refers both to the "similarity" among factors (they are "identical") as well as the sense of self. *See* Hildebrandt, *supra* note 36, at 312. The context discussed here is of "sameness"—that the individual identified at one point is the same as the one identified later. Steven Davis refers to this as the epistemological

challenge. Trusted intermediaries were called upon to enable identification in a variety of settings.

The most natural identity intermediary was (and still is) the State.[44] The state issued identification measures early on so as to provide travel documents (passports),[45] allow for the fair allocation of benefits (the Social Security card),[46] and vouch that an individual was permitted to engage in specific, regulated activities such as driving, hunting, or carrying firearms (by issuing driver's and gun licenses, as well as hunting permits).[47] The state provided an authenticating document, which could not be easily forged.[48] The document would be issued after interacting with the individual in person (at least initially) and relying upon other official documents he or she obtained.[49] These processes are addressed by a variety of relevant laws and regulations and remain outside the scope of the current discussion.[50]

With time, private entities began commanding crucial and strategic roles in society. To meet their obligations and achieve their goals, these entities are required to engage in identity intermediation as well. Banks and credit card companies, for example, issue various cards which allow individuals to withdraw funds, engage in transactions, and draw credit.[51] These cards are identification instruments which signal to the relevant institute or merchant that funds should be provided and transactions executed.[52] At times, other entities (be they public or private) might rely on these privately issued means of identifications to verify the identity of an individual as well.[53] For instance, states rely upon these private forms of identification for voter identification (traditionally a public/governmental role).[54]

Upon entering the information age, the identity intermediation role faces intriguing opportunities and challenges. The Internet and other measures of cheap communications allow firms to reach out to customers around the globe,

---

meaning of identity. Steven Davis, *A Conceptual Analysis of Identity*, *in* LESSONS FROM THE IDENTITY TRAIL 213, 219 (Ian Kerr et al. eds., 2009).

[44] Fearon, *supra* note 43, at 4.

[45] Davis, *supra* note 43, at 219–21.

[46] *Id.* at 223–24.

[47] *Id.* at 222.

[48] *Id.* at 220.

[49] *Id.*

[50] For a lengthy philosophical analysis of the process of verifying identity through the use of passport control, see *id.* at 219–20.

[51] Davis, *supra* note 43, at 221–22.

[52] *Id.*

[53] *Id.* at 222.

[54] See *Voter Identification Requirements*, NAT'L CONF. ST. LEGISLATURES, http://www.ncsl.org/legislatures-elections/elections/voter-id.aspx (last updated June 27, 2013) for a list of voting ID requirements. For instance, in several states bank statements or utility bills with the voter's name and address count as means of identification (see Alabama, Alaska, and others). *Id.* Also note, for instance, that Arizona allows for reliance on a vehicle insurance card and that Florida allows for the use of a credit or debit card. *Id.*

regardless of physical borders and impediments. Yet these interactions do not provide for identification along the lines on which society has operated in previous generations. The information age enables virtual encounters in which physical cues, traits, and documents used for identification in the past are now unavailable or costly. In some instances, even allowing for a one time, very brief, physical interaction with an individual is very difficult to achieve. This reality generates a need for novel ways of authentication and, with it, opportunities for new forms of identity intermediation—the electronic identification intermediaries—or eID providers. Yet such intermediaries must first figure out how authentication could be achieved in a way that is secure, efficient, cheap, and simple.

It was at this point—the dawn of the digital age—when the EU stepped in to introduce the eSig Directive.[55] This Directive is premised upon the understanding that a novel form of eID intermediaries would (and should) arise.[56] The Directive and the EU Member States' laws that followed moved to facilitate, regulate, and even motivate these forms of intermediaries.[57] These envisioned intermediaries were intended to assist in carrying out identified or authenticated online interactions.[58] To do so, an intermediary will authenticate the identity of an individual upon issuance.[59] Most commonly, such authentication will initially be carried out in person, while relying on acceptable measures of authentication, such as a national ID, passport, driver's license, and photograph (or other biometric means of identification). Thereafter, the individual is issued a technological measure (usually a smartcard).[60] Together with a password, the individual uses these measures to achieve two objectives: (1) indicate that he or she is the author of a relevant text or carried out a specific action, and (2) indicate that a relevant text was not tampered with.[61] Other variations of this method exist, while relying on different business methods and modes of identification and technology (including various ways of using biometrics).[62] These intermediaries, the EU regulators believed, would lead to the fulfillment of the promise the digital age brought about: an international (or at least pan-European) marketplace of trusted transactions, and customers who are not deterred by the risks of remote transactions.[63] For the remainder of this

---

[55] Directive 1999/93/EC, *supra* note 42, at 12.

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *Commission Report of 15 March 2006 on the Operation of Directive 1999/93/EC on a Community Framework for Electronic Signatures*, at 6, COM (2006) 120 final (Mar. 15, 2006).

[60] For a discussion of the high percentage of smartcard usage, see JOS DUMORTIER ET AL., THE LEGAL AND MARKET ASPECTS OF ELECTRONIC SIGNATURES 127 (2003), *available at* http://skilriki.is/media/skjol/electronic_sig_report.pdf.

[61] *Commission Report*, *supra* note 59.

[62] *Id.*

[63] *Id.* at 4.

discussion, we will refer to these forms of identification as "hard eIDs"—they are mainly initiatives which strive to duplicate the offline world's level of security and authenticity in the online realm.[64] It is also important to note that laws governing eIDs were introduced in the United States (and are commonly referred to as "digital signature laws").[65] These state laws mostly address the extent of the validity of using such technologies, especially when compared to laws which present actual signature requirements.[66]

Yet, the intermediaries envisioned by regulators staggered.[67] Beyond limited contexts (such as e-government and banking), the business models which were meant to facilitate these measures rarely got off the ground.[68] However, a new and unexpected form of identity intermediaries, which did not fall within the scope of the existing regulatory structure, began to flourish: intermediaries providing soft eIDs.

B. *Soft eIDs: Definitions, Roles, and Tasks*

As the introductory examples demonstrate, a variety of Web 2.0 websites and applications are now featuring forms of identity issuance, authentication, and management—or in other words, they are acting as "identity intermediaries."[69] These intermediation models feature several key technical differences from the models addressed in the previous section (the hard IDs and eIDs). The central distinction, however, is not technical but economic and social. As opposed to the staggering models of hard identification addressed in the eSig Directive, these forms of identity intermediation are extremely popular. While these new online intermediaries and their models vary, we choose to characterize them by *three* central traits: (1) the identification process is *incidental* to the relevant firm's overall business plan; (2) the initial and subsequent identification and verification processes are carried out *remotely*, and (3) the firm engaged in eID intermediation is operating in a lightly regulated setting. Identifying these three traits allows us to refer to such intermediaries, as a group, as *soft eID intermediaries*. Every one of these three elements plays an important role in our discussion of unique policy recommendations for this specific context. Let us here briefly elaborate on each one of them.

---

[64] *Id.*

[65] A. Michael Froomkin, Lessons Learned Too Well 9–10 (Sept. 2011) (unpublished manuscript) (Miami Law Research Paper Series No. 2011-29), *available at* http://ssrn.com/abstract=1930017.

[66] Or in the words of A. Michael Froomkin: "[D]omesticate deployed technologies and fit them into known categories." *See id.* at 10; *see also* Andrew Barofsky, Note, *The European Commission's Directive on Electronic Signatures: Technological "Favoritism" Towards Digital Signatures*, 24 B.C. INT'L & COMP. L. REV. 145, 146–48, 152–57 (2000).

[67] *Commission Report*, *supra* note 59, 3.3.2.

[68] *Id.*

[69] Sengupta, *supra* note 1, at A3.

1. *Incidental*

As opposed to the business models envisioned by the drafters of the eSig Directive, the process of issuing and authenticating soft eIDs is incidental to the overall objectives of the relevant platform or application. The "incidental" nature of the process could be viewed and derived from several perspectives. Identification intermediation is incidental to the relevant firm's business plan and platform. As opposed to the entities envisioned by the eSig Directive drafters, these intermediaries do not directly generate income by providing an identification and authentication service for their users to use in other realms. Soft eIDs are generated and managed as means to achieve other objectives; they strive to promote commerce of various sorts, distribute content or generate social networks. While these objectives are enabled by identification, identification is not the central service provided. In addition, the identification intermediation aspect is incidental in the eyes of the relevant platform's users. In other words, when users might be asked how they would define Twitter, Facebook, eBay or Amazon, few would include "identity intermediary" in their first, second or even third responses. Common responses would probably include "content provider," "user generated content platform," or "social network site."

Cautious readers might take issue with the assertions noted above—especially with the argument that the identification and authentication processes carried out by social media platforms such as Facebook are merely "incidental" to their overall strategy. At least in the Facebook context, they will note that the website's construction of identity is quite *fundamental* to the platform's business model and revenue stream. After all, these steps render the website an ideal platform for carrying out a digital discourse. Furthermore, such steps enable Facebook's sophisticated behavioral advertising and marketing schemes which rely upon the personal information that identification schemes provide. They also generate a substantial source of revenue and value for the firm.

These critiques are well placed. Nonetheless, such new forms of identity intermediation are quite different from the hard eIDs noted above and addressed by digital signature laws. Even though there are obvious benefits that firms reap from introducing identification schemes, these are not directly and necessarily obvious to their users, upon examining the firms' business model. The identity intermediation abilities are also mostly instrumental by nature—a step on the way to achieve other goals. Thus, we still find these practices to be "incidental."

This categorization has two important implications for our policy discussion. One implication relates to a doctrinal argument; the other relates to the limits of human cognition and consumer protection issues that follow. From these two perspectives, as we now explain, the incidental nature of the identification process is clearer and easier to define. From a doctrinal perspective, according to U.S. law, the fact that identity intermediation is incidental allows the platforms initiating the process to argue that identity-related activities are merely subsets of their actions as information providers,

distributors, and publishers. Taking this position has important legal implications. It allows intermediaries to convincingly argue that many of their activities are immune from tort liability (as "publishers") in view of Section 230 of the CDA.[70] Thus, these firms are left, to a great extent, to voluntarily regulate the identification and verification process, with all the risks that might follow.

Furthermore, from a psychological/consumer protection perspective of law, the incidental nature of "identification"—at least from the perspective of the common user who does not understand the centrality of this role to the overall operation—renders it "non-salient."[71] The concept of "salience" is frequently noted in the contract and consumer protection related literature.[72] As opposed to central, or salient, features (such as price or time of delivery), non-salient features of products, services or even contracts (provisions governing choice of law, jurisdiction, or arbitration) are not fully comprehended and contemplated by purchasers or users at the time of contract formation.[73] This is a result of the limitations of human cognition.[74] Therefore, with regard to these non-salient aspects, markets fail to provide outcomes which are sufficiently protective of users' interests.[75] Courts or regulators might need to step in to assure that the strategies ultimately adopted by firms are fair and efficient (as opposed to overly protective of the firms). In other words, when selecting among various potential websites and their relevant "Terms of Use," users will (at least in theory) signal their discontent with different aspects of the service and, in that way, put pressure on the various online firms to meet their tastes and needs. This might be true for social networks with regard to the number of friends who are part of the network or other elements related to the user interface. In e-commerce platforms, this might be true with regard to price and variety of products. Yet when consumers are faced with non-salient decisions regarding contractual provisions and technical means governing the intermediation of identity (such as the intermediaries' liability in instances of impersonation), they will probably refrain from even considering these aspects and their possible implications at the time of contract formation.[76] Thus, regulatory intervention might be called for. We will return to the implication of this dynamic when considering policy recommendations.

---

[70] 47 U.S.C. § 230 (2006).

[71] For a discussion of salience, and the market failures that result from consumer inattentiveness to non-salient provisions, see Shmuel I. Becher & Tal Z. Zarsky, *E-Contract Doctrine 2.0: Standard Form Contracting in the Age of Online User Participation*, 14 MICH. TELECOMM. & TECH. L. REV. 303, 313, 350 (2008); *see also* OREN BAR-GILL, SEDUCTION BY CONTRACT: LAW, ECONOMICS, AND PSYCHOLOGY IN CONSUMER MARKETS 91–96 (2012).

[72] Becher & Zarsky, *supra* note 71, at 350.

[73] *Id.*

[74] Russell Korobkin, *Bounded Rationality, Standard Form Contracts, and Unconscionability*, 70 U. CHI. L. REV. 1203, 1220 (2003).

[75] Becher & Zarksy, *supra* note 71, at 312–13.

[76] *Id.* at 315, 350.

2. *Remote Verification*

As opposed to the hard identification schemes noted in Part II.A above, the soft eID identification/validation techniques almost never involve a physical interaction between the subject and the issuer. While online ventures are constantly changing and providing new forms of services,[77] they almost always operate virtually and interact remotely with their users, striving to take full advantage of the nearly zero marginal costs of additional users in the online realm. Therefore, these firms are reluctant to set up points of physical interaction with their users, given their high costs. Yet refraining from a physical interaction might lead to inherent weaknesses and vulnerability in the models which might merit regulatory intervention, and generates the concerns noted below.

3. *Lightly Regulated Industries*

One of the central premises of this Article is the recognition that a significant social and economic force—that of the soft eID identity intermediary—has arisen almost unnoticed and outside the confines and reach of the existing legal and policy realm. Yet that is not always true. In some instances, it is possible that soft eID intermediation schemes will be set forth by entities that are part of a regulated environment. This might be the case if soft eID initiatives are initiated by banks and financial institutions who are subjected to some forms of regulation. In a more practical example, soft eID identification schemes might be set forth by telecommunications carriers (both mobile and landline—industries that are heavily regulated in Europe and somewhat regulated in the United States), perhaps in the form of a biometric identification scheme installed in one's smartphone.[78] Our discussion is aimed at the more difficult questions concerning entities which are currently outside the regulators' easy reach. In the examples mentioned here, the firms and practices are not "soft." They are quite often subjected to "hard" law, if needed. For that reason, including these situations within our current analysis will needlessly encumber this discussion. However, the lessons derived from our current analysis of soft eIDs can surely be applied to examine identification schemes implemented by regulated entities.

---

[77] For some more innovative options see Sterritt, *supra* note 11, at 1727.

[78] Note, however, that if such initiatives would be set forth by the mobile phone makers (such as Apple), developers of the operating software (such as Google), or other app developers, such actions should still be considered as soft eIDs, as these are not closely regulated industries at this juncture.

III. SOFT EIDS: COMMON VARIATIONS AND KEY EXAMPLES

After defining the realm of soft eID intermediaries, we must focus on these intermediaries' unique traits. We here address two additional distinctions to enable a full understanding of the benefits, troubles, and policy solutions which we will tackle throughout this Article. We distinguish between *ipse* and *idem* identification schemes. Our current analysis will only refer to the former. In addition, we introduce two forms of identification schemes which dominate the soft eID environment: the use of Real Name IDs and Stable Pseudonyms. Every one of these schemes calls for a discussion of different problems and possible solutions.

A. *The Ipse/Idem Distinction*[79]

First, let us turn to the basic theoretical and philosophical discussion of identity, identification, and profiling in the digital age. When addressing this issue, scholars often note two meanings of identity: *ipse* identity and *idem* identity. The first term ("ipse") refers to a digital identity initiated by the relevant individual.[80] The second term ("idem") addresses instances where others collect and rely upon information they learn about the relevant individual, over time.[81] Clearly, our offline world includes interactions which are mixed and our identity is constantly being structured by both the subject and society.

The online realm, however, introduces a somewhat stark practical distinction among these two theoretical dynamics. In some instances, individuals carefully work to structure their identity and profile by providing various forms of data. This occurs on social networking sites where users carefully attend to their profile, or on e-commerce sites where users strive to assure a positive reputation. Such a dynamic could be easily referred to as the construction of an *ipse* identity and is the core of our discussion in this Article.

At times, in the online realm, profiles are structured exclusively by others, sometimes even without the relevant individual's actual knowledge. Often this is carried out through the use of unique tracking identifiers, such as a "persistent

---

[79] Arnold Roosendaal refers to a similar distinction noted by Roger Clarke between the "projected persona" and the "imposed persona." *See* ARNOLD ROOSENDAAL, DIGITAL PERSONAE AND PROFILES IN LAW 8 (2013) (quoting Roger Clarke, *The Digital Persona and Its Application to Data Surveillance*, 10 INFO. SOC'Y 77 (1994)).

[80] Hildebrandt, *supra* note 36.

[81] These concepts are attributed to Paul Ricoeur, and noted by Hildebrandt, *supra* note 36; *see also* Charles D. Raab, *Identity: Difference and Categorization*, *in* LESSONS FROM THE IDENTITY TRAIL, *supra* note 43, at 227–28 (distinguishing between identity defined by self and identity defined by others); Mary Rundle et al., *At a Crossroads: "Personhood" and Digital Identity in the Information Society* 8 (OECD, STI, Working Paper No. 2007/7, 2008), *available at* www.oecd.org/dataoecd/31/6/40204773.doc.

token"[82] installed on the user's device, which allow for tying all the individual's actions together into an overall mosaic.[83] Cookies, for example, allow for the tracking of online browsing, and for the tailoring of advertisements based on previous preferences.[84] "Flash cookies"[85] are newer adaptations of this basic tool.[86] The outcomes of this process could easily be considered as *idem* identities.

Idem identities raise a variety of important legal and policy questions, mostly in the context of information privacy and data protection. Lawmakers are striving to establish whether and how users should provide consent to the vast collection of personal information this process involves and how they might effectively signal they no longer want to participate in this dynamic (an issue referred to at times as the "Do Not Track" debate).[87] Other issues arising in this context are assuring users a right and ability to examine the information collected about them, or request its correction and even deletion.[88] In addition, the use of these dynamics generates concerns of possible discrimination and potential manipulation. This Article, however, chooses to set all these important issues aside. It opts for focusing on the *ipse* identity process—in which individuals fully embrace their online identities and profiles, and the unique legal and policy issues that follow.[89] Yet one should not worry that the issues here set aside will be left unattended. These privacy issues are gaining recognition. The identity aspects, however, are somewhat neglected and therefore require a focused analysis.

Before continuing, it is important to note that the distinction between these two forms of identity management is obviously blurry.[90] These two

---

[82] Froomkin, *supra* note 65, at 18.

[83] See James Grimmelmann, *First-Class Objects*, 9 J. TELECOMM. & HIGH TECH. L. 421, 424 (2011) for a discussion of "unique identifiers" and their origin. Grimmelmann notes that "[u]nique identifiers come from the world of databases, in which one seeks to store information about the world in a structured manner." *Id.* He further notes that unique identifiers are essential for "transforming messes of unstructured information into useful, structured data about people." *Id.* at 426.

