

## Developments

### ***Review Essay – Helen Nissenbaum’s Privacy in Context: Technology, Policy, and the Integrity of Social Life (2010)***

By Tiffany Wong\*

[HELEN NISSENBAUM, *PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE*, STANFORD UNIVERSITY PRESS, 2010; ISBN-13: 9780804752374, 304 pp.; \$24.95]

#### **A. Introduction**

Social media is a dominating force in modern social life as internet technology has taken hold of our cyber-driven society. Many scholars, as will be explored below, have articulated fears and enthusiasm about what can be interpreted as a reconfiguration of privacy in a culture mediated by technology. Scholarship ranges from those opposing new conception of privacy in favour of protecting rights in traditional private/public distinctions with privacy as a privilege worthy of proprietary protection<sup>1</sup> to those reveling in opening floodgates for information to re-invent or even destroy any semblance of traditional distinctions of privacy.<sup>2</sup> These poles become even more accentuated in light of fast-proliferating technology illustrated by popular social networking websites such as Facebook, Twitter, FourSquare<sup>3</sup> etc. In the North-American debate, the privacy concerns connected with these developments are compounded further by the U. S. Supreme Court’s recent decision, *Nelson v. NASA*,<sup>4</sup> which involves the constitutional right of government to

---

\* JD Candidate 2011, Osgoode Hall Law School, York University (Toronto, Canada); BA McGill University (Montreal, Quebec, Canada); Senior Editor & Book Review Editor, German Law Journal. Email: tiffanywong@osgoode.yorku.ca.

<sup>1</sup> See, Nissenbaum’s discussion of Ruth Gavison’s definition of privacy as a “measure of the access other have to you through information, attention, and physical proximity.” HELEN NISSENBAUM, *PRIVACY IN CONTEXT* 68 (2009) [Nissenbaum]; philosopher, Jeffrey Reiman’s definition of privacy as “the condition under which other people are deprived of access to either some information about you or some experience of you.” *Id.*, 70; legal scholar, Anita Allen’s definition of proprietary privacy as “control over name, likenesses and repositories of personal information.” *Id.*, 71; Charles Fried “who suggested that privacy is a necessary condition for love, friendship and trust.” *Id.*, 97.

<sup>2</sup> See, Nissenbaum’s discussion of social media website, Facebook and its founder, Mark Zuckerberg: *Id.*, 61-2; and her reference to experts and non-experts today asserting categorically that “the youth of today do not care about privacy.” *Id.*, 221.

<sup>3</sup> See, FourSquare, available at: <http://foursquare.com/>.

ask for employee's personal information in the context of national security and surveillance.

Helen Nissenbaum, professor of Media, Culture and Communication and Computer Science and Senior Fellow of the Information Law Institute at New York University is well-situated in a timely debate. Her recent book, *Privacy in Context: Technology, Policy and the Integrity of Social Life*, is the subject of this book review, and speaks from her existing repertoire as coeditor of *Academy and the Internet* (2004), *Computers, Ethics, and Social Values* (1995), and *Emotion and Focus* (1985).<sup>5</sup>

Deeply engaged in an international scholarly dialogue on these questions, Nissenbaum joins a network of scholars such as Daniel J. Solove,<sup>6</sup> author of *Understanding Privacy*<sup>7</sup>, Yochai Benkler, author of *The Wealth of Networks*<sup>8</sup> or Ian Kerr,<sup>9</sup> author of *On the Identity Trail*, all of whom contribute to a lively discourse that reflects these and other scholars' increasing lack of comfort with the re-conceptualization of privacy in the 21<sup>st</sup> century.

---

<sup>4</sup> U.S. Supreme Court case, *NASA v. Nelson* 562 US 2011 is considered one of "the first constitutional rights to information privacy cases in a generation;" see, Lior Strahilevitz, *The Centenarian Who Wasn't, NASA v. Nelson, and the Constitutional Right to Information Privacy*, UNIVERSITY OF CHICAGO LAW SCHOOL, FACULTY BLOG (23 September 2010), available at: <http://uchicagolaw.typepad.com/faculty/2010/09/the-centenarian-who-wasnt-nasa-v-nelson-and-the-constitutional-right-to-information-privacy.html>.