[84] Froomkin, *supra* note 65, at 18.

[85] *Id.* at 18 n.69.

[86] *See* discussion in Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281, 292 (2012).

[87] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 4 (2012) [hereinafter FTC REPORT], *available at* http://ftc.gov/os/2012/03/120326 privacyreport.pdf.; *see also* Claudia Diaz, Omer Tene & Seda Gürses, *Hero or Villain: The Data Controller in Privacy Law and Technologies*, 74 OHIO ST. L.J. 923 (2013).

[88] *See generally* Rundle et al., *supra* note 81, at 33, 35, 50; *see also* Grimmelmann, *supra* note 83, at 430–34 (explaining that unique identifiers allow for automated reasoning, might empower individuals, yet also lead to negative aspects such as control and manipulation).

[89] Hildebrandt, *supra* note 36.

[90] For a similar point, see ROOSENDAAL, *supra* note 79, at 41 (noting the existence of many hybrid forms of identities today).

intermediation options do not present a dichotomy, but a matter of degree. In many instances, the models overlap. For example, many e-commerce websites track their users' behavior in order to present them with tailored advertisements and recommendations.[91] Some users might be unaware of these practices and are possibly annoyed and even intimidated when they learn of them. Others, however, might consider these applications as helpful "recommendation systems," "virtual shoppers," or even "butlers." In some of these cases (such as on Amazon.com), users are able to attend to structuring their profiles in a way that resembles the dynamics we will shortly describe. In such cases, some of the interests and concerns related to "*ipse* identities" are relevant as well.

Similarly, at times "*ipse* identity" intermediaries allow for the structuring of online profiles, yet take the liberty of collecting additional information about their users, or applying the information provided in ways their users did not necessarily understand (Facebook's Beacon fiasco is a clear example of this dynamic).[92] In other words, even in situations where the identity was structured by the individual, there are coinciding "*idem*" dynamics unfolding in the background. Therefore, the existence of an "*ipse* identity" intermediation dynamic does not mean that other issues, such as privacy or discrimination, should not be examined (yet, as mentioned, these matters are beyond the scope of this Article).

B. *Real Names Versus Stable Pseudonyms*

1. *Real Name IDs*

The internet famously promotes anonymous use and speech ("Nobody knows you're a dog").[93] However, a growing trend calls for the usage of "real names" in online interactions.[94] This dynamic is a direct result of a specific form of soft eID intermediation. In the following paragraphs we will discuss Real Name intermediation policies (mandatory vs. voluntary), and verification methods (ex ante vs. ex post). In addition, we will briefly elaborate upon the ways in which the use of Real Names alters the online experience.

---

[91] Froomkin, *supra* note 65, at 18.

[92] James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1147–48 (2009). *See generally* Woodrow Hartzog, *Social Data*, 74 OHIO ST. L.J. 995 (2013); Yang Wang et al., *From Facebook Regrets to Facebook Privacy Nudges*, 74 OHIO ST. L.J. 1307 (2013).

[93] Peter Steiner, *On the Internet, Nobody Knows You're a Dog*, NEW YORKER, July 5, 1993, at 61, *available at* http://www.condenaststore.com/-sp/On-the-Internet-nobody-knows-you-re-a-dog-New-Yorker-Cartoon-Prints_i8562841_.htm.

[94] Lilian Edwards, *From the Fantasy to the Reality: Social Media and Real Name Policies*, *in* FESTSCHRIFT FOR JON BING (forthcoming 2013), *available at* http://ssrn.com/abstract=2262272; Froomkin, *supra* note 65, at 17–18.

a. *Mandatory Versus Voluntary?*

Several dominant identity intermediaries (most famously, Facebook) issue and authenticate the users' online identity while contractually stipulating they will only do so if the identity managed is identical to the one the user applies in the physical world.[95] At times the intermediary moves to assure compliance with this request by sanctioning the relevant identity, changing its name, and even removing it from the platform if a breach in this policy is proven.[96]

The Real Names strategy of identity intermediation is not unique to the soft eID context. Quite to the contrary, up until recently, this model was considered the norm. Real names and IDs are used in personal communications, or in a commercial transaction which requires authentication for payment.[97] Banks, smart cards, and credit cards, not to mention national IDs and passports, all make use of Real Name IDs when issuing and validating means of identification.[98] Yet the online realm has introduced users to anonymous and pseudonymous identification. The fact that the internet offers other forms of identification which users might have grown accustomed to renders a shift to a mandatory Real Names policy a point of contention.[99]

Other intermediaries (such as Google+ or Amazon) are less aggressive and permit their users to make use of either Real Names or a pseudonym of their choice (a strategy we address below).[100] Here, when opting to use a Real Name, some services offer the option of signaling that their name was verified (an option made available, for example, by Amazon and Twitter).[101] It is noteworthy that the option of straying from the use of Real Names is not limited to soft eIDs or the online realm. For instance, some credit card companies allow for the issuing of a prepaid anonymous card.[102]

---

[95] Edwards, *supra* note 94; Froomkin, *supra* note 65, at 17–18. Froomkin specifically refers to Facebook's policy "against pseudonyms." *Id.* at 17. Facebook indeed notes that an individual may not use more than one ID. *See Statement of Rights and Responsibilities*, *supra* note 41, § 4.

[96] For a discussion of a patent issued to Google for the identification of fraudulent names, see Douglas Perry, *Google Gets Social Network Impersonation Detection Patent*, TOM'S GUIDE (July 19, 2012, 6:30 AM), http://www.tomsguide.com/us/google-patent-social-network-hack-fraud,news-15927.html.

[97] Davis, *supra* note 43.

[98] *Id.*

[99] Edwards, *supra* note 94 (manuscript at 9); danah boyd, *"Real Names" Policies Are an Abuse of Power*, APOPHENIA (Aug. 4, 2011), http://www.zephoria.org/thoughts/archives/2011/08/04/real-names.html.

[100] Another example of a firm which recently allowed the use of pseudonyms is FourSquare. *See* Greg Norcie, *Foursquare Updates TOS To Allow Pseudonyms*, NORCIE.COM (Jan. 30, 2013), http://norcie.com/2013/01/30/4sqwin/.

[101] Sengupta, *supra* note 1, at A3 (mentioning that Rushdie uses a Twitter verified account).

[102] *Gift Cards & Prepaid Cards*, AM. EXPRESS, https://www.americanexpress.com/us/content/merchant/get-support/prepaid-cards.html (last visited July 16, 2013).

The shift to a mandatory Real Name identification model in the online realm has generated dispute and discussion. The issue was aptly dubbed the "Nymwars."[103] One of the central points of tension came to light upon the introduction of Google's social network—Google+. Initially, Google+ required the registration of real names (thus opting for a mandatory Real Names regime).[104] After a flurry of criticism, Google eventually conceded this requirement and allowed the use of pseudonyms.[105] Facebook's mandatory Real Name identification has also been criticized. In Germany, for instance, this issue went beyond the public protest and social debate, eventually reaching the courts.[106] News reports indicate that the Data Protection Agency of the German state of Schleswig-Holstein sued Facebook for its prohibition of using pseudonyms, a right arguably provided by German law.[107] The case was eventually thrown out on jurisdictional grounds (as Facebook's European offices are in Ireland and thus subject to Irish, not German law).[108] Indeed, the German sensitivity toward this issue is reflected in an option enabled by German legislation (and technology) to register a pen name into a person's ID card in addition to his or her civil name.[109] This card allows German nationals to interact with various entities without revealing their "real name" (something Facebook users are currently unable to do).[110]

b. *Verification Methods*

The verification of the Real Name is carried out through the use of various strategies. Broadly, we note ex ante and ex post approaches. Some intermediaries require identification *before* using the Real Name. This mostly occurs when the Real Name is voluntary, and the user opts for its use specifically. At that point, a verifying badge is provided by the intermediary. Here we must again remember that these online ventures operate remotely and

---

[103] boyd, *supra* note 99.

[104] Eva Galperin, *2011 in Review: Nymwars*, ELECTRONIC FRONTIER FOUND. (Dec. 26, 2011), https://www.eff.org/deeplinks/2011/12/2011-review-nymwars.

[105] *Id.*

[106] Nick Clayton, *Facebook Pseudonym Ban Breaks German Law*, WALL. ST. J. TECH BLOG (Dec. 19, 2012, 7:12 AM), http://blogs.wsj.com/tech-europe/2012/12/19/facebook-pseudonym-ban-breaks-german-law/.

[107] *Id.*

[108] *See* Edwards, *supra* note 94; Natasha Lomas, *Facebook Wins Court Challenge in Germany Against Its Real Names Policy*, TECHCRUNCH (Feb. 15, 2013), http://techcrunch.com/2013/02/15/facebook-wins-court-challenge-in-germany-against-its-real-names-policy/.

[109] Gesetz über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften [PAuswG] [Act on Identity Cards and Electronic Identification], June 18, 2009, BUNDESGESETZBLATT, Teil I BGBL. I at 1348–50, § 5, no. 2, § 9, no. 3 (Ger.), *quoted in* GERRIT HORNUNG & JAN MÖLLER, PASSGESETZ PERSONALAUSWEISGESETZ 188–89, 207–08 (2011).

[110] *Id.*

need to overcome the challenges of scale and distance. One possible option, used for instance by Amazon, compares the name selected to the one appearing on the user's credit card previously used through the Amazon system. Here, in fact, the identity intermediary is relying on the original identification and authentication process carried out by the credit card company (which, in turn, greatly relies on authentication processes carried out by banks and credit agencies). In other instances, firms merely verify identity ex post—after a complaint was posted[111] or other indications of a possible breach of the "Real Names" policy. In these cases, firms tend to engage in a more aggressive inspection, such as requiring that copies of official state-issued papers indicating the name of the relevant user are sent to the intermediary.[112] Other sites engage in far more imaginative ways to verify user identity, such as presenting users with quizzes about their own (claimed) personal lives based on information found in public records.[113]

c. *Real Name eIDs: Unique Benefits and Uses*

The introduction of Real Name policies has impacted the online realm in several ways. First, the use of Real Names allows for an ongoing flow of reputational information from the online to the offline world; actions of an individual offline will be attributed to the online persona (and vice versa).[114] The use of Real Names enables speakers to easily capitalize on their offline social capital in an online world (and vice versa).[115] It instantly and simply allows individuals to move their offline social circles online.[116] Yet it also allows reputational harms to flow from the online realm to the offline one (and vice versa).[117] This flow of reputational information has a direct impact on the overall social discourse online. If mandated or broadly accepted, the use of Real Names can assure that online participants conduct themselves in a respectable manner, while understanding that the social (and, at times, legal) sanctions against unruly conduct in the online realm will follow in the offline realm as well, where they can impact one's actual life and liberty.[118] Yet this dynamic

---

[111] Facebook presents a button for reporting possible breaches of the Real Name policy.

[112] As occurred with Salman Rushdie in this Article's opening example. *See* Sengupta, *supra* note 1, at A3.

[113] *See* Sterritt, *supra* note 11, at 1726–27.

[114] *See* discussion in Tal Z. Zarsky, *Information Privacy in Virtual Worlds: Identifying Unique Concerns Beyond the Online and Offline Worlds*, 49 N.Y.L. SCH. L. REV. 231, 243 (2004). For a discussion and definition of the important role of reputation in the internet economy, see Eric Goldman, *The Regulation of Reputational Information*, *in* THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET 293, 295–96 (Berin Szoka & Adam Marcus eds., 2010), *available at* http://ssrn.com/abstract=1754628.

[115] *See* Zarsky, *supra* note 114, at 243.

[116] *Id.*

[117] *Id.*

[118] Interesting empirical work regarding this specific issue was made possible in South Korea, where a law (which was already repealed) generated a form of "Real Name Policy."

might also inhibit individuals from conducting themselves freely online and enjoying the social benefits such behavior might entail.

Furthermore, the use of Real Names generates another important dynamic when it meets the realm of social networks—it allows online users to signal and indicate the structure of real world/offline social graphs and their position within them. In doing so, individuals are able to signal their social stature (given the number of people they know, the actual people they know, or their centrality in a social network), or even enable others to authenticate their identity by indicating who can vouch for them.[119] This function is an important feature for websites such as LinkedIn, which are used for networking, job seeking, and recruiting.[120]

With the growing and successful use of Real Name policies, Facebook and other identity intermediaries have emerged as tools for identification and even authentication.[121] Consider the now-popular phrase, "Check out my Facebook page." In this statement, users encourage others to take the authenticated information available in the online realm, and apply it to other contexts (both online and offline). In fact, authentication via Facebook's identification system is a growing trend which is migrating to other models and websites. A broad variety of applications, such as online games, virtual worlds,[122] and other

---

See Daegon Cho & Soodong Kim, *Empirical Analysis of Online Anonymity and User Behaviors: The Impact of Real Name Policy*, *in* PROCEEDINGS OF THE 45TH HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES 3041, 3042–43, 3046 (2012), *available at* http://origin-www.computer.org/csdl/proceedings/hicss/2012/4525/00/06149194.pdf. Note that here users were only required to provide their names to the government and not to other users. *Id.* Researchers found decreases of some forms of antisocial behavior. *Id.*

[119] *See* discussion in John Brainard et al., *Fourth-Factor Authentication: Somebody You Know*, *in* PROCEEDINGS OF THE 13TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 168, 168–69 (2006), *available at* http://www.rsasecurity.ca/rsalabs/staff/bios/ajuels/publications/fourth-factor/ccs084-juels.pdf ("User authentication in computing systems traditionally depends on three factors: something you have (e.g., a hardware token), something you are (e.g., a fingerprint), and something you know (e.g., a password) . . . [T]his paper . . . explore[s] a fourth factor, the social network of the user, that is, *somebody you know*.").

[120] The existence of a social context or even a social graph alters a popular limitation of a "real name" identification scheme—that in many cases the mere usage of a Real Name cannot lead to an identification of a "real person," especially if the name is a popular one. Yet with the social graph and context, one has additional tools which will assist in verifying that the specific "John Doe" he is interacting with is the one he had in mind (the plumber from Berlin and not the singer from Paris, for instance).

[121] *See* Sengupta, *supra* note 1, at A3 ("Facebook insists on what it calls authentic identity, or real names. And it is becoming a de facto passport vendor of sorts, allowing its users to sign into seven million other sites and applications with their Facebook user names and passwords.").

[122] For a discussion, see Eva Galperin, *New Blizzard Forum Policy Will Require Posters To Use Real Names*, ELECTRONIC FRONTIER FOUND. (July 8, 2010), https://www.eff.org/deeplinks/2010/07/new-blizzard-forum-policy-will-require-posters-use.

websites[123] allow individuals to identify themselves using their Facebook username and password.[124] This dynamic indicates that problems with soft identity intermediation in one context (errors and all) spill over to other realms which rely upon the original identity intermediation process. This point illustrates the significance of the identity intermediation process, and perhaps, at times, the need for regulatory intervention.

In addition, the shift toward Real Names policies (especially if they are mandatory) generates vast benefits to the intermediaries themselves.[125] They are now vested with a rich corpus of knowledge—personal information pertaining to their users.[126] In addition, they also may track social ties and therefore gain insights into structures of power and measures of influence throughout society.[127] Recent reports have indicated the use of such knowledge in the 2012 presidential campaign,[128] following success in the commercial realm. At times, these insights might even be used to the users' detriment. Therefore, intermediaries might be "over-motivated" to shift users to a Real Names regime. If this model generates problems to users and society in general, the law might be required to somewhat chill such motivation.[129]

---

[123] The number of websites and platforms making use of the Facebook identification scheme is growing at a quick pace. Skype, Spotify, Netflix, Washington Post, and LinkedIn are only a few examples of the long list of these websites and platforms. *See also Integrating Facebook in iOS*, PARSE, https://parse.com/tutorials/integrating-facebook-in-ios (last visited July 16, 2013); Nick Margerrison, *UK Government To Use Facebook in "New" National ID Scheme*, DISINFORMATION (Oct. 5, 2012), http://disinfo.com/2012/10/uk-government-to-use-facebook-in-new-national-id-scheme/.

[124] For more on this dynamic see Simson Garfinkel, *Facebook Wants To Supply Your Internet Driver's License*, MIT TECH. REV. (Jan. 5, 2011), http://www.technologyreview.com/news/422285/facebook-wants-to-supply-your-internet-drivers-license/; *see also* Omer Tene, *Me, Myself and I*, 8 J. INT'L COM. L. & TECH. 118, 119 (2013).

[125] *See* Edwards, *supra* note 94, at 7–9.

[126] *Id.*

[127] *Id.*

[128] *See* Charles Duhigg, *Campaigns Mine Personal Lives To Get Out Vote*, N.Y. TIMES, Oct. 14, 2012, at A1, A18, *available at* http://www.nytimes.com/2012/10/14/us/politics/campaigns-mine-personal-lives-to-get-out-vote.html?pagewanted=1&hp.

[129] Note that at times the law itself might be encouraging a shift toward an identification scheme which calls for strictly gathering information about the users' real identity. For instance, according to a news report, a recent U.K. defamation law encourages user-generated content websites to gather information which enables victims to directly sue tortfeasors. Eric Goldman, *UK's New Defamation Law May Accelerate the Death of Anonymous User Generated Content*, FORBES (May 9, 2013, 3:05 PM), http://www.forbes.com/sites/ericgoldman/2013/05/09/uks-new-defamation-law-may-accelerate-the-death-of-anonymous-user-generated-content-internationally/. When doing so, the websites will qualify for the law's protection from the victims' claims. *See id.*

2. *Stable Pseudonyms*

Not all soft eID intermediaries or users make use of Real Names. As noted, some intermediaries allow users to assume an online identity, and interact while using a pseudonym, nickname, or "handle." For instance, in addition to using their Real Names, Amazon also allows users to make use of a "Pen Name."[130] This Pen Name could be used at all junctures throughout the Amazon website.[131] If the user chooses to change it, all references to such a name will change accordingly.[132] It is, in other words, a stable pseudonym linked to a specific user. Google's social networking site Google+ allows users, with some restrictions,[133] to identify themselves using pseudonyms and handles when interacting throughout the network. Here, the role of the identity intermediary is still important and substantial. It must assure that only the relevant and authenticated users have access to their handles. In these cases (assuming the relevant individual does not expose identifying information) there is no flow between the physical and online persona; whatever happens online, stays online.[134]

The benefits and concerns of this model are the mirror image of those discussed in the context of Real Names. It allows individuals to exercise pseudonymous speech and conduct, with all the possible advantages it entails. It also might generate some of the concerns related to uninhibited speech online. It allows for the structuring of elaborate social graphs, yet these are limited to online personas and therefore far less illuminating, especially for those viewing them externally.[135]

---

[130] *Help: About Pen Names*, AMAZON, http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=201145360 (last visited Sept. 13, 2013).

[131] *Id.*

[132] *Help: Edit Your Pen Name*, AMAZON, http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=14279641 (last visited Sept. 13, 2013).

[133] Violet Blue, *Google's Pseudonym Problem: New Implementation Revealed*, ZDNET (Jan. 26, 2012), http://www.zdnet.com/blog/violetblue/googles-pseudonym-problem-new-implementation-revealed/992.

[134] One might note that the mere option of Real Names—even if they are voluntary—will lead to a dynamic that eventually shifts the entire discourse to Real Names. This will result from an "unraveling effect" in which trusted users will shift to the use of Real Names given the fact that they have "nothing to hide." Thereafter, those using pseudonyms will be treated with suspicion, pressuring these pseudonymous users to shift to Real Names as well, and so on. For more on this "unraveling effect" in a somewhat different context, see Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus & the Threat of a Full Disclosure Future*, 105 NW. U. L. REV. 1153, 1176–90 (2011). It is unclear whether this dynamic will indeed transpire in this context, and for that reason this issue is not addressed further in this Article.

[135] It is possible that firms controlling the social graph are able to establish the users' identity or other personal traits from their location within the social graph. This important point is beyond our current discussion.

In addition, the growing importance of individuals' actions in the online realm now generates novel forms of identity interests—interests solely relating to the online identity. Maintaining trust and reputation within the online realm is an important objective on its own.[136] It may have substantial emotional and even monetary implications for avid online users. For instance, in virtual marketplaces, such as eBay, the individual's livelihood might depend on maintaining a sound online persona.[137] A tarnished identity will lead to a slide in sales and even abolishment from the marketplace. Returning to the market with a new identity will hardly prove helpful. Newcomers with clean histories are treated with suspicion.[138] Beyond the business realm and in other contexts, the implications are personal and social. For instance, in the context of multiplayer online games or other realms of ongoing social interaction, tarnishing the online identity could inflict severe grief upon the relevant individual. These are realms in which the individual spends many hours of human interaction, invests social capital and in some instances forms strong ties with other participants. These are all jeopardized when the integrity of the individual's virtual identity is compromised.[139]

Upon concluding this part, we note that intermediaries enabling the use of stable pseudonyms collect vast amounts of personal information as well. While this intermediation model does not call for sharing the users' Real Name with others, these intermediaries might be collecting information connecting the online persona to the pseudonym of choice directly from its users through various factors which are accessible to them.[140] They might also be privy to the social graph formulating among their users. However, the knowledge intermediaries accumulate here will not be as insightful as that made available

---

[136] *See* discussion in Zarsky, *supra* note 114, at 251.

[137] Daniel H. Kahn, *Social Intermediaries: Creating a More Responsible Web Through Portable Identity, Cross-web Reputation, and Code-Backed Norms*, 11 COLUM. SCI. & TECH. L. REV. 176, 186 (2010).

[138] Paul Resnick et al., *The Value of Reputation on eBay: A Controlled Experiment*, 9 EXPERIMENTAL ECON. 79, 97–98 (2006), *available at* http://link.springer.com/article/10.1007%2Fs10683-006-4309-2 (arguing that a public profile, even one that includes negative feedbacks, is preferable to a blank profile).

[139] F. Gregory Lastowka & Dan Hunter, *The Laws of the Virtual Worlds*, 92 CALIF. L. REV. 1, 6, 63, 67 (2004). Note, however, that policy decisions recognizing the value and importance of the virtual persona should perhaps also reflect society's attitudes towards the extensive usage of such online realms. If over-usage of these online realms is considered wasteful, perhaps the recognition of such virtual reputation should be limited. It also should be noted that, at times, the virtual reputation might "bleed" into the real name behind the pseudonym. Therefore, the importance of these virtual personas might be even greater. For a discussion of this dynamic in a somewhat different context, see Jennifer E. Rothman, *The Inalienable Right of Publicity*, 101 GEO. L.J. 185, 217 (2012) ("People have multiple identities (both public and private) that they perform. These different identities are not separable from one another; instead, the boundaries are fluid and flow in and out of one another." (footnote omitted)).

[140] Such as IP addresses, credit card information, email addresses, and mandatory or voluntary registration.

with Real Name intermediations. With pseudonymity available, networks might overlap, as individuals might appear several times in various networks, while using different names.

IV. THE BENEFITS AND PITFALLS OF SOFT EID INTERMEDIATION

To establish the proper regulatory scheme for identity intermediation, we must understand whether such regulation or legal intervention might promote an important social purpose.[141] For that, we must recognize the benefits of competent intermediation, and the detriments of negligently (or purposefully) failing to carry out this role. We begin with a very brief normative overview of possible benefits, and thereafter map out how they could be compromised, drawing from both the theoretical analysis carried out above and actual instances which occurred in previous years, as noted by both the courts and the press.

A. *The Benefits of Soft eIDs: Economic, Personal, and Social*

The benefits[142] of soft eID intermediaries and intermediation emerge on several dimensions. The first benefit is *economic*—related to the enablement of transactions and commerce in a trusted environment. While digital anonymity generates vast benefits, it might inhibit commerce given the lack of information regarding the parties involved. For instance, in the context of buyer to customer (B2C) transactions, vendors might suffer from their inability to know their (anonymous) customers well enough online. In such a case both transacting parties are subject to high search costs while seeking out an optimal transaction. With stable identities, vendors are able to tailor offers and advertisements on the basis of identity traits, and provide consumers with what they are most likely to purchase (note of course that this final assertion is easily subjected to powerful critiques).[143]

Identity intermediation is far more important in the customer to customer (C2C) context. Virtual marketplaces, such as eBay, rely upon stable identities for both buyers and sellers so as to generate trust.[144] C2C markets do not enable

---

[141] For a somewhat different mapping of the benefits and concerns of electronic identities, as set forth by the British Government, see CABINET OFFICE, PRIVACY AND CONSUMER ADVISORY GROUP: DRAFT IDENTITY ASSURANCE PRINCIPLES (2013) (U.K.), *available at* https://www.gov.uk/government/consultations/draft-identity-assurance-principles/privacy-and-consumer-advisory-group-draft-identity-assurance-principles.

[142] Perhaps the most basic and intuitive benefit of these tools is that they generate personal enjoyment and wellbeing. This is evident from the massive and extensive participation in these social networks. The analysis, however, must go beyond this point and examine whether additional benefits arise.

[143] Tailored advertising and marketing might upset consumers or lead to biased outcomes. It might also allow marketers to discriminate and manipulate the public.

[144] See also discussion as to how eBay and other websites use various measures to capture "word of mouth." Reputation systems play an important role in achieving this

the collection of and reliance upon physical cues which provide information regarding the nature and trustworthiness of both sellers and buyers—information societies have relied upon for centuries. Functioning identity intermediaries promote efficiency in these markets by enabling the creation of trust on the basis of previous transactions—all linked to a constant online identity. Thus, these intermediaries, at least in theory and in this context, enhance efficiency and promote commerce.[145]

Identity intermediation might hold many benefits with regard to other important aspects, such as the protection of *personality (identity)* interests,[146] the development of individual *autonomy*, or advancing human *rights*.[147] Identity is inextricably linked to our personality, embodying both an interest and right, collectively categorized as personality rights. The latter are "private law (subjective) rights which are by nature non-patrimonial and highly personal in

---

objective. Eric Goldman, *Online Word of Mouth and Its Implications for Trademark Law*, *in* TRADEMARK LAW AND THEORY: A HANDBOOK OF CONTEMPORARY RESEARCH 404, 411–12 (Graeme B. Dinwoodie & Mark D. Janis eds., 2008), *available at* http://ssrn.com/abstract=1020695.

[145] The text does not specifically address a salient form of identity intermediaries: dating websites. Indeed these websites might be in a category of their own. On the one hand, they promote social interactions which have important benefits (that are somewhat different than those addressed in the text). In addition, misrepresentations carried out within them can seriously hamper individuals' wellbeing. On the other hand, they are commercial ventures and therefore protecting the nature of the identities promotes the business objectives of the website operators. For these reasons, they might require a separate analysis and discussion. For some additional sources regarding this specific matter, see Susan Haigh, *States Seek To Make Online Dating Safer with New Laws*, HUFFINGTON POST (Apr. 21, 2011, 7:25 AM ET), http://www.huffingtonpost.com/2011/04/21/online-dating-laws_n_851946.html; Anita Ramasastry, *Legislating Love Online: Should States Mandate that Online Dating Sites Do Criminal Background Checks of Their Users?*, FINDLAW (Sept. 28, 2006), http://writ.news.findlaw.com/ramasastry/20060928.html. For a recent law passed in New Jersey regarding such sites, see Internet Dating Safety Act, N.J. STAT. ANN. § 56:8–1, 168 (West 2012).

[146] Roscoe Pound, *Interests of Personality*, 28 HARV. L. REV. 445, 445–46 (1915); *see also* J. NEETHLING ET AL., NEETHLING'S LAW OF PERSONALITY 39 (1996) ("Identity as an interest of personality can be defined as a person's uniqueness or individuality which identifies or individualises him as a particular person and thus distinguishes him from others. Identity is manifested in various indicia by which that particular person can be recognised; in other words, facets of his personality which are characteristic of or unique to him, such as his life history, his character, his name, his creditworthiness, his voice, his handwriting, his appearance (physical image), etcetera. A person has a definite interest in the uniqueness of his being and conduct being respected by outsiders." (citations omitted)).

[147] For the argument in favor of an explicit and specific right to identity and the debate on the need and desirability of considering it (or upgrading it to) a human right, see Norberto Nuno Gomes de Andrade & Paul De Hert, *Proposing a Right to Identity Within the International Framework of Human Rights: Issues and Prospects*, *in* NEW TECHNOLOGIES AND HUMAN RIGHTS 231, 231 (Mario Viola de Azevedo Cunha et al. eds., 2013); *see also* Paul Bernal, The Right to Online Identity 2 (Sept. 7, 2012) (unpublished manuscript) (University of East Anglia (UEA), Norwich Law School, Working Paper), *available at* http://ssrn.com/abstract=2143138 (referring to documents written by the United Nations and the ECHR).

the sense that they cannot exist independently of a person since they are inseparably bound up with his personality."[148] Under the broader notion of personality rights, many European countries established a right to personal identity in their legal systems.[149] It is precisely the idea of the uniqueness and singularity of the human being that has conferred to the right to personal identity its own conceptual autonomy within the group of personality rights to which it belongs. Apart from control over the several indicia of one's identity,[150] the right to identity presupposes a "definite interest in the uniqueness of his being."[151]

Well-functioning identity intermediaries of the forms noted above are crucial for protecting individuals' personality interests, namely their specific identity interests. Faulty identity intermediation systems may exacerbate the ways through which a person's identity can be distorted, deleted, stolen, misappropriated, impersonated, falsified, and misrepresented, rendering it increasingly vulnerable.[152] In sum, this right cannot be exercised when the intermediaries' activities are compromised.

In the internet context and beyond, scholars have noted the importance of providing individuals with the opportunity to develop their identities, preferably using different identities for different audiences and social contexts (and indeed this aspect might be compromised when Real Names are mandated).[153] Identity "development" can be understood as the ability to "create" and "assert"[154] or "construct[]" and "manage[]"[155] the online profile. Others explain how these virtual identities could be used for articulation and exploration and thus enhance

---

[148] Johann Neethling, *Personality Rights: A Comparative Overview*, 38 COMP. & INT'L L.J. S. AFR. 210, 223 (2005).

[149] In fact, the right to identity has been recognized *eo nomine* in countries such as Italy, France, Switzerland, South Africa, and Portugal. *Id.* at 235. Regarding the latter, the right to personal identity is explicitly enshrined in PORT. CONST. art. 26, § 1:

> Everyone shall possess the right to a personal identity, to the development of their personality, to civil capacity, to citizenship, to a good name and reputation, to their likeness, to speak out, to protect the privacy of their personal and family life, and to legal protection against any form of discrimination.

[150] William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. ILL. L. REV. 1105, 1132 (addressing the importance of identity control, which he sees as an extension of the self, and noting that this interest could even be derived from the seminal privacy article by Warren and Brandeis); *see also* Mark P. McKenna, *The Right of Publicity and Autonomous Self-Definition*, 67 U. PITT. L. REV. 225, 282 (2005).

[151] NEETHLING ET AL., *supra* note 146.

[152] In addition, the need to ensure the proper functioning of identity intermediaries is also related to what Oreg has defined as a "right to information identity." *See* Oreg, *supra* note 19, at 2 ("the right of an individual to the functionality of the information platforms that enable others to identify and know him and to remember who and what he is").

[153] ROOSENDAAL, *supra* note 79, at 46 (referring to the ability to engage in "representation," and drawing on the work of Erving Goffman).

[154] *See* Bernal, *supra* note 147.

[155] Grimmelmann, *supra* note 92, at 1152–53.

autonomy.[156] Again these are all objectives that a well-functioning identity intermediary can forward.

In addition, and beyond individual rights, identity intermediaries can play an important role in promoting a rich *social discourse*, which in turn can advance *democracy* and *speech-related interests*. Soft eIDs have proven constructive in creating and maintaining social ties of various strengths (given the ability to signal social stature and other important attributes). Furthermore, they provide a powerful platform for creating and diffusing ideas and expressions. With these social ties in place and given the digital technology available, the internet already provides for easy, cheap, and sophisticated ways to communicate. Yet identity intermediaries allow for the enhancement of such communications, given the ability to interact with others while understanding what they did and said in the past, acknowledging their social graph and recognizing they will maintain a stable online persona.

Yet before proceeding it is important to note that extensive usage of soft eIDs, especially as Stable Pseudonyms (rather than Real Names), might prove harmful to weaker segments of society—such as minorities and women. When no one is held accountable and social norms of civility cannot be enforced, the ugly face of society surfaces. The contribution of pseudonymous social networks (which are enabled by eIDs) to such attacks unfolds on two levels: either by abusing minorities and women within the social network, or by planning harmful activities against individuals outside the social network.[157] Both outcomes are enabled by an intermediation system which allows for maintaining an inner circle of trust and acquaintance on the inside, and a mask of anonymity on the outside. For that reason, we must be cautious of excessive efforts to enable and even immunize these forms of identity intermediation.

B. *Identity-Related Harms and Soft Identity Intermediaries*

After broadly noting the interests identity intermediaries promote, we can now move to address harms which arise when the intermediation process is interrupted or "attacked." For our discussion of this matter, and its relation to the process of soft eID intermediation, we chose to focus on two groups of concerns: those generated by third parties, and those directly resulting from the problematic actions of the intermediary.[158]

Beyond these issues (and the discussion of the Article) is the common concern often noted in this context—that of information privacy and security. These relate to questions as to how the information could be used by the

---

[156] *See generally* SHERRY TURKLE, LIFE ON THE SCREEN: IDENTITY IN THE AGE OF THE INTERNET 177–255 (1995).

[157] Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 64, 75 (2009).

[158] Bernal, *supra* note 147, at 13 (offering the following three categories of online identity interests which require protection: (1) protecting harm to that identity, (2) protection from impersonation, (3) protecting links between online and offline identity). We address all of these elements and more in the analysis below.

platform operator and shared with third parties. In addition, they address how information must be stored, when it should be passed on to government, and when it should be deleted. The privacy related issues are broad and complex. In some contexts, the privacy-based analysis will overlap with the issues discussed here. Indeed, similar broad interests—such as promoting autonomy, expression, and democracy—are shared by both privacy and the property/identity/dignity interests we now address. Yet this Article sets these privacy-related matters aside, and turns to interests which were not necessarily integrated into existing privacy law and even theory—the identity rights of virtual and pseudonymous identities.

1. *Identity, "Virtual Identity" Theft and Fraud, and the Possible Role and Responsibility of the Intermediary*

An intuitive concern which arises when dealing with systems that generate identities and strive to create trust is that the identities' integrity might be compromised (a practice recently dubbed as "e-personation").[159] Over time, and as these failures become public, the intermediation process's trust will be undermined. Without trust, none of the economic, personal, and social benefits noted above will follow, and the rights noted above will not be protected. In addition and as explained below, these concerns generate various harms to the relevant parties involved.

Several variations of these concerns come to mind. Let us consider situations in which (1) a soft eID is hijacked; (2) a soft eID is formulated so as to impersonate another; (3) a virtual identity engages in identity misrepresentation vis-à-vis its physical identity.[160] We briefly explain these three concerns and how such attacks might unfold. We also explain how the intermediaries' conduct indirectly impacts the likelihood of these events. In doing so, we will distinguish between Real Name identities and those that are merely Stable Pseudonyms. Throughout our discussion, we also briefly discuss the current role of law in battling or enabling these dynamics.

---

[159] *See, e.g.*, Anita Ramasastry, *Does Match.com Have To Make Sure Its Member Profiles Are Real and Accurate?: Why a Federal Judge Correctly Ruled No*, VERDICT (Sept. 11, 2012), http://verdict.justia.com/2012/09/11/does-match-com-have-to-make-sure-its-member-profiles-are-real-and-accurate.

[160] While the concerns noted and the distinctions among them are of greatest relevance in the online realm, they are reflected, at times, in the offline realm. For instance, note *Flores-Figueroa v. United States*, 556 U.S. 646 (2009). In this case, the Supreme Court examines whether an individual using counterfeit identification papers needs to "know" that the social security numbers included are merely false, or belong to someone else in order to be found guilty of "aggravated identity theft" (and thus receive an extended sentence). *Id.* at 647. In other words, the Court examines some aspects of the distinction between impersonation and identity misrepresentation. We thank James Grimmelmann for making this point.

Before proceeding, a short general note as to the current role of the law regarding these matters and the role of intermediaries: At present, the relevant intermediaries try to "lawyer away" the implications arising from the problems mentioned. Amazon, for instance, confronts the risk that these problems will harm their users and subject Amazon itself to liability claims by acknowledging these issues in its terms of use. Amazon specifically stipulates that it is a "passive conduit" and that it "cannot and do[es] not warrant, verify or guarantee the quality accuracy or integrity of information" the users may access.[161] Thus, according to such contractual language, the individual's reliance on the intermediary's authentication systems should be limited and the intermediary should not carry any liability. Yet the existence of contractual provisions should not "close the book" on these discussions. Courts might find that these provisions, as being part of a contract of adhesion, should not be upheld. In addition, courts might allow third parties to bring action against the intermediary given their reliance on the identification and authentication process (and limit the immunity provided through tort law via Section 230 of the CDA). Therefore, the following policy analysis is crucial for responding to these and other open and unfolding legal questions.