<sup>5</sup> See, Helen Nissenbaum's New York University faculty biography, available at: [http://www.nyu.edu/projects/nissenbaum/main\\_cv.html](http://www.nyu.edu/projects/nissenbaum/main_cv.html).

<sup>6</sup> Solove has also commented on privacy rights in *NASA v. Nelson* in Daniel Solove, *NASA v. Nelson: Is There a Constitutional Right to Information Privacy?*, CONCURRING Opinions (9 March 2010), available at: <http://www.concurringopinions.com/archives/2010/03/nasa-v-nelson-is-there-a-constitutional-right-to-information-privacy.html>.

<sup>7</sup> See, DANIEL J. SOLOVE, *UNDERSTANDING PRIVACY* (Harvard University Press, 2008); Solove is a Professor of Law at George Washington University Law School who in this cited book provides an overview of surveillance, data mining, identity theft and other privacy related issues, available at: <http://docs.law.gwu.edu/facweb/dsolove/Understanding-Privacy/>.

<sup>8</sup> See, YOCHAI BENKLER, *THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM* (Yale University Press, 2006); Benkler is a Professor of Law at Yale Law School who discusses in this cited book the phenomenon of "social production in reshaping markets, while at the same time offering new opportunities to enhance individual freedom, cultural diversity, political discourse, and justice," available at: <http://yalepress.yale.edu/yupbooks/book.asp?isbn=0300110561>; see also, electronic version of this book available at: [http://cyber.law.harvard.edu/wealth\\_of\\_networks/index.php?title=Download\\_PDFs\\_of\\_the\\_book](http://cyber.law.harvard.edu/wealth_of_networks/index.php?title=Download_PDFs_of_the_book). For a review of the book, see James Brink, *Book Review – Yochai Benkler, The Wealth of Networks: How Social Production Transforms Markets and Freedom (2006)*, 7 GERMAN LAW JOURNAL 853-862 (2006), available at <http://www.germanlawjournal.com/index.php?pageID=11&artID=765>.

<sup>9</sup> Ian Kerr is the Canada Research Chair in Ethics, Law and Technology at the University of Ottawa, Faculty of Law; see, *LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY* (Ian Kerr, Valerie Steeves, and Carole Lucock, eds., Oxford University Press, 2009); see also, electronic version of this book available at: <http://www.idtrail.org/content/view/799>.

The next part of this book review includes a brief summary of the main ideas of Nissenbaum’s *Privacy in Context*. Part C will provide a critical analysis of her ideas with some concluding remarks and an outlook in Part D. This review attempts to assess the potential of Nissenbaum’s book to generate future discussion on pressing issues pertaining to the re-contextualization of privacy in social life mediated by the proliferation of emerging social networking technology.

### **B. Mapping Traditional Privacy Concerns and Proposing its Recontextualization**

*Privacy in Context* is evenly divided into three parts: Part I “Information Technology’s Power and Threat” which provides context for her book’s discussion, Part II “Critical Survey of Predominant Approaches to Privacy” which provides an overview of existing conceptions of privacy, and these opening two-thirds of the book culminate in Nissenbaum’s thesis in Part III “The Framework of Contextual Integrity” where she expands on her theory of privacy beyond traditional notions of the public-private distinction into political and legal philosophy.

More specifically, Part I presents an overview of fears surrounding a history of emerging technology, privacy issues that flowed from it and resolutions for re-ordering our approach to privacy. Nissenbaum discusses how “monitoring and tracking is not a new addition to an existing range of human social activities.”<sup>10</sup> Examples include the impact of technology on privacy and social activity, such as video surveillance in public places by CCTV (closed-circuit television),<sup>11</sup> public roadways equipped with Radio Frequency Identification (RFID) technology systems that log the passage of registered vehicles particularly for toll plazas,<sup>12</sup> online monitoring using authenticated logins, and cookies tracking IP addresses<sup>13</sup> etc. By providing this overview, Nissenbaum illustrates how our daily social interactions are mediated by prevalent systems for “watching over people” that consist of “massive storage and analytic capabilities,” not all of which are controversial.<sup>14</sup>

This is followed by Part II, which features a description of some prevailing approaches to the concept of privacy. Central here is the private/public distinction<sup>15</sup> that Nissenbaum aims to deconstruct in the last third of her book. She explains that “in some arenas, the

---

<sup>10</sup> NISSENBAUM (note 1), 21.