The *first* variation of these forms of identity concerns involves the hacking and hijacking of an eID. Here, an adversary accesses the user's account and assumes his or her identity, via the relevant intermediary. The "hacker" can then move to tarnish the user's reputation, or to carry out other attacks undetected. The hacker might abuse this situation so as to also attack third parties who trust the original user (yet not the attacker). The reputational damage caused to the victim is severe. It goes beyond negative content stated about him or her in the online realm. The damage is exacerbated due to the fact that the negative statements are actually attributed to the specific individual. In addition, the victim in many instances is harmed by the sense of self violation and loss of control over an identity, which comes with this form of attack.[162] Finally, given the possible impersonation such a hack enables, financial losses might of course

---

[161] *See Profile and Community Guidelines*, AMAZON, http://www.amazon.com/gp/help/customer/display.html?ie=UTF8&nodeId=14279631 (last visited July 20, 2013); Facebook notes this point, while generally stating that:

> WE TRY TO KEEP FACEBOOK UP, BUG-FREE, AND SAFE, BUT YOU USE IT AT YOUR OWN RISK. WE ARE PROVIDING FACEBOOK AS IS WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES INCLUDING . . . WE DO NOT GUARANTEE THAT FACEBOOK WILL ALWAYS BE SAFE, SECURE OR ERROR-FREE . . . FACEBOOK IS NOT RESPONSIBLE FOR THE ACTIONS, CONTENT, INFORMATION, OR DATA OF THIRD PARTIES, AND YOU RELEASE US, OUR DIRECTORS, OFFICERS, EMPLOYEES, AND AGENTS FROM ANY CLAIMS AND DAMAGES, KNOWN AND UNKNOWN, ARISING OUT OF OR IN ANY WAY CONNECTED WITH ANY CLAIM YOU HAVE AGAINST ANY SUCH THIRD PARTIES.

Statement of Rights and Responsibilities, *supra* note 41, § 16(3).

[162] *See* Smith, *supra* note 11.

follow. Damages can go beyond the victims of the hijacking and include third parties that relied on actions and statements made during the impersonation process. These third parties might have trusted the original identity holder and taken action based upon the instructions, insights, or advice of a hacker. Their reliance upon a mistaken identity might have caused them monetary or other losses, possibly due to the negligence of the identity intermediary.

Identity hijacking cases are already reaching the courts. This was the case with *In re Rolando*, which involved a new addition to the California Penal Code—Section 528.5.[163] Rolando used a password he received (without his actual solicitation) to access the victim's Facebook account and altered it "in a vulgar manner."[164] Rolando was found criminally liable.[165] Similar cases and new laws have been introduced in other states as well to address these instances. The actions noted might also constitute an "unauthorized access" to the victim's account. In these cases, such actions will be considered a breach of anti-hacking laws (most notably, the CFAA).[166] Yet the complex legal question as to whether these laws[167] will apply has led to the specific criminal laws mentioned. Finally, the acts of hacking and unauthorized usage are clearly contrary to the relevant eID intermediary's terms of use or service[168] (although the actor might not be in privity with the relevant intermediary given the fact that the account is being hacked, and therefore the discussion of contractual remedies might not be of relevance).

As this example and others demonstrate, attackers could try to obtain the subject's password through social engineering or other illicit measures. They could also try to attack the relevant website's security directly. Or, they might have received access from a third party.[169] In some of these cases, the intermediary's architecture and vigilance (for instance the level of security measures that a relevant intermediary uses) can clearly impact the extent of this form of risk and the damages that follow. Therefore, the intermediary should perhaps be considered responsible, even liable, for these actions and their consequences.

A final interesting point concerns the Real Name/Stable Pseudonym distinction. The issue at hand is usually associated with the abuse of Real Name

---

[163] CAL. PENAL CODE § 528.5 (West 2013) (also allowing for filing a civil action, claiming punitive damages and attorney's fees).

[164] *In re* Rolando S., 197 Cal. App. 4th 936, 939 (2011).

[165] *Id.*; *see also* Owen J. Sloane & Rachel M. Stilwell, *Online Impersonation*, GLADSTONE MICHEL, ALC, http://www.gladstonemichel.com/onlineimpersonation.shtml (last visited July 17, 2013).

[166] 18 U.S.C. § 1030(c)(2)(B)(ii) (2006). The issue of applying the CFAA to these situations is beyond the confines of this Article.

[167] *See infra* note 201 and accompanying text.

[168] *Statement of Rights and Responsibilities*, *supra* note 41, § 3(5) ("You will not . . . access an account belonging to someone else.").

[169] Very difficult questions arise when the victims themselves were the ones providing access information to the "hacker" who moved on to betray their trust. We will not address this thorny matter (which might arise when couples break up) in this Article.

systems (as in the *Rolando* example noted above). With Real Name identities at stake, a breach of the virtual identity can lead to serious "real world" implications: severe financial losses in all aspects of life, considerable reputational harms, and a strong visceral sense of the violation of a personal space. In addition, damages to third parties are foreseeable in this case as individuals might wrongfully rely upon an offline identity they already know.

Yet it is also possible that these harms pertain to the hacking of stable pseudonyms as well (perhaps to a lesser degree). For instance, in the much-cited "Rape in Cyberspace" incident (as reported by Julian Dibbell, in which a male individual took over a female's avatar and proceeded to engage in a virtual sexual assault),[170] the relevant individuals reported a strong sense of harm and a real-world trauma (note that this case probably did not involve actual hacking but abuse of an existing loophole in the system). Therefore, even those using stable pseudonyms can suffer actual hardship when such breaches occur, which in turn might transform into actionable legal rights.[171] In addition, for those using pseudonyms or handles when engaging in e-commerce, the hijacking of their digital identity could lead to serious financial losses, even though they are confined to the online realm. Finally, the hacking of a stable pseudonym might impact third parties. This will occur when third parties develop a relationship (be it economic, personal, or social) with the stable pseudonym and rely upon the information it conveys (regardless of the nature of the identity of the physical individual behind it).

The *second* concern arising from identity intermediation addresses situations in which a physical person's identity is assumed by another. Rather than hijacking an existing account, the attacker creates a new account under the name of another and thereafter impersonates her identity in the virtual realm.[172] The detriments of this outcome are quite similar to those mentioned above. The relevant victim suffers from the financial, social, and personal harms of impersonation. Such harms have been found to compromise basic human rights in some countries. In Germany, for instance, such damages are considered as impeding on one's "right to a name"—a right provided in Section 12 of the German Civil Code.[173]

---

[170] Julian Dibbell, *A Rape in Cyberspace: How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society*, VILLAGE VOICE (Oct. 18, 2005), http://www.villagevoice.com/2005-10-18/specials/a-rape-in-cyber space/.

[171] Jack M. Balkin, *Virtual Liberty: Freedom To Design and Freedom To Play in Virtual Worlds*, 90 VA. L. REV. 2043, 2062–63 (2004) (addressing the applicability of tort and speech related crimes in virtual spaces).

[172] At times, the "impersonator" chooses to generate an identity in the name of another—but chooses to leave it dormant. Here the "impersonator" might be striving to engage in "identity squatting"—causing the individual to pay the impersonator to provide him or her access to the identity carrying their actual name. We will not be addressing this specific matter in this Article.

[173] BÜRGERLICHES GESETZBUCH [BGB] [CIVIL CODE], Jan. 2, 2002, BUNDESGESETZBLATT [BGBL. I] at 2909, *amended by* BGBL. I at 1600 (Ger.). This powerful

However, the damages in this situation are less severe than those noted above. Here, the victim is not subjected to the actual sense of violation which comes with the overtaking of an active persona.[174] On the other hand, the damages here might be more severe to individuals who are unaware of the impersonation. Such impersonation might transpire for a lengthy period of time unbeknownst to them and for that reason users will not take action (as opposed to the instance of identity hijacking which the individual can learn of quite quickly given his inability to access his own account). In this case damages could even exceed those of the previous variation discussed.

Impersonation may involve possible damages to third parties as well—all similar to the damages discussed with regard to the concern above. Again, it is difficult to ascertain which of these concerns is more severe. Intuitively, damages of impersonation might be lighter, as the reliance on an identity structured by an impersonator would be lesser than reliance upon an identity structured by the actual individual and hacked at a specific point.[175]

Clearly, the impersonation here discussed is normatively problematic, although legal issues are somewhat more complex for famous names, or for those of celebrities. Assuming the identity of another, at times, might constitute a political or social statement (and therefore to a certain degree allowed as a form of satire even though damages to both the subject of impersonation and third parties might follow).[176]

The concerns here noted are not only theoretical, but have reached the courts as well. For example, news reports indicate the indictment of a New Jersey woman who set up a fake Facebook page under her ex-boyfriend's (a police officer) name.[177] She then proceeded to write derogatory comments (that were therefore assumedly written by her ex).[178] The woman was charged with

---

premise in German law can provide a fertile ground for causes of action. Indeed, in a recent case in the Regional Court of Cologne, the court has responded to a celebrity's request, and ordered Twitter to remove an account impersonating this celebrity. Oberlandesgerichte [OLGZ] [Regional Court of Cologne] July 18, 2011, RECHTSPRECHUNG DER OBERLANDESGERICHTE IN ZIVILSACHEN [31 O 396/11] (Ger.).

[174] *See, e.g.*, Smith, *supra* note 11.

[175] As those familiar with the actual individual behind the online persona would be able to notice that the identity is fraudulent, as opposed to instances of hacking, in which the identity was initiated by the actual individual.

[176] For a call for exceptions in identity theft and impersonation laws for these situations in the state of Pennsylvania, which might include an exemption for parody, see Melissa Daniels, *Fake Facebook Profiles Could Be Criminalized*, PA. INDEP. (Sept. 20, 2012), http://paindependent.com/2012/09/fake-facebook-profiles-could-be-criminalized/. Note, however, that this question is somewhat complicated in the age of "reality TV" and instant-celebrities.

[177] Gregory J. Krieg, *"Scum with a Gun": Facebook Fraud Case Heats Up New Jersey*, ABC NEWS (Nov. 2, 2011, 6:13 PM), http://abcnews.go.com/blogs/headlines/2011/11/scum-with-a-gun-facebook-fraud-case-heats-up-new-jersey/; David Porter, *NJ Woman Fights Charge over Fake Facebook Page*, N.J. NEWS (Oct. 26, 2011), http://abclocal.go.com/wabc/story?section=news/local/new_jersey&id=8407195.

[178] Porter, *supra* note 177.

fourth degree identity theft.[179] States such as California[180] and New Jersey have amended existing statutes to specifically refer to these forms of impersonation through social networks (these statutes require impersonation with the attempt to cause harm, intimidate, threaten, or defraud as a cause of action).[181]

In many cases, the impersonation acts noted here also constitute a breach of the identity intermediary's terms of use. When Real Name policies are applied, the individual agrees that she is not misrepresenting herself when providing her name and other personal information. Therefore, in these cases, upon learning of the misrepresentation, the identity intermediary can subject the impersonator/user to the relevant contractual remedies noted in the relevant terms of use, which mostly also include the right to terminate the relevant account.[182] Thus, the acts of private parties can potentially limit the problems at hand.

Arguably, such actions also constitute a breach of anti-hacking laws (most notably the CFAA)[183] and therefore bring forth the civil and criminal sanctions the law includes; when accessing an identity profile while providing false information, one is possibly engaging in "unlawful access." While some prosecutors have considered this legal construct, applying anti-hacking laws in these cases might prove to be somewhat of a stretch.[184]

---

[179] *Id.*

[180] These laws have already led to prosecutions of individuals setting up fake Facebook pages under the name of others so as to intimidate them. *See* Ramasastry, *supra* note 159.

[181] James Esposito, *Woman Faces up to 18 Months in Prison for Fake Facebook Page*, KNOWEM (Nov. 4, 2011), http://knowem.com/blog/2011/11/04/woman-faces-up-to-18-months-in-prison-for-fake-facebook-page/.

[182] *See Statement of Rights and Responsibilities*, *supra* note 41, § 4(1)–(2) (stating that a user will not provide any false personal information on Facebook, or create an account for anyone other than himself without permission, and will not create more than one personal account). Section 4(10) stipulates that if user selects a username, or similar identifier, for her account or Facebook page, Facebook reserves the right to remove or reclaim it if they find such action appropriate. *Id.* § 4(10). Section 15 grants Facebook the right to stop providing the user all or part of Facebook services if the user violates the letter or spirit of the Statement of Rights and Responsibilities, or otherwise creates risk or possible legal exposure for Facebook. *Id.* § 15. The same section also stipulates that the aforementioned section 4 (amongst others) will apply even in such cases that Facebook's *Statement of Rights and Responsibilities* shall terminate. *Id.*

[183] 18 U.S.C. § 1030(c)(2)(B)(ii) (2006).

[184] *See* Orin S. Kerr, *Should Faking a Name on Facebook Be a Felony*, WALL ST. J., Sept. 14, 2011, http://online.wsj.com/article/SB10001424053111903285704576562294116160896.html. The nature of the law regarding the question as to whether breaching terms of use could be considered "unlawful access" is unclear and courts are split on this issue, especially in the employment context. *See* Lori Romer Stone, *Using the Computer Fraud & Abuse Act To Protect Law Firm Data*, LAW PRAC. TODAY (Mar. 2012), http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/march12/using-the-computer-fraud-and-abuse-act-to-protect-law-firm-data.html.

While impersonation is a result of the malicious acts of a third party (setting aside the case for satire and parody of the famous),[185] it again is impacted by the actions and oversights of the identity intermediary. Here, the problematic outcome unfolded due to the intermediary's lack of successful identification and authentication of the registering individuals. It is interesting to note that although the concerns mentioned here and above might seem very similar to the untrained eye, they result from very different potential omissions and inactions on behalf of the identity intermediary. They therefore might call for different regulatory responses.

Arguing that the damages and concerns here noted resulted from actions and omissions of the identity intermediaries did not succeed in court. Beyond suing the impersonators, at times victims turned to bring action against the relevant platform themselves, but often met the brick wall of Section 230 immunity. In one famous case, *Carafano v. Metrosplash.com, Inc.*,[186] a "prankster" set up a fake profile for actress Christianne Carafano (of *Star Trek* fame) on an online dating website (Matchmaker.com). He proceeded to also include her real personal and contact information on her profile page, and noted that she was seeking an "unconventional liaison."[187] Carafano sued the website for defamation and other speech-related torts as well as for negligence.[188] Yet the court found that the website was not liable, while applying the abovementioned Section 230.[189] The court further noted that the website did not encourage this outcome in any way.[190] Below we will examine whether these legal outcomes should be reconsidered.

Finally, we examine this "impersonation" concern in light of the Real Name/Specific Pseudonym distinction. Clearly, the concerns noted pertain to identity intermediaries applying Real Names. Here, one user can clearly register

---

[185] For arguments to assure that free speech interests are protected while moving to limit the concerns here discussed, see Ramasastry, *supra* note 159.

[186] Carafano v. Metrosplash.com, Inc., 339 F.3d 1119, 1121 (9th Cir. 2003).

[187] Carafano v. Metrosplash.com, Inc., 207 F. Supp. 2d 1055, 1061 (C.D. Cal. 2002).

[188] *Id.* at 1055. The negligence claim is discussed in depth by the District Court. It explains that the negligence claim "stems from the alleged injurious falsehood of the Profile." *Id.* at 1077. Yet because the defamation claim fails in view of lack of "malice" (given the fact that this was a public figure) the negligence argument cannot stand. *Id.* at 1073. The court did not accept the argument that damages here go beyond the defaming words stated (as opposed to the text and analysis above that notes other sources of damages beyond these actual words). *Id.* at 1072.

General negligence claims are often dismissed on the basis of the "immunity" provided by Section 230 of the CDA. *See* David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 452 (2010) (noting, as an example, Doe v. MySpace, 474 F. Supp. 2d 843, 852 (W.D. Tex. 2007)).

[189] *Carafano*, 207 F. Supp. 2d at 1064.

[190] Another famous Section 230 case involved a similar fact pattern. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1099 (9th Cir. 2009). In *Barnes v. Yahoo!*, a false identity was created and Yahoo! chose not to remove it. *Id.* at 1098. The court again found that Section 230 immunity would apply yet found for the plaintiff based on other claims. *Id.* at 1109.

an ID and impersonate another. A difficult question arises as to whether these issues might pertain to Specific Pseudonyms. This issue might arise when an individual has a well-accepted "handle," which is registered by someone else in another virtual realm. In these cases, the damages of such actions can impact both victims and third parties relying upon the false pseudonymous profile, yet they may be somewhat farfetched.

The *third* element of this discussion provides yet another variation of concerns related to inaccurate identity intermediation—identity misrepresentation. In this case, there is no victim of impersonation or hacking—the damages are confined to third parties.[191] This concern comes about when a user creates an identity which does not exist. It should be noted that a similar concern arises when an individual purposefully misrepresents various personal traits in his or her profile. This latter concern is often noted in the context of dating websites, where users often include "white lies" regarding their weight, height, or age in their profile (in this case, the social norm might actually allow for such inaccuracies).[192] For this Article, we will merely focus on the first example (and the issue of "identity misrepresentation") rather than the latter. As our discussion focuses on the responsibility and possible liability of the intermediary, considering the broader implications of this final example within our analysis leads to substantial difficulties; would it be possible to require that identity intermediaries authenticate every personal factor set forth by a user? This issue also takes us beyond the core of our discussion (identity) and into examining the importance of verifying various personal traits.[193]

As mentioned, the concerns noted here only pertain to third parties who might have relied upon the identity misrepresentations and acted accordingly. Such false reliance might cause commercial loss and other damages that are far more severe. Yet beyond those interacting with the misrepresenting party, such actions undermine trust throughout the relevant virtual realm, and thereafter the loss of all the various gains identity intermediation can bring about.

---

[191] For a discussion of such instances in the offline realm, see *supra* note 160.

[192] In some cases, such misrepresentations on dating websites (especially with regard to age) lead to serious criminal charges, such as statutory rape. In this context, courts have explored the liability of dating websites for these unfortunate outcomes. See for instance Doe v. SexSearch.com, 551 F.3d 412, 415 (6th Cir. 2008) (court examined whether website made binding representations regarding age authentication and rejected this claim). The issue of age verification (and negligence to do so) was also addressed in *Doe v. MySpace, Inc.*, 528 F.3d 413, 422 (5th Cir. 2008) (court rejected claim that MySpace was negligent when engaging in age verification).

[193] We concede that the line between mere and identity misrepresentations is blurry at best. For instance, when an individual misrepresents that she lives at a specific location or owns a specific establishment, should such actions be considered as identity misrepresentation? On its face the answer is negative. However, what if the misrepresented factor is related to very few individuals and these actual trait holders are known? Arguably these instances probably feature identity misrepresentation as well (even though such intermediation is merely implicit). We thank James Grimmelmann for articulating this point.

The most famous and tragic example of this concern relates to the story of Lori Drew.[194] Drew was worried that a teenager, Megan Meier, was spreading gossip about her daughter. Drew created a fictitious identity—"Josh Evans"—who befriended Megan Meier only later to break up with her, and insult her.[195] Consequently, Megan Meier took her own life.[196] Here, the process of identity misrepresentation caused Megan to rely upon the actions of "Josh" and form a close attachment, which Drew abused. This entire dynamic resulted from a failure in the identity intermediation process.[197]

More recently, other, less severe cases have unfolded in the national press. Even a specific term—*catfishing*—has been coined to address "[t]he phenomenon of internet predators that fabricate online identities and entire social circles to trick people into emotional/romantic relationships (over a long period of time)."[198] For instance, Manti Te'o, a college football star, was duped into a courtship with a fake girlfriend, Lennay Kekua, who "died" just before a crucial game.[199]

As noted above, new laws have been set in place to deal with various concerns related to online impersonation—especially in social networks. Yet, as legal experts opined with regard to the Te'o affair,[200] legal action against the initiator of a false profile under these new laws is difficult. The anti-impersonation laws, by nature, call for impersonation of an actual person—an element missing in this example.[201] Another possible strategy explored in the *Drew* case is prosecuting those engaged in identity misrepresentation using anti-hacking laws. Here the argument will state that the individuals engaged in "unlawful access," by using the intermediary system while breaching its terms of use (for instance, using a false name rather than a real one). The court in

---

[194] Drew was indicted and eventually acquitted of computer fraud claims. United States v. Drew, 259 F.R.D. 449, 468 (C.D. Cal. 2009). The indictment was premised upon Drew's breach of MySpace's contractual terms in opening and operating the account. *Id.* at 457. The court found that the prohibitions on negative behavior in the MySpace ToS were too "vague" to be the basis of a criminal indictment. *Id.* at 465–66.

[195] *Id.* at 452.

[196] *Id.*

[197] Note again that, in some cases, it would be difficult to establish whether a tragic outcome resulted from an identity or other misrepresentation. For instance, in a case in which an individual encourages others to commit suicide in related chatrooms, while claiming he is a clergyman or doctor.

[198] Zimmerman v. Bd. of Trs. of Ball State Univ., No. 1:12-cv-01475-JMS-DML, 2013 WL 1619532, at *14 (S.D. Ind. Apr. 15, 2013) (citation omitted).

[199] Victor Luckerson, *Can You Go to Jail for Impersonating Someone Online?*, TIME, Jan. 22, 2013, http://business.time.com/2013/01/22/can-you-go-to-jail-for-impersonating-someone-online/.

[200] *Id.*

[201] Some commentators noted that changing these laws to bring cases against these actors might infringe upon their free speech and thus prove to be unconstitutional. *See, e.g.*, Bradley Shear, *Notre Dame, Manti Te'o, Catfishing, Online Impersonation, and the Law*, SHEAR ON SOC. MEDIA L. (Jan. 17, 2013), http://www.shearsocialmedia.com/2013/01/notre-dame-manti-teo-catfishing-online.html.

Drew rejected this claim.[202] However, with some alterations, this argument might be used again in the future. In addition, there is the option of bringing a variety of tort claims against users for these abuses.[203]

The role (and fault) of the intermediary in this context is similar to the one noted in the context of impersonation. In effect, had the identity intermediary assured that the identities assumed through the intermediation process were "real" and the identifying information was accurate, some of the problems noted in this section would have been avoided. Note however that the task intermediaries face here is different and sets forth serious challenges. In this context, the firm cannot rely upon victims of impersonation to come forth and report fake profiles (because there are no such persons). In addition, they will be unable to "quiz" individuals using information they collected elsewhere about them (as indeed there is no such information). In fact, courts are reluctant to order intermediaries to carry out these verification tasks. For instance, this issue was recently discussed in a class action brought against Match.com.[204] In this case, plaintiffs argued that many of the dating website's profiles were a fake.[205] The legal arguments were generally premised upon breaches of actual and implied contractual promises made by the dating website.[206] Given the fact that Match.com specifically notes that it does not carry out any background checks, the court easily rejected this claim.[207] It is fair to assume that in other cases, which will not be premised upon a contractual framework, intermediaries will again benefit from Section 230 immunity. Below we will examine how law should address this set of concerns.

Again, upon conclusion, we must examine whether these concerns of identity misrepresentation pertain to Stable Pseudonyms as well or only Real Names. At first blush, the issue here discussed can probably only relate to the intermediation of Real Names. Only in these contexts can one state that a legal expectation regarding the authenticity of the identified individual exists. When interacting in a pseudonymous environment, it is difficult to assert that there is an expectation that the individual is "real." Yet environments with stable pseudonyms can generate very interesting concerns and possible legal claims regarding the failure of intermediation. For instance, a possible concern might arise when it becomes apparent that a pseudonymous identity is not powered by

---

[202] *See* discussion *supra* note 194.

[203] Possible tort claims are: intentional infliction of emotional distress, misrepresentation, and perhaps negligence. These claims at times fail because of the inability to prove actual damages.

[204] Robinson v. Match.com, LLC, No. 3:10-cv-2651-L, 2012 WL 3263992, at *1 (N.D. Tex. Aug. 10, 2012).

[205] *Id.* at *5.

[206] *Id.* at *5–8.

[207] *See* discussion and analysis in Ramasastry, *supra* note 159; Nate Raymond, *Match.com Lawsuit 2012 Throw Out: Disgruntled Daters Find No Love in Court*, HUFFINGTON POST (Aug. 10, 2012), http://www.huffingtonpost.com/2012/08/10/matchcom-lawsuit-2012_n_1766115.html.

a human, but merely a bot[208] (a problem which might be resolved using some form of a Turing test upon registration). In other cases, individuals created virtual identities which were inflicted with terrible troubles (some of which they eventually "killed") while others followed the outcomes with worry and empathy, only later to learn that these identities were fake.[209] These examples demonstrate the difficulty of distinguishing between acts that are illegal and those that are merely morally and ethically unacceptable or perhaps only in bad taste, yet still must be allowed and even protected so as to promote free speech objectives. Therefore, establishing the liability of identity intermediaries in this context and with regard to Stable Pseudonyms is a very difficult task.

2. *Virtual Property Rights, Publicity, and Dignity: Intermediary Discretion, Interoperability, and Mobility*

The identity-related harms arising from the intermediation process can result from a very different set of problems. Not only can concerns arise from other problematic users, whose actions might be enabled by the intermediaries' neglect. In some cases, concerns are derived from the direct actions and policies of the intermediary itself. To understand this point, we focus on the contractual and technological relationship between the user and the identity intermediary.[210] Here, we must establish whether we might allow markets to unfold as they may, or, whether law must intervene by limiting the remedies the intermediary might exercise toward users and perhaps even add mandatory requirements (be they technological or contractual) which the intermediaries must fulfill.

The interests related to the concerns here discussed are premised upon a somewhat different theoretical context than those addressed above. Here, we mostly reflect upon instances in which users engage in the extensive and intensive use of their virtual identity, and by doing so develop a close attachment to it. The importance and significance of this connection could be articulated in economic terms; if users apply these virtual identities to commerce, loss of control over them could be translated into financial loss. Yet the usage patterns noted at times generate an even closer attachment between the user and the relevant identity—one that users believe should be translated into a certain degree of "control" over their profile—or even a property right.[211] Other users might see these rights as a form of "personality right," or perhaps

---

[208] *See* discussion in Bernal, *supra* note 147, at 16.

[209] *See, e.g.*, Esther Addley, *Syrian Lesbian Blogger Is Revealed Conclusively To Be a Married Man*, GUARDIAN, June 12, 2011, http://www.guardian.co.uk/world/2011/jun/13/syrian-lesbian-blogger-tom-macmaster; Tracy Spaight, *Who Killed Miss Norway*, *in* THE STATE OF PLAY 189 (Jack M. Balkin & Beth Simone Noveck eds., 2006).

[210] For a discussion as to the relation between online technological design and contract, see generally Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635 (2011), *available at* http://ssrn.com/abstract=1808108.

[211] *See* discussion in Rundle et al., *supra* note 81, at 9–10.

somewhat of a blend of property and personality interests.[212] The relationship between user and profile/identity is strengthened as users add information to the relevant identity (such as photos or text) and formulate valuable social ties. In some cases, such as those of virtual worlds, the profile might include virtual goods of actual value. In addition, allowing users to exercise control (and providing them with assurances they will be able to do so) will also promote the general personal and social benefits discussed in Part IV.A *supra*.

While individual users have an interest in controlling their identity and will therefore argue for maintaining such ability, intermediaries have interests of their own. The intermediaries' commercial interests might provide substantial incentives for maintaining a broad prerogative to limit or even sever the users' control, at will.[213] This conflict leads to points of contention where identity interests might come into play and legal intervention is needed. We will hereby address three such points pertaining to the right and ability to engage in *termination and deletion*, *interoperability*, and *mobility* of the online identity and profile.

Perhaps the most intuitive capacity linked to "controlling" the relevant eID is the ability to use it. This ability, or even "right," conflicts with the intermediaries' almost unfettered ability to *terminate* the identity at their discretion. Most contractual frameworks between identity intermediaries and their users include broad termination clauses. These allow intermediaries to disconnect the users when various alleged contractual breaches are found.[214] Law perhaps must intervene in this contractual relationship, rather than merely uphold it.[215]

A lesser concern arises when the intermediary might alter the identity-based profile, deleting parts of it at its discretion. Again firms can do so, on the basis of broad discretion provided in the terms of use. Furthermore, Section 230 of the CDA allows firms to remove information when acting in good faith (which is broadly construed).[216] Thus, users have very limited claims to set forth if

---

[212] On the relation and interaction between property and personhood in this context, see Norberto Nuno Gomes de Andrade, *Striking a Balance Between Property and Personality: The Case of the Avatars*, 1 J. VIRTUAL WORLDS RES., Feb. 2009, at 3, 11, 14, *available at* http://journals.tdl.org/jvwr/index.php/jvwr/article/view/362/423.

[213] *See* discussion in Grimmelmann, *supra* note 83, at 429 as to the intermediaries' incentives to generate user dependence and lock-in.

[214] *Statement of Rights and Responsibilities*, *supra* note 41, § 15 (granting Facebook the right to stop providing the user all or part of Facebook services if the user violates the letter or spirit of the Statement of Rights and Responsibilities, or otherwise creates risk or possible legal exposure for Facebook).

[215] For a different opinion, finding that contractual language should prevail, see Eric Goldman, *Online User Account Termination and 47 U.S.C. § 230(c)(2)*, 2 U.C. IRVINE L. REV. 659, 670 (2012) (arguing that broad termination rights to providers are sound policy, and that such rights could actually be derived from Section 230 itself, which should even be broadened to allow greater termination rights).

[216] 47 U.S.C. § 230 (c)(2)(a) (2006); *see* discussion in Goldman, *supra* note 215, at 660, 662.

content they themselves authored is removed from their profile. These outcomes however should be reconsidered in view of the interests here addressed.

Issues of proper intermediation have already arisen in a context where the interests of users are of perhaps greatest significance—virtual worlds.[217] In one incident broadly reported in the literature, Electronic Arts ("EA," the operators of "The Sims Online") terminated Peter Ludlow's account and removed him from the game. The parties disagreed as to the real reason behind this step. EA argued it took this aggressive step because Ludlow included a link to an external website (an act the terms of service (ToS) prohibited). Ludlow—an avid user of the Sims platform—claimed it was because of his critique of the way EA managed the system.[218] Whether the truth is with Ludlow or EA is beside the point. This example is merely a demonstration as to the ease with which the intermediary can exercise excessive force, while compromising important interests of the user. Another case which already reached the courts is that of Marc Bragg and the virtual world "Second Life." Here again Linden Labs, the website operator, terminated the user's cherished account.[219] The parties disagreed as to whether the user breached the website's terms of service, and whether the use of the "account termination" remedy was balanced and proper at this juncture.[220] While the case was ultimately settled, the court addressed and ruled on the issue of the mandatory arbitration provision included in the ToS.[221] In doing so, the court did *not* accept the arbitration terms set out in the ToS, while indicating this contract was one of adhesion.[222]

Disputes and concerns addressing the specific interests here discussed need not only arise in view of the aggressive actions of the intermediary. They might also arise from the intermediaries' effective "locking" of the user into one realm of intermediation. In other words, we refer to the lack of interface *interoperability* and user *mobility* the platforms might exhibit. *Interoperability*

---

[217] *See* Goldman, *supra* note 215, at 660.

[218] *See* discussion in Balkin, *supra* note 171, at 2075.

[219] Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593, 595 (E.D. Pa. 2007).

[220] *Id.*

[221] *Id.* at 603–12.

[222] *Id.* at 606–12. In this case, Bragg apparently acquired virtual land in an improper manner. *Id.* at 597. In the sections of the case ruled upon, the court set aside a binding arbitration agreement, finding it to be unconscionable. *Id.* at 611. As part of the analysis, the court noted that "[o]wning property in and having access to this virtual world is, moreover, apparently important to the plaintiff in this case." *Id.* at 595. In addition, when examining whether the terms of service are a contract of adhesion the court noted that there were no "reasonably available market alternatives [to defeat] a claim of adhesiveness." *Id.* at 606. A possible problem with this attempt to extrapolate from the *Bragg* decision to the broader notion of protecting identity interests from the actions of intermediaries is that this case involved actual financial harms, rather than strictly virtual ones. Bragg spent "real" money in "Second Life" to acquire virtual goods. Upon cancelling the account, these goods evaporated. However, we believe that the points made by the court here could be easily expanded to instances in which the damages cannot be reduced to dollars and cents, but can be articulated through notions of autonomy and dignitary harms.

here refers to the intermediary platform's ability to effectively interact with other identity platforms or intermediaries, while allowing users to benefit from the services and features made available on these other sites.[223] Interoperability allows for fully exercising the (personality, property, or other) rights here discussed. Yet, firms (especially the large ones) have limited incentives to provide or even enable interoperability. They rather weaken their smaller competitors and hope to gain their market share after they fail. *Mobility* (or portability) refers to a similar—yet more extreme—notion. Achieving portability would allow users to terminate their relationships with their identity intermediary with limited costs and harm. When doing so, the user would be able to transport his identity and profile from one platform to another. Again, large and successful firms clearly have limited incentives to provide such abilities. Thus, law might be required to intervene.

Without the ability to engage in interoperability or mobility, users are unable to exercise "control" over their identity rights. Rather, they must solely interact within the confines designated by the intermediary. They are also *de facto* restricted from moving to another platform, given the high costs of such a move; with no mobility, opting for another platform will require leaving their content and contacts behind and starting a new identity.

Calls for assuring and promoting interoperability and mobility have already been raised in the legal discourse when discussing the regulation of internet intermediaries. They are often mentioned in the context of competition law (although their wisdom has, at times, been questioned).[224] They have also been recently set forth as part of users' privacy (or data protection) rights and ability to control personal information pertaining to them.[225] In other instances (such as that of cell phone operators), data mobility has been promoted as a measure of consumer protection.[226] Yet promoting interoperability and mobility can also be justified by the personality-based theories and objectives here discussed. The ability to exercise interoperability and mobility could be understood as a

---

[223] Grimmelmann, *supra* note 83, at 429–30.

[224] *See* Peter Swire & Yianni Lagos, *Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique*, 72 MD. L. REV. 335, 337–40 (2013). For the DRM Context, see Tal Z. Zarsky, *Assessing Alternative Compensation Models for Online Content Consumption*, 84 DENV. U. L. REV. 645, 659 (2006).

[225] *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, at 53, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *EU 2012 Proposal*], *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf; *see also* discussion in Swire & Lagos, *supra* note 224, at 336–37. In fact, the draft Data Protection Regulation, published in January 2012 and aimed at revising and replacing the EU Directive, explicitly enshrines in Article 18 "a right to data portability." *See* discussion in Paul De Hert & Vagelis Papkonstantinou, *The Proposed Data Protection Regulation Replacing Directive 95/46/EC: A Sound System for the Protection of Individuals*, 28 COMPUTER L. & SECEURITY REV. 130, 137–38 (2012).

[226] BAR-GILL, *supra* note 71, at 243–44.

manifestation of a crucial segment of property's "bundle of rights"—the right of alienability[227] or the ability to control one's information and persona to the greatest degree possible.[228]

We conclude by examining whether the rights and concerns here discussed pertain to Real Names and/or Stable Pseudonyms. For some of the issues—such as content and contacts lost due to the intermediaries' actions—there seems to be little difference. In other contexts, the rights of Stable Pseudonyms require additional protection. Those using Real Names can easily "export" some of their reputational capital out of the identity system operated by the intermediary; those striving to contact them could do so in other ways. Yet for those using a stable and unique pseudonym, silencing or limiting their use of this identity by the intermediary (through limiting portability or even termination) amounts to the individual's total loss of control—there is no simple way this point of control could be routed around. For that reason, perhaps additional forms of legal protection are called for in the Stable Pseudonym context.

C. *Interim Summary: Identity Intermediaries, Concerns and the Law—Taking Stock and Looking Forward*

As our discussion thus far shows, the emergence of soft eID intermediaries is generating an abundance of novel benefits, as well as problems and concerns. These concerns arise in a setting where commercial entities are in a position of power. Therefore a discussion of legal intervention at this juncture is crucial.

Yet some would argue against aggressive and active legal intervention. They would note that the problems here discussed are mostly minor and easily manageable through existing laws. They might also be resulting from a passing trend, and regulation in this context usually proves futile. Technologies move ahead, rendering the law quickly irrelevant. Moreover, the law might stifle innovative practices. Therefore, law should strive to remain as "neutral" as possible, rather than end up picking winners. Finally, those objecting to legal intervention will state that market pressures have a good chance of regulating these matters on their own, as market players adapt their technologies and business plans to meet the users' preferences and tastes.