<sup>11</sup> *Id.*, 22.

<sup>12</sup> *Id.*, 25.

<sup>13</sup> *Id.*, 29.

<sup>14</sup> *Id.*, 64.

<sup>15</sup> *Id.*, 90.

term private signals the realms of the familial, the personal, or intimate relations, while the term public signals civic actions (e.g. in the Habermasian 'public sphere')<sup>16</sup> beyond the home and the personal.<sup>17</sup> This distinction is considered in light of other contexts influencing privacy beginning with the historical protection of constitutional rights against unreasonable search and seizure by the government of private individuals namely in the criminal context<sup>18</sup> and the on-going debate about the collection of personal data, such as online credit card information with and without explicit permission from the user.<sup>19</sup> A common fear among the scholars that she cites is that "an ever-growing array of technology-based systems and practices have radically altered the flows of personal information" in a manner that conflicts with the public/private dichotomy that is "commonly supported in academic work and supported in law and policy."<sup>20</sup> Nissenbaum emphasizes that her critique is "does not amount to a total rejection" of a black-and-white approach of dividing social life into two parts, rather the one consisting of multifarious contexts each governed by its own set of particular norms, such as contexts with privacy norm governing the workplace, health care, schools, or among family and friends. She asks instead for a nuanced approach that considered "privacy restriction tailored to the actors in question."<sup>21</sup>

The main crux of *Privacy in Context* emerges in Part III where Nissenbaum expands on her thesis amid existing discourse presented in Part II. Her central thesis is that "a right to privacy is neither a right to secrecy nor a right to control, but a right to *appropriate* flow of personal information."<sup>22</sup> The author then proceeds to develop her "framework of contextual integrity." Beginning in Chapter 7, "Contexts, Informational Norms, Actors, Attributes, and Transmission Principles,"<sup>23</sup> Nissenbaum "builds fundamental building blocks of contextual integrity" by defining social contexts and context-relative information norms as:

---

<sup>16</sup> See, generally, JÜRGEN HABERMAS, *THE STRUCTURAL TRANSFORMATION OF THE PUBLIC SPHERE: AN INQUIRY INTO A CATEGORY OF BOURGEOIS SOCIETY* (1991).

<sup>17</sup> NISSENBAUM (note 1), 90.

<sup>18</sup> *Id.*, 92; see also, *id.*, 99 for a discussion of U.S Supreme Court case, *California v. Greenwood* (1998) 486 U.S. 35 where persons have no reasonable expectation of privacy for personal garbage placed on a curbside can be the subject of government searches by virtue of being discarded in a public space.

<sup>19</sup> *Id.*, 100.

<sup>20</sup> *Id.*, 125.

<sup>21</sup> *Id.*, 126.

<sup>22</sup> *Id.*, 127.

<sup>23</sup> *Id.*, 129.

...depend[ing] on the function of the types of information in question, the respective roles of the subject, the sender and recipient of the information and the principles under which the information is transmitted from the sender to the recipient.<sup>24</sup>

Three case studies, the Clinton-Lewinsky Scandal, the *Gramm-Leach-Bliley Act*<sup>25</sup> of 1999, and Canada’s controversy surrounding the *Personal Information Protection and Electronic Documents Act* (PIPEDA) of 2000<sup>26</sup> pertaining to the privacy of medical prescriptions,<sup>27</sup> illustrate various transgressions over the line dividing public from private. Chapter 8 “Breaking the Rules for Good” elucidates additional context-relative information norms with respects to a variety of modern technological social contexts such as voting, employment, caller ID and so forth.<sup>28</sup>

Mindful of these controversies, Nissenbaum nevertheless believes that privacy is not only about personal information. As stated in a press interview, her thesis aims to:

First, demonstrate that the private-public distinction, as useful as it may be in other areas of political and legal philosophy, is a terrible dead-end for conceptualizing a right to privacy and for formulating policy [...] Second, challenge the definition of privacy as control over information about oneself [...] If the right to privacy is the right to control then of course it must be moderated, traded-off, compromised for the general good!<sup>29</sup>

---

<sup>24</sup> *Id.*, 127.

<sup>25</sup> The *Gramm-Leach-Bliley Act* (GLB) Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999, also known as the *Financial Services Modernization Act* of 1999, sought among other matters, to redraw conditions under which financial institutions disclosed nonpublic personal information about consumers and resulted in law suits against the Federal Trade Commission (FTC) that its rules flowing from this legislation were unlawful and unconstitutional: *Id.*, 100, 153-156.

<sup>26</sup> The *Personal Information Protection and Electronic Documents Act* (PIPEDA) 2000, c.5 is Canadian federal legislation relating to data privacy that governs how private-sector organizations collect, use, and disclose personal information in the course of commercial business. It influences many areas of privacy including the privacy of medical prescriptions and consumer trust in electronic commerce. The Act was also intended to reassure the European Union that Canadian privacy law was adequate to protect the personal information of European citizens. Since 2010, PIPEDA has been subject to a number of significant amendments regarding personal information and internet spam. For more legal information about PIPEDA, see Office of the Privacy Commissioner of Canada, available at: [http://www.priv.gc.ca/leg\\_c/leg\\_c\\_p\\_e.cfm](http://www.priv.gc.ca/leg_c/leg_c_p_e.cfm).

<sup>27</sup> NISSENBAUM (note 1), 156-7.

<sup>28</sup> *Id.*, 158.

<sup>29</sup> See, interview with Nissenbaum: Danielle Citron, *Bright Ideas: Helen Nissenbaum’s Privacy in Context: Technology, Policy and the Integrity of Social Life*, CONCURRING OPINIONS (18 January 2010), available at:

In short, Nissenbaum's thesis counters against a one-dimensional private/public distinction to encourage a recontextualization model where information ought to be distributed and protected according to norms governing distinct social contexts.<sup>30</sup> *Privacy in Context* therefore presents a pivotal tension between concern for the improper sharing of information by alleviating it with the concept of the "context-appropriate" flow of information integral to social and political life.<sup>31</sup> As such, she asserts that individuals should only be alarmed when contemporary information systems function in a manner that weakens social norms and values could weaken the "fabric of social life."<sup>32</sup>

### C. Embracing a Future of Recontextualized Privacy Norms

Prior literature that is influential on Nissenbaum's theory of contextual privacy is also comfortable accepting the pace of technology change and the impact that it has on traditional notions of privacy. In light of prior discourse, such as the development of constitutional rights, and normative conceptions of privacy argued by legal philosophers ranging from John Stuart Mill's *On Liberty* to Ruth Gavison's article, "Privacy and the Limits of the Law,"<sup>33</sup> who are in a traditional vein of theorists that purport the dominance of the public/private distinction. As a departure from this traditional distinction, Nissenbaum's book might be read as an alarmist polemic about the period of the degradation of these traditional notions of privacy in 21<sup>st</sup> century (post)modern, urban life. However, she has presented a fair, balanced, densely-written and rigorous viewpoint on considering privacy in a variety of contexts. Although Nissenbaum puts forth some concrete arguments justifying this alarmist fear, she also points out modes of resistance (and perhaps a generationally-based tendency) towards recontextualization that is driven largely by technology. For a new generation "digital natives,"<sup>34</sup> in my view, many alarmist fears have been brushed aside, dealt with by a few clicks of a mouse, and most notably, by intuitively

---

<http://www.concurringopinions.com/archives/2010/01/bright-ideas-helen-nissenbaums-privacy-in-context-technology-policy-and-the-integrity-of-social-life.html>.

<sup>30</sup> *New Book – Privacy in Context*, THE NEW TRANSPARENCY: SURVEILLANCE AND SOCIAL SORTING, available at: <<http://www.sscqueens.org/news/new-book-privacy-in-context>>.

<sup>31</sup> NISSENBAUM (note 1), 187.

<sup>32</sup> *Id.*, backcover, 3.

<sup>33</sup> *Id.*, 68, 78, 92; Nissenbaum particularly focuses on a comparative analysis of the ideas of Ruth Gavison, *Privacy and the Limits of the Law*, 89 YALE LAW JOURNAL 421-471 (1980).

<sup>34</sup> This term was originally coined by Mark Prensky, *Digital Native, Digital Immigrants*, 9(5) ON THE HORIZON, (MCB University Press, October 2001), available at: <http://www.marcprensky.com/writing/prensky%20-%20digital%20natives,%20digital%20immigrants%20-%20part1.pdf>; Prensky's ideas have expanded into an entire project on Youth & Media at the Berkman Center for Internet & Society at Harvard University, available at: <http://youthandmedia.org/>.

reframing these negatives related to the loss of privacy as potential opportunities to develop social life in a radically different way.