Rather than a fad, we believe the current shift toward soft eID intermediation and the novel problems it brings about are only the beginning of a greater movement coming in the next few years. In the future, we might see a shift of additional identification and verification roles to these realms—in both

---

[227] One should not confuse the right to shift from one platform to another with the right to sell one's personality right. Recognizing the latter calls for a deeper discussion and considering the potential problems of commodification. *See generally* Rothman, *supra* note 139.

[228] NSTIC REPORT, *supra* note 35, at 25.

commercial and governmental settings.[229] For instance, we might have state voting via Facebook (in some states you can already use the site to register).[230] The growing use of tablets and smart phones as mobile means of communication and transaction will call for additional identification schemes making use of these technologies, thus leading to additional sets of problems.[231]

Furthermore, the markets for these forms of intermediation might be consolidating. Therefore, market forces will most likely fail to lead to an optimal outcome. One of the moves toward consolidation is the introduction of Facebook's "Open Graph" (or "Facebook Connect").[232] This tool enables Facebook identity intermediation on a variety of platforms.[233] Thus, we will see several soft identity intermediaries gaining dominance, and as a result, we will lose the benefits of market forces which are attentive to consumer interests. In such a case, law and policy must step in.

Even if markets were to remain competitive, the issues here discussed call for legal scrutiny and even intervention in many cases, as the markets here discussed are probably deemed to fail for two main reasons. First, note the *non-salience* problem.[234] Even if the concerns addressed in Part IV.B above appear serious after the fact, there is a good chance that individuals will tend to underestimate the pertinent contractual provisions and technical measures which enabled them *ex ante* (that is, when creating the soft eID). In other words, users will agree to terms of use which will shield the intermediaries from the liability the concerns mentioned generate and to technological settings which generate vulnerabilities. Users will tend to do so, as they will focus their attention on other contractual and factual attributes. This will leave these important issues unattended, thus requiring governmental intervention.

Second is the *collective action* problem. The examples above note upsetting and drastic cases. However, in many other instances, the identity harms caused are not as serious. A one-time hack, an impersonator that stopped after a short time, or an interaction with a bot—these might all indeed cause aggravation and harm. Yet they will probably not generate sufficient user motivation to engage in a lawsuit against the identity intermediary (and possibly not even a complaint). Here one must also note that such legal actions carry considerable

---

[229] For a discussion on the merits and drawbacks of using social networking services for government eID in Europe, see Aaron K. Martin & Norberto Nuno Gomes de Andrade, *Friending the Taxman: On the Use of Social Networking Services for Government eID in Europe*, 37 TELECOMM. POL'Y (forthcoming 2013).

[230] Jacob Porter, *Facebook Voter Registration by Washington State Will Become Commonplace*, POLICYMIC (2012), http://www.policymic.com/articles/11484/facebook-voter-registration-by-washington-state-will-become-commonplace. Note that this process does not involve identity intermediation.

[231] *See* NSTIC REPORT, *supra* note 35, at 25.

[232] *See* Justin Lafferty, *What Can Facebook's Open Graph Do?*, ALLFACEBOOK (Sept. 18, 2012, 3:59 PM), http://allfacebook.com/what-can-facebooks-open-graph-do_b99921.

[233] *Id.*

[234] *See* discussion *supra* Part II.B.2.

costs, especially given the fact that the intermediaries are often located at a distant location or even country.[235] Therefore, the intermediaries will not internalize the full extent of the damages they inflict in view of high litigation costs (as well as high coordination costs among potential plaintiffs) and the spread of damages across the broader population. In this case, law and regulation must intervene.

Even after recognizing that law should play a larger role in the regulation of soft eID intermediaries, we must decide what the nature of that role would be. There are three forms of possible regulatory steps: *limited*, *responsive*, and *strategic*. A limited response is very similar to the current U.S. legal strategy: general deference to market forces, while focusing on the pursuance of third parties which generated the concerns noted (such as the account hijacker or impersonator). However, law can also adopt a *responsive* role, which is led by the courts. Here, courts might find that the intermediaries are liable for the concerns mentioned and the damages that followed. Thus, they will take action either by assigning liability, or striking down specific provisions in the intermediaries' terms of service. It is possible, however, that this approach is insufficient. Given the ever-changing nature of the problem at hand, the slow responses of courts, and their limited technical expertise, a more aggressive approach might be called for.

That brings us to law's *strategic* role. Lawmakers and regulators can move to resolve the concerns here addressed in a more aggressive manner. For instance, they might set clear guidelines as to the acceptable practices of relevant firms—practices that they believe will generate stability and trust. Although somewhat unfitting for a technological context, we are already seeing such action in the broader context of data security.[236] In addition, with regard to privacy law (an issue which shares many attributes with the one here addressed), regulators in both the United States[237] and the EU[238] are moving to implement "Privacy by Design"[239]—a strategic regulatory response which calls for structuring technology in a way which would enforce privacy principles and

---

[235] Note that the extent of this problem is affected by the willingness of courts to uphold jurisdiction clauses in the intermediaries' terms of use. While this is an important issue, we choose to set it aside for this analysis.

[236] *See Prepared Statement of the Federal Trade Commission on Data Security Before the Comm. on Energy and Commerce Subcomm. on Commerce, Manufacturing, and Trade U.S. H. of Reps.*, 112th Cong. 22–23 (2011) (statement of David C. Vladeck, Director, Bureau of Consumer Protection), *available at* http://www.ftc.gov/opa/2011/05/pdf/110504 datasecurityhouse.pdf. In addition, the State of Massachusetts has set standards as to proper technological steps to be taken to guard the security of personal data. *See Standards for the Protection of Personal Information of Residents of the Commonwealth*, MASS.GOV, http://www.mass.gov/ago/doing-business-in-massachusetts/privacy-and-data-security/standards-for-the-protection-of-personal.html (last visited July 21, 2013).

[237] FTC REPORT, *supra* note 87, at 22–32.

[238] *EU 2012 Proposal*, *supra* note 225, art. 30(3) at 60.

[239] *See* discussion in Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1421–31, 1436–39 (2011).

limit future harms. Thus, law is indeed striving to take a more active role which will limit concerns *ex ante*, rather than punishing and compensating *ex post*.

What path must law follow in the context of soft eIDs? To try to gain additional insights to this issue, we look to the EU which faced a similar problem more than a decade ago. When striving to deal with the emergence of digital eIDs, the EU adopted the eSig Directive.[240] This directive made use of both the regulatory and strategic responses, with interesting variations.[241] It would be helpful to examine what we can learn from the EU experience, and examine whether the structure used is fitting to the novel setting of soft eID intermediaries (which are clearly outside the Directive's scope). It is also helpful to note that the existing eSig Directive is under review in the EU, with the prospect that its scope will be considerably expanded. Thus it would be interesting to contemplate and consider whether this legal structure can be used (after proper amendments) for the regulation of soft eID intermediaries. We therefore turn to discuss the EU eSig Directive as well as its critiques and failures. We also address two additional novel governmental steps, both in the United States and the EU, which closely coincide with some of the eSig Directive general themes.

V. THE LAW AND/OF ID INTERMEDIARIES: AN EU PERSPECTIVE THROUGH THE ESIG PRISM

A. *The E-Signature Directive in a Nutshell*

In 1999, the European Parliament and Council enacted Directive 1999/93/EC.[242] This Directive established a legal framework for electronic signatures and certification services.[243] The Directive was broadly adopted, with variations, by the Member States.[244] The Directive operates on several dimensions. First, it clarifies the legal standing and validity of these technologies[245]—both in the context of evidentiary rules and formal requirements for contract formation (or, in other words, indicates when a digital signature could serve the same purposes as a handwritten one). As noted above, the United States has introduced similar laws.[246]

Next, the Directive applies a three-part taxonomy for mapping out the realm of signatures, identification, and authentication. The Directive does so by referring to "Electronic Signatures," "Advanced Electronic Signatures," and "Qualified Advanced Electronic Signatures."[247] The first term refers to the most

---

[240] Directive 1999/93/EC, *supra* note 42, at 12.
[241] *Id.* arts. 1–15, at 14–17.
[242] *See id.* at 12.
[243] *See id.* art. 5, at 15.
[244] JOS DUMORTIER ET AL., *supra* note 60, § 1.2.1, at 4–8.
[245] Directive 1999/93/EC, *supra* note 42, art. 5, at 15.
[246] *See* Froomkin, *supra* note 65, at 9–12.
[247] *See* Directive 1999/93/EC, *supra* note 42, ¶¶ 19–20, at 13.

basic technological measure (even if completely unsecure) of authentication.[248] This might even include the process of signing an email message.[249] The next two options, however, rely on more elaborate schemes for identification and authentication.

The Directive introduces the concept of "Qualified Advanced Electronic Signatures" in Article 5.1.[250] To receive the "Qualification" standing, the Directive implements an aggressive, command-and-control form of regulation.[251] For that, government sets in place mandatory technological requirements.[252] In addition, the Directive introduces the concept of "Advanced Electronic Signatures."[253] For entering this category, the Directive calls for a process of voluntary accreditation (as explained in Article 3.2).[254] Here, the regulator sets up a regulatory approval scheme which firms, at their discretion, may enter so as to receive a stamp of quality.[255] This accreditation process could be carried out by either a public or private entity, so long as it is introduced by a Member State.[256] Yet those operating an "Advanced Electronic Signature" scheme are permitted to proceed without joining these voluntary schemes.[257] Therefore, the Directive introduces two innovative and strategic steps: a mandatory and voluntary pre-approval process for the use of ID intermediaries.[258]

The Directive introduces another strategic step, by striving to promote "harmonization."[259] In EU documents (as in this case), this term usually refers to assuring that laws governing a specific issue are similar within the Union.[260] Yet given the technological context, "harmonization" carries an additional meaning. The drafters feared the situation in which individuals move from one Member State to another while losing the ability to use their original authentication service.[261] Thus, "harmonization" refers to the technological concept of interoperability.

Finally, the Directive addresses the "responsive" role of law in Article 6, by noting the liability of service providers in the identity intermediation markets.[262] It states the "qualified" intermediary's liability for not conveying

---

[248] *Id.* art. 2(1), at 14.
[249] *Id.*
[250] *Id.* art. 5(1), at 15.
[251] *Id.* art. 5, at 15.
[252] *Id.*
[253] Directive 1999/93/EC, *supra* note 42, art. 2(2), at 14.
[254] *Id.* art. 3(2), at 15.
[255] *Id.*
[256] *Id.* art. 2(13), at 14.
[257] *Id.* ¶ 12, at 13.
[258] *Id.* art. 3, at 15.
[259] Directive 1999/93/EC, *supra* note 42, art. 12, at 17.
[260] *Commission Report*, *supra* note 59, § 3.3.2, at 7.
[261] Directive 1999/93/EC, *supra* note 42, ¶ 5, at 12.
[262] *Id.* art. 6, at 15–16.

the revocation of a signature and other elements.[263] It does so, however, while recognizing the intermediary's ability to limit (to some extent) their liability contractually.[264] It also recognizes the ability to strike down unfair contractual terms.[265]

The Directive applies several interesting "strategic" responses which might be further considered for the regulation of soft eIDs. Yet, expanding the ideas set forth in the EU eSig Directive might not constitute the best strategy. While the scope of online actions and transactions has grown exponentially, laws regulating electronic signatures have not substantially contributed to such growth. The Directive and subsequent laws have not generated much interest and traction.[266] This finding has not escaped the EU authorities, who moved to issue several reports to examine this apparent failure. These noted that Member States have enacted relevant laws to transpose the Directive's general principles and rules. Yet beyond some uses in private banking, the central realm of relevance for both the directive and the state laws is that of e-Government. In this context several follow-up regulatory structures were introduced, such as those pertaining to public procurement.[267] However, the overall failure in the commercial sector is quite clear.

There are varied reasons for the Directive's relative failure to substantially affect online commerce and trust. The use of digital signatures requires time, understanding of technology, and a grasp of complex concepts of cryptology. These all might be beyond the reach of the average busy online user, who therefore simply ignores these secure intermediation tools.[268] In addition, the Directive was set in place with a specific vision of the online realm in mind. Yet the e-commerce market (and the Internet in general) developed in unpredictable ways. These developments generated limited incentives for business models promoting the use of digital signatures and other advanced identification models the drafters of the Directive envisioned.[269] As in other contexts, it appears that the public is reluctant to spend money to promote its privacy. It is also possible that the Directive was not aggressive enough in solidifying the legal standing of

---

[263] *Id.*

[264] *Id.* arts. 6(3)–6(4), at 16.

[265] *Id.* art. 6(5), at 16.

[266] *Commission Report*, *supra* note 59, § 3.3.2, at 7–8; JOS DUMORTIER ET AL., *supra* note 60, § 1.2.1, at 4–8.

[267] Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 Coordinating the Procurement Procedures of Entities Operating in the Water, Energy, Transport and Postal Services Sectors, 2004 O.J. (L 134) 1; *see also* Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the Coordination of Procedures for the Award of Public Works Contracts, Public Supply Contracts and Public Service Contracts, 2004 O.J. (L 134) 114.

[268] For a similar argument, see JOS DUMORTIER ET AL., *supra* note 60, § 4.3, at 134.

[269] *Commission Report*, *supra* note 59, § 3.3.2, at 7–8.

online identity authorization.[270] We will bear these reasons in mind when considering the next steps to be taken for soft eIDs.

B. *ESig Regulation: The Next Step on Both Sides of the Atlantic—Expanding the eSig Directive and the National Strategy for Trusted Identities in Cyberspace (NSTIC)*

As a substantial amount of time has passed since the introduction of the eSig Directive, it is helpful to point to recent developments regarding this matter. In the EU, the existing eSig Directive is under review. As part of this process, EU policymakers are considering ways to incorporate this Directive into a broader strategy to promote "Identification, Authentication and Signature" (IAS). In doing so, the Commission has opted for a new Regulation—that of "Electronic Trust Services."[271] Note that this legal instrument provides greater certainty as it is immediately applicable to all EU Member States. In this respect, one of the central objectives of the proposed Regulation is to promote harmonization and mobility among Member States for citizens making use of various identification and authentication measures.[272]

To achieve these objectives, the new regulatory framework calls for "mutual recognition" of eIDs;[273] states are free to select which eID platforms could be used for their public services, and notify the EU Commission of such selection.[274] Yet they must then recognize and accept the eID systems other states have selected as well, so as to enable user mobility and interoperability.[275] While the proposed Regulation will be considerably broader

---

[270] There might be other, speculative, reasons as well. For instance, the governments' insistence on maintaining a backdoor key to many of these systems discouraged users from engaging with these technologies. They perhaps understood that their actions and transactions were not really secure. *See* Froomkin, *supra* note 65, at 37.

[271] *See Proposal for a Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market*, ¶ 17, at 14, COM (2012) 238 final (June 4, 2012) [hereinafter *Proposal for a Regulation*].

[272] The new framework for electronic identification and electronic trust services will: ensure mutual recognition and acceptance of electronic identification across borders; give legal effect and mutual recognition to trust services including enhancing current rules on e-signatures and providing a legal framework for electronic seals, time stamping, electronic document acceptability, electronic delivery, and website authentication. For more information, see Press Release, Eur. Comm'n, Draft Regulation on Electronic Identification and Trusted Services for Electronic Transactions in the Internal Market (Sept. 20, 2012), *available at* http://ec.europa.eu/digital-agenda/en/news/draft-regulation-electronic-identification-and-trusted-services-electronic-transactions-0.

[273] *Proposal for a Regulation*, *supra* note 271, § 1, at 2, § 3.3.2, at 5.

[274] *Id.* § 3.3.2, at 5.

[275] *Id.*

than the existing eSig directive, it would most likely still *not* pertain and govern the commercial entities defined as soft eID intermediaries above.[276]

The issue of eID intermediation has also caught the attention of the highest level of government in the United States as in this context, the White House issued its *National Strategy for Trusted Identities in Cyberspace* (NSTIC) report.[277] The project's guiding principles are privacy, security, interoperability, and ease-of-use.[278] It focuses on the emergence and development of an "identity ecosystem"—"an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities."[279] The report is quite general in its discussion and calls for a multiyear project of examining these matters.[280] It launches an extensive initiative (NSTIC) to be headed by the Department of Commerce to achieve the objectives noted.[281] Given its scope, it could certainly be considered a blueprint for a strategic response for dealing with eIDs. The scheme developed in the U.S. government's document makes no specific reference to websites which provide soft eIDs through social networks and social media. It does, however, greatly rely on mobile technology as perhaps a tool which will facilitate authentication.[282]

The scheme promoted by NSTIC includes many similarities to the one offered in the eSig Directive (although, sadly, it makes no reference to it). It is premised upon public–private collaboration[283] that will generate the above mentioned "ecosystem." This scheme calls for the creation of an "accreditation authority" to validate the systems and methods used by the various participants in the "ID ecosystem."[284] If the relevant system is found to be in compliance with a minimal standard, it will receive a "trustmark" which cannot be

---

[276] As noted by the Head of the Task Force "Legislation Team (eIDAS)" at the European Commission, the eIDAS regulation does not cover "soft ID" (e.g. Facebook), only official eID. *See* Andrea Servida, *Proposal for a Regulation on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market*, IAS PROJECT 12–13, (June 4, 2012), http://www.iasproject.eu/attachments/File/Workshop_2/workshop_IAS_-_Servida.pdf.

[277] NSTIC REPORT, *supra* note 35, at 1–4; *see also* THE WHITE HOUSE, INTERNATIONAL STRATEGY FOR CYBERSPACE: PROSPERITY, SECURITY, AND OPENNESS IN A NETWORKED WORLD 25 (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; A. Michael Froomkin, *"PETs Must Be on a Leash": How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology*, 74 OHIO ST. L.J. 965 (2013).

[278] NSTIC REPORT, *supra* note 35, at 2–3.

[279] *Id.* at 2.

[280] *Id.* at 41.

[281] The NSTIC project has also awarded funding to five pilot projects and issued calls for additional pilots. *See Happy NSTIC-iversary!*, NSTIC NOTES (Apr. 17, 2013), http://nstic.blogs.govdelivery.com/2013/04/17/happy-nstic-iversary/.

[282] NSTIC REPORT, *supra* note 35, at 25.

[283] *Id.* at 9.

[284] *Id.* at 25.

forged.[285] This mark will act as a signal to users that the services should be trusted.[286] Not only will this system be secure and authenticated, and thus minimize the concerns noted above, but it will also be interoperable (and thus meet the second set of interests noted above).[287] The report notes several times that the scheme would be voluntary, and led by government.[288] However, the government will move to promote and encourage the use of measures operating within the ecosystem, while relying upon its various capacities as purchaser and user of technologies (such as in e-gov).[289] In doing so, government will give preference to technologies that are in compliance with standards set by the NSTIC scheme.

As part of this project, the government will make additional strategic policy moves. Among others, it will promote standards of technical conduct for the operation of the identity intermediation process.[290] Setting such a standard is an interesting strategic move which might later be applied in other realms of the law—such as by regulators that will mandate this standard, or by courts which will see it as a threshold for acceptable conduct in this context. The report also notes governmental influence in setting levels of liability for firms operating within the ecosystem.[291] Clearly setting a low level of liability will prove to be a powerful incentive to join this scheme (as it will provide firms operating within it with a liability safe harbor).

Although this initiative is only taking its first steps, it is already generating a vibrant discussion and some sharp criticism in the academic and policy world. This discussion is of interest, as the arguments presented might also be applied when considering the proper policy responses for soft eIDs (and is yet another benefit of incorporating these discussions into the themes addressed in this Article). Michael Froomkin is skeptical of NSTIC and cautions against what he views as steps which are part of a "second wave" of internet regulation.[292] He sees these initiatives as measures striving to undermine the extent of anonymity available online. While these regulatory moves might seem innocuous at first blush, they must be viewed as part of a broader historical trend. Froomkin notes earlier moves in the mid-nineties, when governments tried to crack down on internet anonymity by requesting backdoor access to encryption schemes (a wave that ultimately mostly failed).[293] Froomkin finds this second wave very upsetting and fears it might succeed this time (as governments have learned from their previous mistakes).[294] This time around, the government is not

---

[285] *Id.* at 22.
[286] *Id.*
[287] *Id.* at 13.
[288] NSTIC REPORT, *supra* note 35, at 3, 11.
[289] *Id.* at 32.
[290] *Id.* at 30–31.
[291] *Id.* at 31.
[292] Froomkin, *supra* note 65, at 14–30.
[293] *Id.* at 7–12.
[294] *Id.* at 14–30.

forcing private entities to provide access, but is setting up seductive voluntary schemes which large commercial entities will feel obligated to join (possibly because those participating in the scheme will receive tax breaks and benefits).[295] The troubling outcome of this dynamic, according to Froomkin, would be a system which allows government to uncloak the anonymity and privacy of users—thus compromising important social values.[296] This infrastructure could then be used to enable mass surveillance—a simple task for governments given the fact that they assisted in planning this project's infrastructure.

The Electronic Freedom Foundation (EFF) is also skeptical of this initiative and begs caution.[297] The EFF questions whether the government's strategy, which calls for all identities to be controlled at one point, does not generate greater (rather than fewer) security risks and vulnerabilities. Another concern is that with a government controlled ID system,[298] federal agents could be easily issued false credentials so as to engage in surveillance. In other words, the ID system will "vouch" that undercover agents are individuals the target might know or trust, while in fact they are not.

VI. BRINGING IT ALL TOGETHER: REGULATING SOFT EID INTERMEDIARIES

After examining the definition, evolution, forms, benefits, and detriments of soft eID and its intermediation, as well as noting EU and U.S. regulatory frameworks which address similar issues, we now move to set forth a series of recommendations for legal responses. Law can indeed move in several directions. The somewhat passive/market-driven approach currently implemented has contributed to great innovation and growth in the relevant technology sectors. Yet as the multiple events noted above show, this came at a price. Individuals suffered various harms as intermediaries were free to escape liability and exercise broad discretion. It appears that economic forces are leading platforms to take greater risks, namely risks to their users' identity interests. In view of these developments, should other, strategic legal steps be considered? The eSig Directive notes three such options: (1) mandatory approval/supervision for identity intermediaries; (2) voluntary approval/supervision for identity intermediaries; (3) tort liability.[299] Some of these responses were also echoed in the other contemplated policy regimes noted above. In the next few pages we will examine the wisdom of adopting these ideas in the context of soft identity intermediaries.

---

[295] *Id.* at 11–12.

[296] *Id.* at 40–41.

[297] Lee Tien & Seth Schoen, *Real ID Online? New Federal Online Identity Plan Raises Privacy and Free Speech Concerns*, ELECTRONIC FRONTIER FOUND. (July 20, 2010), https://www.eff.org/deeplinks/2010/07/real-id-online-new-federal-online-identity-plan.

[298] *Id.*

[299] Directive 1999/93/EC, *supra* note 42, ¶¶ 13, 22, at 13.

A. *Mandatory Approval/Supervision for Identity Intermediaries*

Should identity intermediaries whose overall operation goes beyond a specific threshold (set while accounting for the amount of users, tasks, data controlled, or other factors) be subjected to mandatory regulatory requirements? Should they be treated similarly to Qualified Advanced Electronic Signature Providers in the EU, or other entities which provide essential services and are often subjected to this form of regulation? While this notion has some appeal, it should be ultimately rejected, as it is a poor fit for this rapidly changing technological environment.

In this context, an aggressive mandatory strategy might be justified on the basis of three intuitive arguments, all noting that the mere reliance on tort liability or voluntary compliance is insufficient. *First* (and as noted briefly above), is the "collective action problem" argument. Users facing harms and damages, for various reasons (mostly the limited prospect of compensation, limited damages, and high litigation costs)[300] will not move to sue the intermediaries. Thus, tort liability will provide insufficient incentives for intermediaries to take proper steps to protect the users' interests and internalize the harms they cause.[301] *Second*, the damages caused at this juncture due to the intermediaries' actions and omissions are of great severity. They pertain to important notions such as the sense of identity and self. In such cases, society would be ill advised to merely rely on the forces of tort law to regulate outcome. These forces might play out too slowly and ineffectively while the social damage will persist. A similar argument motivates the introduction of worker and car safety regulations which go beyond tort liability. *Third*, the situation at hand might be one which generates great negative externalities. In other words, soft eID intermediaries cause damages which go beyond their users or other direct victims. For instance, reports on the various incidents discussed above might deter individuals from participating in the online discourse—and thus limit the important social benefits of the discourse and the information flows it enables. Therefore, society cannot rely on those seeking tort damages as a mechanism which will achieve an optimal social outcome. While these three arguments have some merit, they do not carry sufficient weight to overcome the substantial problems this regulatory strategy brings about.

---

[300] *See* discussion *supra* Part IV.C.

[301] It should be noted that some of these "collective action" related concerns might be mitigated given the specific context discussed—virtual identities which pertain to individuals which are discussed in the online realm. The online realm enables cheap and efficient collaboration and organization, and thus might allow for overcoming the high coordination costs often noted in this context. For more on the strengths and possible limits of online information flows, see Becher & Zarsky, *supra* note 71, at 320–33. In addition, one might note that a common response to this collective action problem is allowing for "class actions." As the damages here noted are very particular, one can question whether such a strategy (which carries with it vast costs and detriments) will prove helpful.

The prospects of the mandatory supervision scheme's success are not high, to say the least. A slow-paced regulatory approval or even supervision scheme will have a very difficult time keeping pace with new innovations which will be constantly challenging the regulator's definitions and authority. What they might indeed, inadvertently, end up achieving is a tax on innovation, as firms strive to work around governmental regulation, or are blocked from adopting new models.[302] Yet the regulator's incompetence might turn out to be the least of our troubles. The worst will follow when the regulator is corrupt, or at least subjected to influence of interest groups. Here, existing powerful commercial entities will strive to structure regulatory requirements to meet their current capabilities, rather than the actual social needs.[303] Thus, not only will the mandatory regulatory approach fail, but it will lead to unfair and inefficient outcomes. Given this risk, such forms of mandatory schemes should probably be avoided.

Finally, there is the delicate matter of enforcement. While most identity intermediaries are U.S. companies today, there is no guarantee this will always be the case. Even today's large U.S. Internet corporations might choose to move their operations offshore so as to escape mandatory regulation. Attending to the enforcement of technological standards with regard to multi-national Internet companies is a complex, costly, and often futile matter. Therefore, perhaps other options should be explored.

Before concluding this discussion, three short caveats are worth noting. *First*, this argument can only pertain to "soft eIDs" as defined above. If identification features are central to the firm's business plan and showcase prominently on their platform, business model, and marketing strategy, the regulatory response might be different (and indeed as explained above, in the EU, it already is or shortly will be).

Second, the arguments set forth here do not apply with equal force to all forms of identity intermediation. It is fair to assume that, in some contexts, the arguments for taking a more aggressive regulatory stance are stronger for Real Names identities. As explained, the damages to both the relevant individual, whose name or identity is abused, as well as to third parties who relied upon it, tend to be greater.

Third, while mandatory standards set and enforced by government are a problematic idea, there might be other ways for regulators to assure that identity

---

[302] *See* JONATHAN E. NUECHTERLEIN & PHILIP J. WEISER, DIGITAL CROSSROADS: AMERICAN TELECOMMUNICATIONS POLICY IN THE INTERNET AGE 394 (2005) (explaining that regulatory minimalists believe government intervention in the standard-setting process is dangerous and that standards selected by regulators may be inferior to those emerging in the marketplace); *see also* discussion in Michael I. Krauss, *Regulations vs. Markets in the Development of Standards*, 3 S. CAL. INTERDISC. L.J. 781, 798–99 (1994).

[303] For a discussion of this problem in the context of VOIP regulation, see Susan P. Crawford, *The Ambulance, the Squad Car, and the Internet*, 21 BERKELEY TECH. L.J. 873, 877–88 (2006); see also, in a broader telecom context, NUECHTERLEIN & WEISER, *supra* note 302, at 398–99. For a general discussion of this problem, see Krauss, *supra* note 302.

intermediaries internalize the damages they inflict. For instance, the government might consider the setting of *fines* to achieve this objective. These might be of greatest relevance and importance with regard to Real Name identity intermediaries, given the enhanced concerns they generate. We will return to this "softer" form of regulation, and its difficulties, below.[304]

B. *Voluntary Approval/Supervision for Identity Intermediaries*

As noted in the previous section, an interesting notion set forth both by NSTIC and the eSig Directive in Europe is a voluntary supervision and approval scheme by the government. While these noted initiatives do not pertain to soft eIDs, we must ask whether adopting such a strategic expansion to the intermediaries here discussed is a wise choice. However, even though this option sounds interesting, it can only have limited utility in this specific context.

The voluntary scheme works as a signaling mechanism. In other words, firms complying with the governmental standard signal high quality and reliability. The existence of the voluntary mechanism will allow firms to easily distinguish themselves. It will also assist consumers in identifying quality and risk, and in that way limit doubts and confusion. Therefore, users who seek to protect the interests noted above (especially while using Real Names) might only make use of or rely upon verified intermediaries. Others will be free to use or rely upon communications with identities which did not receive (or even seek) governmental approval, at their own risk.

On its face, the voluntary approval scheme could provide the benefits of the previous mandatory option, without the problematic shortcomings. The process does not necessarily chill innovation (or will do so to a much lesser extent), as firms that find the process impeding on their technological and business plans can simply choose to ignore it. These actions will also enhance overall trust in such intermediation systems. Finally, they are clearly easier to enforce, as the party voluntarily joining will hopefully cooperate, rather than raise jurisdictional defenses.

Yet, one can easily argue that the benefits of such a voluntary scheme are quite limited. At first, one can question whether a signal of compliance and competence from *government* in the innovative and ever-changing realm of identity intermediation is a factor users will find helpful and satisfying. Given the known problems of governmental ignorance and incompetence, users might be unimpressed when an intermediary has received a governmental stamp of approval.

They might even be worried. Recall our previous discussion regarding NSTIC and the thoughtful critiques set forth by both Michael Froomkin and the

---

[304] Another mandatory strategy that might be applied is a breach notification requirement for some of the breaches which cause the concerns noted. To some extent, this notion has been adopted by the recent EU Proposal, Articles 15(2) and 15(3). *Proposal for a Regulation*, *supra* note 271, arts. 15(2)–(3), at 27.

EFF.[305] Users might fear that governmental certification is not only an approval of security, but approval of the intermediaries' compliance with the government's various requests and needs—needs which might undermine the users' privacy and autonomy.[306] For that reason, the governmental stamp of authority might even be considered a "scarlet letter" for some cautious users.

Beyond these two arguments, users will probably ignore the governmental signal of approval (or lack thereof) for yet another reason. The seductive pull of many of the entities which incidentally generate "soft eIDs" might lead users to disregard the problematic aspects of identification. Much has been written about the magnetic draw of social networking sites (SNS).[307] In some social circles, social pressures almost force individuals to participate. These forces have arguably led individuals to use platforms which provided a very limited form of privacy protection. Such social pressures will most likely have a similar effect upon the process of selecting soft eID intermediaries as well. To note a similar example, commercial schemes to provide approval stamps of privacy protection (through the use of privacy seals) have generally failed to provide a suitable solution to the problems of online information privacy.[308] It is fair to predict that a similar dynamic will unfold with regard to approval (albeit, by the government) for identity intermediaries.

Nonetheless, let us not close the book on this voluntary approval scheme so quickly. While it would most likely fail as an effective signaling tool for users, voluntary schemes might fulfill other strategic roles. For instance, the standards set by government might either serve as a "safe harbor" or initiate another form of signaling to courts when establishing the intermediary's liability and duty of care for the harms discussed above. In other words, a governmental entity can set standards which courts will later use when ruling on liability. In many instances, regulators rather than courts will have the proper level of expertise to

---

[305] *See* discussion *supra* Part V.B.

[306] Recent reports regarding the NSA's activities (as allegedly leaked by Edward Snowden) indicate that this agency has strived to deliberately weaken both national and international encryption standards. Nicole Perlroth, Jeff Larson & Scott Shane, *N.S.A Able To Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 5, 2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&hp.

[307] *See, e.g.*, Grimmelmann, *supra* note 92, at 1161 (with regard to joining the network due to its size); *see also id.* at 1155 (with regard to adding "friends" who are not really friends).

[308] *See, e.g.*, Anthony D. Miyazaki & Sandeep Krishnamurthy, *Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions*, 36 J. CONSUMER AFF. 28, 34–37 (2002), *available at* http://onlinelibrary.wiley.com/doi/10.1111/j.1745-6606.2002.tb00419.x/abstract; *see also* Benjamin Edelman, Adverse Selection in Online "Trust Certification" 5–8 (Oct. 15, 2006) (unpublished manuscript), *available at* http://www.benedelman.org/publications/advsel-trust-draft.pdf (noting the ineffective role of certifiers and how they are subjected to capture).

address this issue and provide overall guidance to the industry.[309] Yet to fully understand this point, we must move to examine liability as a measure to regulate soft eIDs—a task we attend to now.[310]

C. *Identity Intermediaries and Tort Liability*

As noted throughout this Article, the current U.S. legal setting has allowed identity intermediaries to escape tort liability for various reasons. However, the eSig Directive, as well as both NSTIC and proposed new European eIDAS Regulation, address and to some extent set forth liability schemes for identity intermediaries. Therefore, reexamining the role of tort liability for the actions and omissions of the identity intermediaries is called for.

Overall, regulation through liability (or what we referred to above as a "responsive" legal strategy) does not entail many of the concerns inflicting the two regulatory options noted above. It does not allow government to closely regulate technology as it places courts as a central mitigating player. In theory at least, courts can examine whether these regulatory steps are merely measures to entrench incumbents or advance various governmental objectives. This scheme generates issues of enforceability—yet it is easier to enforce a monetary judgment as opposed to compliance with a technical standard, even regarding an offshore entity. This strategy, does, however, exacerbate problems of limited expertise on the legal end. Courts are incapable of understanding new technologies, much less steering them in the right direction. Thus, some form of regulatory influence would be wise.

A full analysis as to implementing a proper tort regime in this context requires addressing a variety of factors. Above all, we must attend to examining whether such claims will be blocked by the current legal doctrine derived from Section 230 of the CDA.[311] If so, should courts reinterpret the statute based on legislative intent? And even if the answer to this last question is negative, should the statute be amended? If so, in what way? Other questions we must consider are whether liability should be assigned to these intermediaries directly, or merely as contributing to the actions of a direct tortfeasor. Finally, we must establish the most appropriate tort to be applied at this juncture, while distinguishing among the different forms of victims noted above.[312] Some of

---

[309] This statement does not contradict those made above regarding the inability of regulators to address this ever-changing context. While regulators face challenges, they are in a better position to do so than courts.

[310] This solution might allow courts to take into account the various noted problems with certification mentioned above. It might also allow courts to set different standards for different forms of intermediation, such as Real Names or Stable Pseudonyms.

[311] An analysis of the role of Section 230 in this context might also call for examining the difficult relation between marketing representations made by a firm regarding identity intermediation, and the "immunity" section 230 provides. *See* discussion *supra* note 188.

[312] One student note has offered the tort of "negligent enablement of imposter fraud." Sterritt, *supra* note 11, at 1714–29.

these questions were recently reflected upon in thoughtful student notes.[313] Given the limited confines of this Article, it would be impossible to do justice to all these very difficult doctrinal questions. Any such discussion must also confront an even broader question—whether the overall balance set out in Section 230 is appropriate, or perhaps must be reconfigured altogether.

In the context of our limited discussion of tort liability for identity intermediaries, what we try to achieve is far less ambitious. Approaching the issue at a higher level of abstraction, our contribution would be first in examining if liability should normatively be assigned to these powerful players. Second, we strive to incorporate into this discussion the various distinctions set out above. In other words, we find it somewhat unhelpful to discuss the role and extent of liability in merely general terms. Rather, we believe that standards of care and responsibility must be matched to different forms of intermediation (Real Names vs. Stable Pseudonyms). We must also specifically address the three forms of concerns noted above (ID hijacking, impersonation, and identity misrepresentation) in our basic discussion of liability. The analysis thus creates a two-by-three matrix, which strives to address every one of the six rubrics separately.[314] In doing so, the analysis will generally assign a level of relative standard of care, which could be compared to the other instances addressed in the analysis.

It should be noted that the analysis also lacks a clear theoretical mapping of the rationale for assigning tort liability in this context. Given the Article's constraints, it generally points to intermediaries as entities capable (at times) of limiting the risks of damages, and therefore the proper bearers of liability.[315] Clearly a far more elaborate normative analysis is called for. Yet the insights here discussed would prove helpful in mapping out an overall response to the problems of identity intermediation.