Thankfully, Nissenbaum paints a picture of modern life without one-mention of the clichéd Orwellian “Big Brother”<sup>35</sup> watching over citizens— a literary figure that conjures-up paranoid images of surveillance by power over privacy in untrustworthy hands. She cites rather from a wide range of classical and contemporary legal scholars, sociologists and philosophers, including Jeremy Bentham, Michel Foucault, Pierre Bourdieu, Ronald Dworkin, Richard Posner, and Lawrence Lessig. Although she considers a variety of online examples impacted by the subject of privacy, it would be beneficial to her book’s thesis to include scholarship from blogs by digital media specialists, grassroots advocacy organizations, industry experts, and media law academics, such as Michael Geist.<sup>36</sup> Institutes such as Harvard University’s Citizen Media Law Project at the Berkman Center for Internet and Society,<sup>37</sup> Oxford’s Programme in Comparative Media Law and Policy at the Centre for Socio-Legal Studies,<sup>38</sup> Osgoode Hall Law School’s Intellectual Property Law and Technology Program (IPOsgoode)<sup>39</sup> in Toronto and advocacy organizations such as the British Columbia Civil Liberties Association,<sup>40</sup> the latter of which is active in protecting privacy and personal information as well as criminal records disclosure, that are also important sources pushing for the recontextualization of privacy.

Therefore, Nissenbaum builds her thesis incrementally by mapping out a theoretical landscape and responds directly to it. She suggests a nuanced, un-paranoid approach to privacy that considers “context-appropriate flows” of information<sup>41</sup> to conclude that a proper understanding of the social structure of contexts prevents a slippery slope down to

---

<sup>35</sup> See, GEORGE ORWELL, *NINETEEN EIGHTY-FOUR* (1949) that originally created the fictional character, “Big Brother,” an enigmatic dictator of a dystopian world surveilled by a paternalistic-governmental entity.

<sup>36</sup> Michael Geist is the Canada Research Chair of Internet and E-commerce Law at the University of Ottawa and publishes a scholarly blog featuring commentary and analysis about recent developments in Canadian internet law, available at: <http://www.michaelgeist.ca>.

<sup>37</sup> Citizen Media Law Project, available at: <http://www.citmedialaw.org/>; Berkman Center for Internet & Society at Harvard University, available at: <http://cyber.law.harvard.edu/>.

<sup>38</sup> University of Oxford’s Programme in Comparative Media Law & Policy (PCMLP), available at: <http://pcmlp.socleg.ox.ac.uk/>; PCMLP is affiliated with the University of Oxford’s Centre for Socio-Legal Studies, available at: <http://www.csls.ox.ac.uk/>.

<sup>39</sup> Osgoode Hall Law School’s Intellectual Property Law and Technology Program (IPOsgoode) features an academic blog by students and legal professionals about a wide variety of recent developments in Canadian and global intellectual property issues, available at: <http://www.iposgoode.ca/>.

<sup>40</sup> British Columbia Civil Liberties Association, available at: <http://www.bccla.org/>.

<sup>41</sup> NISSENBAUM (note 1), 187.

a society “throwing away [its] privacy in tiny bits.”<sup>42</sup> Nissenbaum, however, could have taken a more forceful stance on what has become a reordered society based on a redefined notion of privacy. While she aims at echoing what she perceives as a widespread concern that “the youth of today do not care about privacy,”<sup>43</sup> as previously mentioned, she could have elaborated further on these changes being impacted by generational differences in approaches and conceptualization of privacy mediated by new technologies. Indeed, privacy as a concept in today’s society is embarking upon a high-speed, revolutionary pathway (that is patently obvious to any regular internet-user), and which is lost upon those uncomfortable with the impact of connecting via social networks individual strangers globally and which changes within intervals of a few years, even months, when a new website, mobile application, or computer technology appears almost immediately on the mass commercial market. The recent box-office popularity of *The Social Network* movie,<sup>44</sup> an Oscar award-winning Hollywood hit that dramatized the development of the social networking website Facebook in the early 2000s, is already coming across as a historical commentary of a time when we could still remember privacy in its traditional context; a simple public/private distinction that is much less relevant today. Indeed, today’s context involves rapidly changing contexts, which in themselves are the new contexts of which Nissenbaum speaks and where traditional notions of privacy are increasingly marginalized and reformulated.

The last third of Nissenbaum’s *Privacy in Context* could, therefore, segue into a subsequent book on recontextualized privacy. Particularly, the first two thirds has potential to further map out an intricate web of issues covering key contexts, such as medical disclosure,<sup>45</sup> social discussions in the context of personal friendships,<sup>46</sup> surveillance in the workplace,<sup>47</sup> and tracking individuals in the public sphere via GoogleMaps<sup>48</sup> and CCTV.<sup>49</sup> In future works, Nissenbaum could delve deeper on the notion of appropriate contextual flows on information in light of specific contexts like online social media and surveillance which are

---

<sup>42</sup> *Id.*, 243.

<sup>43</sup> *Id.*, 221.

<sup>44</sup> See, movie review of *The Social Network*: J.R. Jones, *The Price of Privacy: In ‘The Social Network,’ Facebook founder Mark Zuckerberg Learns a Thing or Two About It*, CHICAGO READER (30 September 2010), available at: <http://www.chicagoreader.com/chicago/the-social-network-movie-review-chicago/Content?oid=2492182>; see also, THE SOCIAL NETWORK’s official movie website, available at: <http://www.thesocialnetwork-movie.com/>.

<sup>45</sup> NISSENBAUM (note 1), 156-7.

<sup>46</sup> *Id.*, 59-62.

<sup>47</sup> *Id.*, 216.

<sup>48</sup> *Id.*, 217.

<sup>49</sup> *Id.*, 192-3.



becoming the most dominant contexts today with still developing norms and likely to be target of striking global debate in the near future.

Indeed, these contexts for privacy have been the subject of concern by various, often alarmist, online rights groups and legal interveners reinforcing traditional notions of privacy, led especially by groups such as Privacy Rights Watchdog,<sup>50</sup> Electronic Frontier Foundation (EFF),<sup>51</sup> and the Electronic Privacy Information Center.<sup>52</sup> What these groups do is recognize that new contexts have appeared in the social landscape and therefore argue in favour of creating acceptable norms to govern privacy in such contexts. In my view, a traditional private/public distinction could be balanced further with the opposite extreme of post-modern free-play and unfettered free-flow of information in a society increasingly comfortable with “private” information intermingling with “public” information (e.g. by surveying the mass popularity of reality television,<sup>53</sup> up-to-the-minute personal status and video updates that “go viral” on blogs and YouTube,<sup>54</sup> and celebrity sex tape scandals<sup>55</sup> etc. that voyeuristically celebrate the loss of traditional notions of privacy by mixing it with too-often low-brow entertainment).

Finally, while Nissenbaum acknowledges that her book is written mostly from an American perspective,<sup>56</sup> she has considered examples and international scholarship from European, Canadian and Australian perspectives in formulating her thesis about context-specific norms in contemporary information systems. For instance, she provides a brief case study of Canada’s PIPEDA<sup>57</sup> acknowledging that “I know too little about the details of PIPEDA and of this case [about medical prescription disclosure]” compared to Canada’s privacy commissioner, George Radwanski. She nevertheless drew a conclusion that eschews an overreliance on an “artificial distinction between information *about* a person and

---

<sup>50</sup> See, Privacy Rights Watchdog, available at: <http://protectprivacyrights.com/>.

<sup>51</sup> The Electronic Frontier Foundation (EFF) is also acting as intervener for recent U.S. Supreme Court case, *Nelson v. NASA*, see *supra* note 4; EFF’s *amicus curiae* on the impact on civil liberties for collection of state employee information are available at: [https://www.eff.org/files/filenode/nasa\\_v\\_nelson/nasavnelsonamicus.pdf](https://www.eff.org/files/filenode/nasa_v_nelson/nasavnelsonamicus.pdf).

<sup>52</sup> See, Electronic Privacy Information Centre, available at: <http://epic.org/>.

<sup>53</sup> See, for example, popular television shows such as MTV’s *Jersey Shore*, *The Hills*, and Fox Network’s *American Idol* etc.

<sup>54</sup> A self-posted YouTube video launched the career of international celebrity, Canadian teenaged pop singer-performer, Justin Bieber.