A final introductory note goes to the role of the contractual language which might govern some of the relationships between potential plaintiffs and the relevant intermediary. As noted above,[316] some of those injured by the intermediaries' actions and omissions are in privity of contract with the identity intermediary—governed by the terms of use signed when generating the identity, and possibly reaffirmed every time the user enters the relevant

---

[313] *See id.*; Wesley Burrell, Note, *I Am He as You Are He as You Are Me: Being Able To Be Yourself, Protecting the Integrity of Identity Online*, 44 LOY. L.A. L. REV. 705, 738–47 (2011).

[314] See summary *infra* Table 1.

[315] For general sources regarding this matter, see GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 139 (1970) (economic analysis); George P. Fletcher, *Fairness and Utility in Tort Theory*, 85 HARV. L. REV. 537, 537–64 (1972) (fairness-based analysis); Doug Lichtman & Eric Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 222–48 (2006) (economic analysis of online intermediaries).

[316] *See, e.g.*, Robinson v. Match.com, LLC, No. 3:10-cv-2651-L, 2012 WL 3263992, at *5–8 (N.D. Tex. Aug. 10, 2012).

platform. As part of this contractual framework, users often waive their rights to bring actions regarding many of the claims we will now discuss. Therefore, liability will also be governed by the contractual framework pertaining to the parties. The problem, however, is that this contractual framework is rarely negotiated fairly. The contracts themselves are those of adhesion, presented to users on a "take it or leave it" basis. Furthermore, given the concentrated nature of some of the markets for SNS and related products, users cannot properly exercise their "leave it" option. In addition, it might even seem that whether the relationship in the relevant case is governed by contract is most of all a product of chance.

Therefore, at some points, the analysis below will disregard the specific nature of the contracts set among the parties and assume that even if liability will be limited contractually, courts should set these provisions aside. By ignoring the nature of the contracts, we are taking an informed legal position; we recognize the need for limiting the enforcement of these relevant provisions in the identity intermediaries' terms of use. However, at times, courts should refrain from intervening in the agreed-upon legal framework. In these instances, markets will sort out liability, in accordance with the contractual framework governing the parties. Here, market forces and the potential of negative political backlash from imbalanced provisions would suffice in assuring that these contractual waivers are fair and balanced.

1. *The Liability Matrix*

a. *ID Hacking*

As explained above, the damages resulting from this concern are inflicted upon the user whose ID was hacked, and on a third party who (wrongfully) relied upon such a hacked persona. While many ID hacks and breaches result from the sophistication of the attacker and negligence of the user, many others are caused by an insecure infrastructure set in place by the soft eID intermediary. Intermediaries could limit these forms of risks by requiring stronger passwords, engaging in advanced forms of authentication and verification, as well as tightening up their overall infrastructure security.

Clearly, however, setting a high standard of care at this juncture will generate additional costs which will, no doubt, be passed on to all users. Usability of the overall system will probably suffer as well given the installation of additional security measures. Nonetheless, this high standard is called for at this juncture to assure that this concern would be minimized by a party who is quite capable of doing so—the soft identity intermediary.

A high standard of care should indeed be applied in instances where the relevant soft eID is a Real Name. Here, damages to both identity users and third parties are substantial. The ease with which such an identity could be linked to the offline realm enhances the damages and thus the platforms' responsibility. However, liability (while relying on a somewhat lower standard of care, given

the differences noted above) should still be assigned to identity intermediaries enabling Stable Pseudonyms. Here too, users and third parties may suffer damages related to the loss of control over an extension of the self, as well as reliance upon an assumedly trusted persona.

A very difficult question arising in this context is whether a different standard must be set for damages related to Real Names applied in either a mandatory or voluntary scheme. Contradicting arguments could be set forth. Intermediaries applying mandatory Real Name schemes should perhaps be subjected to a higher standard of conduct because they do not allow their users to select an option which will allow such users to limit the risks of online hacks. On the other hand, when applying a voluntary scheme, one might argue that in this context, individuals specifically opt for a real name, clearly signaling their expectation that the security of their persona would be maintained. This might also be the expectation of third parties relying upon voluntary (as opposed to mandatory) IDs. It is also quite difficult to predict how the market will react to different levels of liability for these two different forms. Given our discussion above, it is challenging to establish which form of intermediation is normatively superior (and thus should receive a higher level of protection). For these reasons, perhaps a mandatory/voluntary liability-based distinction should not be made at this juncture, but only after additional study. This analytical point pertains to the subsequent segments of the analysis as well (and thus will not be repeated).

Finally, one might argue that setting the relatively high standard level here noted might provide a substantial disincentive to firms, who will thereafter refrain from offering (or mandating) the Real Names option. Such a concern is probably misplaced. Firms have many incentives to provide for this option—as it generates benefits in terms of the personal data they may collect and the advertising value they may reap.[317] A higher standard of care would not dampen the appetite for these identification measures.

b. *Impersonation*

With regard to this potential concern of identity intermediation, it is first important to note that the distinction between this and the previous example is somewhat delicate and easily overlooked. The damages caused at this juncture to both the relevant individual impersonated and third parties are very similar to those noted above (yet as explained both the sense of losing control as well as the actual damages in this instance are usually less severe). However, the steps to be taken by an identity intermediary to limit these harms are very different. Here, the direct tortfeasor does not "hack" an existing account, but starts an account using the name of another. To mitigate harms related to impersonation, eID intermediaries can engage in user verification prior to opening a Real Name account. They may, for instance, rely on other established verification methods

317 *See* Edwards, *supra* note 94, at 9, and accompanying text.

(as Amazon makes use of credit cards) to limit impersonation *ex ante*. They can also rely on recommendations of other users (similar to the way Facebook allows for the indication of an impersonating account) *ex post*. The options for doing so are endless. Identity intermediaries, however, have only limited motivation to engage in these activities and thus liability should be assigned.

As noted above, assigned liability generates problematic outcomes. Beyond the costs, a strict level of liability will motivate firms to apply aggressive measures to limit this form of impersonation. As this Article's opening example demonstrates, such steps might also lead to harms and aggravation to various users. They also require identity intermediaries to collect even more personal data. Applying various aggressive measures to limit this concern might even generate unjust distributions; the high costs of proving one's true identity upon registration might limit the access of specific, weaker segments of the population (for instance, individuals without credit cards) to these powerful tools of speech and discourse. For this reason, the threshold of care in this context should be lower than the one applied in the previous segment.

At this point again, the distinction between Real Names and Stable Pseudonyms must be noted and leads to different legal conclusions. Impersonation clearly generates harms when a Real Name is applied. In such a context, liability should be assigned, as discussed. Yet finding liability when merely Stable Pseudonyms are impersonated might be unwise. Indeed users of a stable and known "handle" could be harmed when others assume their name—and third parties might also rely on such a misrepresentation. Their reputation might be tarnished and they will suffer from their inability to express themselves while using this virtual persona in all realms. However, recognizing this form of liability might come at too high a cost. For firms to protect themselves sufficiently, they might be required, upon authorizing the usage of every new Stable Pseudonym, to examine whether it is being used by others in different platforms. Such an inquiry will be complex and not always fruitful. Thus, here liability in the context of Stable Pseudonyms should be limited, perhaps only established by market forces; firms will only be subjected to the contractual obligations they specifically undertake.

A final point regarding this issue calls for an exception to liability. In some rare cases, impersonation of celebrities must be allowed, as it can prove to be powerful and important form of criticism. In many instances it is quite clear that the Pope, President Obama, or Bill Gates is not using specific profiles given the nature of the content or other elements. Thus, they will not suffer from an identity-related harm.[318]

c. *Identity Misrepresentation*

In this final scenario, damages (and thus the liability that might follow) do not inflict users of the intermediation process, but third parties who relied upon

---

[318] *See* Ramasastry, *supra* note 159; *see also* discussion *supra* note 176.

the identity-based misrepresentations the intermediaries enabled. While these damages are severe, they might be countered by social norms which call for treating much of the information conveyed by people one never met in person (or have limited prior connections with) skeptically and with caution.

Generating liability for platforms in the case of reliance on such inaccurate information and misperceived identity will in fact require platforms to find ways to limit these forms of misrepresentation. Here, although the damages are somewhat different, the reaction is similar to the one noted above (with regard to impersonation). Intermediaries will be required to examine, upon registration, whether the identity used online reflects the one applied offline. The main difference between these cases being that, in this latter case, there is no individual who can step forward and complain that his or her persona was abused. This renders authentication challenging, even for the prudent intermediary (a factor to be accounted for when considering the intermediary's diligence). Note that for this discussion, we merely focus on the authentication of "identity" as narrowly defined (the individual's name), rather than other factors that might enable identification.

At this juncture, and given the limited damages which only pertain to third parties (who could limit such damage by engaging in cautious behavior) one must question whether indeed setting even a moderate standard of care is called for. As noted above, the measures intermediaries will take to limit this risk might be viewed as intrusive. In addition, to adequately set the level of care and liability, referring to the Real Name/Stable Pseudonym distinction can prove helpful. For Real Names, a similar level of care to the one addressed in the previous segment (regarding impersonation) is called for. After all, the steps required to limit these two risks are quite similar—matching identification information with the online persona.

Yet things are quite different when facing intermediation of Stable Pseudonyms. If liability is set, the intermediary will be facing an almost impossible task of limiting these risks. To do so, the intermediary might be required to examine and investigate private identity information pertaining to a pseudonymous user—a task which even sounds like a contradiction in terms. These inquiries will indirectly inhibit the online discourse. Individuals will fear that their presentations would be subjected to examination and inquiries by the platforms, and thus limit their exchanges. It is also unclear whether platforms are well equipped to achieve these objectives. In addition, it will prove quite difficult to distinguish between the authentication of "identity" and the abundance of other factors used as part of such intermediation (which are beyond the scope of this analysis and require a different set of balances). Therefore, in the interest of mitigating privacy and security concerns (and allowing for some form of anonymous discourse), liability is best limited at this latter juncture. Furthermore, given the low level of reliance, this context should allow deference to the contractual framework set forth by the relevant platforms.

It should be noted that, nonetheless, some platforms move to address these issues in various ways. In some contexts, they strive to assure that presentations made by their users are accurate. They sanction users (at times by removing them from the service) when they present inaccurate identity-related information. Platforms include relevant provisions in their user agreements to enable such actions. We believe they should be allowed to do so and act upon them. Courts, however, will have an important role in assuring that platforms carry out such internal policing fairly. They must limit the firms' discretion and allow users to explore, when such actions do not generate harm, the limits and borders of virtual identity structuring.

Table 1: *Summary of Liability Recommendations*

	ID Hacking	*Impersonation*	*Identity Misrepresentation*
Real Name	High Standard of Care	Intermediate Standard of Care	Intermediate Standard of Care (yet lesser damages given lower social expectations)
Stable Pseudonym	Intermediate Standard of Care	Limited Liability – Market Forces + Court Supervision of Contractual Framework	No Liability (greater deference to contractual framework)

2. *Setting a Standard: Courts or Regulators?*

While the discussion above provided some basic benchmarks regarding the forms of liability and standards of care to be set at various junctures, we must further inquire as to how courts will establish whether the intermediaries have acted suitably. Usually, the court's opinion is formulated after examining the facts at hand and possibly the opinions of experts. These will inform the court as to the state of the art, and the way it relates to the actual practices applied.

Yet the advanced technological setting here discussed might be a poor fit for such a legal practice. Courts are ill equipped to interpret these situations properly, especially after the fact. In addition, the mostly general and vague rules set by courts will impede the firms' ability to structure and update technological interfaces given legal uncertainty. Therefore, and as explained above, even when opting for a liability-based regime for regulating soft identity intermediaries, law can take a strategic stand by indicating the acceptable level of technological standards.

Here again, the ideas noted in EU law might prove helpful, but with somewhat of a twist. Rather than setting a mandatory or voluntary regime in place, regulators can set a "safe harbor" form of identity intermediation—both for the security and the verification tasks. These rules can serve as a minimal standard of behavior and care, later to be used by courts approaching the issues

noted above. In addition, a breach of such a minimal standard might also lead to fines, thus resolving some of the issues noted in Part IV.B.1 *supra*. In conclusion, although this solution calls for a somewhat reactive role for law, which is led by courts, additional strategic steps for regulators serve as an important supplement to this overall legal response.

D. *Legal Strategies To Enhance Property/Publicity Rights*

The law can also play a role in resolving this second set of concerns, and on various levels. As the eSig and other newer regulatory and technological ventures indicate, the law may respond by directly encouraging *mobility* and *interoperability*. Law could set mandatory or voluntary standards, delineating ways in which these important objectives should be achieved. The law can also play an active role in enhancing the individual's property/public interest by limiting the intermediaries' ability to *terminate* the user account.

For reasons noted above in various contexts (regarding the risk and futility of directly regulating technology by government), we find these somewhat aggressive steps unwise. Governments are poorly positioned to force firms into engaging in mobility and interoperability in this context, or to note what forms of termination are unacceptable. Yet there are "softer" and less intrusive ways in which the law can enhance mobility and interoperability, and thus the property/personality rights related to identity.[319] As Randy Picker notes, at times third parties strive to provide users with either the mobility or interoperability experience.[320] They do so by creating technological solutions which facilitate such services while piggybacking on the intermediaries' systems.[321] These initiatives can enhance the user interests here discussed. The powerful intermediaries are however less than pleased with these forms of innovative developments. They strive to block such initiatives both technologically and legally. To do so, they prohibit the use of these measures in their terms of use and sanction users who do not comply (at times by terminating their accounts).[322]

At this point, Picker observes, law can intervene.[323] Courts can find that these contractual terms (or in other instances, attempts to rely upon property or IP rights) are enforced in bad faith, and require the intermediaries to enable

---

[319] For a similar argument, see Ruben Rodrigues, *Privacy on Social Networks: Norms, Markets, and Natural Monopoly*, *in* THE OFFENSIVE INTERNET: PRIVACY, SPEECH, AND REPUTATION 237, 246–49 (Saul Levmore & Martha C. Nussbaum eds., 2010).

[320] Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 NW. U. L. REV. 1, 6–8 (2008), *available at* http://www.law.northwestern.edu/lawreview/colloquy/2008/25/LRColl2008n25Picker.pdf.

[321] *Id.*

[322] See discussion regarding the use of the Plaxo screen scraper by a Facebook user, the fact that this practice constituted a breach of Facebook's terms of service, and Facebook's termination of the user's account thereafter. *See* Grimmelmann, *supra* note 92, at 1198.

[323] Picker, *supra* note 320, at 11–12.

these interoperability/mobility-via-third-parties activities.[324] Courts can actively refrain from upholding contractual provisions which aim to inhibit the developing of tools for transferring information to other platforms or allowing these platforms to interact. While Picker makes this argument in the antitrust context, a similar argument for limiting the reach of these contractual and legal provisions could be premised upon identity interests as well. This, in fact, might be the extent of the proper role for law in promoting identity interests at this juncture. In doing so, courts should also distinguish between Real Name and Stable Pseudonym-based intermediation. As explained above, it is the latter case in which users require greater protection, and thus courts should be more aggressive in allowing third parties to enable interoperability and mobility (and remove contractual and technological obstacles intermediaries might set in place to block them).

Courts (and thus the law, in its responsive capacity) can also play an important role in limiting the firm's ability to unilaterally *terminate* user accounts, while noting the identity interests articulated above. Again, in doing so, courts should provide greater protection to Stable Pseudonyms. At least in one case (that of *Bragg*) this was precisely the position the court took.[325]

To conclude, here the proper role for law is responsive, rather than strategic. The law should probably not lead the way in a move to promote these identity interests in the soft eID context, but allow third parties to enhance the users' autonomy. Yet the government can promote the identity interests noted while assuming an *educational* role as well. Regulators, for instance, can promote awareness of the ways in which platforms enable or inhibit interoperability and mobility or tend to terminate accounts. For instance, regulators may introduce a disclosure format which platforms must follow, and clearly report on the extent of mobility, interoperability, and termination to their users and the public in general. These and other disclosure and educational initiatives might prove constructive in promoting the discussed identity-based objectives by either third parties or the intermediaries' direct competitors. They might also inhibit intermediaries from taking such aggressive actions in advance, as they would fear the repercussions of such public "shaming."

VII. CONCLUSION: WHAT IS NEXT FOR ONLINE INTERMEDIARIES?

This Article chose to address the legal response to a specific novel issue—soft eID intermediation. However, the discussion above could not do this matter justice. A discussion of identity intermediation is both over- and under-inclusive. It is over-inclusive, as regulating these intermediaries calls for discussing the acceptable level of privacy and security protection—an issue which was intentionally overlooked yet must be integrated into any policy discussion carried out at this juncture. The same could be said regarding the

---

[324] *See* Kahn, *supra* note 137, at 227–28.

[325] *See* Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593, 608 (E.D. Pa. 2007).

lack of a discussion as to the problems of "hate speech," "identity theft," and "cyber bullying"[326]—all dynamics enabled by the identity intermediation process and overlooked in this analysis. Policy decisions addressing how these troubling issues should be approached will no doubt impact the way the law regulates identity intermediation and intermediaries.

Our discussion is under-inclusive as well. Discussing the notion of the identity intermediaries' liability and responsibility is merely a segment of a broader set of rules governing the digital environment. The identity intermediaries are at times powerful market players. Thus, regulating their identity intermediation capacities must be part of an overall competition law strategy for dealing with these dominant online entities. Furthermore, identity intermediaries are "online intermediaries." Thus, their regulation is part of an overall debate as to the level of scrutiny (or immunity) online intermediaries and platforms must be subjected to.[327] Only after approaching these broader notions, can the proper regulation of this specific matter of identity intermediation be finalized.

Yet with all its flaws, the discussion above provides important insights. It generates an overall mapping of the issues related to identity intermediation, and allows policy makers to prioritize among them. The key to the regulator's success in the digital age is in properly selecting battles worth fighting—as every battle requires substantial force, manpower, and attention—as well as concessions made in other contexts. The analytical structure provided above can prove helpful in setting forth a regulatory agenda with short and long term goals.

Above all and as noted at several points throughout this Article, identity intermediation raises intriguing questions which call for additional examination and analysis. We hope this Article provides a helpful contribution for beginning this inquiry and achieving a better understanding of the benefits and challenges of soft eIDs and their intermediaries in the years to come.

---

[326] *See* Megan Meier Cyberbullying Prevention Act, H.R. 1966, 111th Cong. §§ 2–3 (2011), *available at* http://www.govtrack.us/congress/bills/111/hr1966/text (this bill was not enacted).

[327] For a discussion of Section 230 in this context, see David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373 (2010).