<sup>55</sup> See, e.g., celebrity sex-tape scandals with billionaire hotel heiress, Paris Hilton, Heidi-Spencer from popular MTV reality television show series, *The Hills*, etc.

<sup>56</sup> NISSENBAUM (note 1), 16.

<sup>57</sup> *Id.*, 156-7.

information *associated with* a person.<sup>58</sup> Nissenbaum also provided a case study of the UK experience with CCTV surveillance<sup>59</sup> that could have expanded further into debate for national contexts for security and law enforcement in a post-9/11 world that extolls fears of terrorism and results in governmental control over personal information,<sup>60</sup> and the application of this political context to the no longer mundane utility of Google Maps' Street View.<sup>61</sup> As privacy issues particularly related to the internet is a global issue, it is beneficial to her thesis of recontextualization that assumed a global application to have more closely explored treatments of privacy in other jurisdictions.

By exploring international aspects of privacy in a global context, the applicability of Nissenbaum's thesis could be expanded by examining the reformulation of privacy on an international level using legal, cultural, political, social, and economic approaches abroad. It would be insightful to read her future predictions and solutions on the basis of suggesting specific examples of how to rethink privacy in a globalized context: Does Nissenbaum advocate strict confidentiality in any contexts? Is there a meaningful or practicable impact of absolute emancipation of free-information? Are there reasonable limits to privacy in some contexts over others? Can contexts continually adapt to changing technology and hence our norms relating to it? By addressing these questions, Nissenbaum could propose a more revolutionary re-ordering of approaches to privacy that I interpret as a more accurate reflection of actual worldwide trends that are currently throwing away vestiges of privacy regardless of naysayers trying to recapture a seemingly uncontrollable phenomenon that has already sprinted out of the gates.

#### D. Conclusion

In conclusion, Nissenbaum's *Privacy in Context* is a timely, densely written, comprehensive, well-organized book on a contemporary topic. Her central points are evenly summarized after each chapter to provide clarity and purpose to the reader. It is readable for general, academic, and legal audiences by presenting privacy as a hot topic of debate without the alarmist rhetoric featured in the news media trumpeting allegations of privacy breaches.<sup>62</sup>

---

<sup>58</sup> *Id.*, 157.

<sup>59</sup> *Id.*, 16, 192-3, 217, 234-5, 245n2.

<sup>60</sup> *Id.*, 22, 188, 192.

<sup>61</sup> *Id.*, 193.

<sup>62</sup> See, e.g., Bill Curry, *Privacy Breach at Veterans Affairs 'Struck Terror in Our Hearts,'* THE GLOBE AND MAIL (22 September 2010), available at: <http://www.theglobeandmail.com/news/politics/privacy-breach-at-veterans-affairs-struck-terror-in-our-hearts/article1718767/>; see, e.g., use of "super-injunctions:" Cassell Bryan-Low, *Celebrities Boost Use of U.K. Gag Order,* WALL STREET JOURNAL (8 October 2010), available at: <http://online.wsj.com/article/SB10001424052748704011904575538002160153046.html>; see, e.g., Wendy

Information based on context-appropriate flows therefore becomes relevant as privacy is currently taking on a new dimension as the “personal,” for example, is increasingly intertwined with the “professional” in the public sphere.<sup>63</sup> Nissenbaum does, however, discuss a context where both personal and professional information is volunteered on Facebook profiles that results in the user increasing his or her risk of getting “Facebook fired”<sup>64</sup> if discovered by a watchful employer. As such, a greater exploration of social media and networks in its increasing complexity in specific contextual norms would be beneficial to the reader in further positioning Nissenbaum’s concepts in everyday cyber-reality. *Privacy in Context* ultimately appeals to law students, legal scholars and technophiles alike who are interested in the issues that drive today’s approach to law and technology in re-contextualizing privacy rights.

---

Kaminer, *Restoring American Privacy*, THE ATLANTIC (7 October 2010), available at: <http://www.theatlantic.com/national/archive/2010/10/restoring-american-privacy/64221/>.

<sup>63</sup> NISSENBAUM (note 1), 225.

<sup>64</sup> “Facebook fired” is a colloquial term referring to the phenomenon that Nissenbaum’s describes without using this particular term: see, *id.*