Millennial Dissonance:
An Analysis of the Privacy Generational Gap

Matthew J. Sher
Department of Computing Sciences
Villanova University
Villanova, Pennsylvania 19085, U. S. A.
matthew.sher@villanova.edu

Abstract. The young Millennial generation has adopted social media and internet technology to an unprecedented degree. But this generation's extensive usage of online services leaves Millennials open to various privacy vulnerabilities that have emerged with the new technology. Older generations hold concern that Millennials are ignoring the value of privacy when disclosing their personal information in exchange for online connectivity. This paper investigates the generational privacy concern through different perspectives. It cites studies of Millennial behavior to ascertain the generation's outlook on privacy. It extrapolates from recent online privacy trends to outline possible consequences of Millennial privacy behaviors. It concludes with some reasons the Millennial generation may effectively resist exploitation by invasive database corporations.

Keywords: privacy, social media, Millennial generation, Facebook, Google

1 Introduction

Forty years ago, few people would have imagined a future in which every person lives through both a physical form and a virtual identity. Few people would have guessed that human beings could be socially connected to one another through a series of digital signals and the exchange of their own personal information. The emerging digital society of the new millennium could be interpreted as a historical anomaly by some, or as a natural progression of information exchange by others. But regardless of social perspective, the fact remains that the world is changing by means of the internet. And the internet itself is evolving even more rapidly. Online services like Google and Facebook have changed the lives of hundreds of millions of people through their powerful management and distribution of information. But much of this is information about us. It has been said that using such services comes at a price: our privacy. Much debate has surrounded this topic as Google and Facebook continue to alter their own privacy policies so that less and less of our personal information is kept secret. Internet privacy policies, like the internet itself, will inevitably continue to evolve over time. Rather than discuss the reasonability of these changes, this paper explores how this evolution is changing us.

Every generation holds the belief that its collective identity is unique. However, the Millennial Generation, the population that came of age during the new

millennium, has an objective basis for believing itself unique: the usage of new technology. "It's not just their gadgets," says a Pew Research report on U.S. Millennial social trends, "it's the way they've fused their social lives into them. For example, three-quarters of these Millennials have created a profile on a social networking site" [1]. Millennials are involved with modern internet technology in a profound way. Their behaviors are, in a sense, the first significant result of the internet's social effects. Consequently, older generations fear that Millennials' acceptance of online connectivity might lead to the end of online privacy, or more generally, a redefinition of privacy itself. A common concern is that Millennials' persistent involvement with online social media has built up a level of indifference towards online anonymity and privacy. Facebook CEO Mark Zuckerberg referenced this apparent trend towards openness to justify yet another corporate shift away from a private Facebook infrastructure. He said, "People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people… We view it as our role in the system to constantly be innovating and be updating what our system is to reflect what the current social norms are" [2]. Zuckerberg's assertion, while not incorrect, raised concerns about the issue of privacy among Millennials and non-Millennials alike.

This paper will investigate the validity of the generational privacy concern and then explore some explanations and consequences for this social phenomenon. It is important to note, however, that most studies of Millennial tendencies are necessarily limited in geographic scope, applying primarily to advanced Western societies and less so to the developing world. Furthermore, the studies only reveal general trends within this exceptionally diverse and individualistic generation.

2   Millennial Attitudes on Privacy

2.1   Deliberate Disclosure

The decision to share information online is a conscious choice, and most Millennials understand the tradeoff that comes with connectivity. In an April 2010 Harris poll [3], 85% of the surveyed Millennials acknowledged that, by participating in social media, they are giving up part of their privacy. 81% said that they share only a small portion of their personal information in crafting their online identities. These percentages are actually very similar to those of the preceding generations. From these data, it appears that Millennials are just as aware of the risks of online connectivity as any other generation.

In spite of their awareness, Millennials apparently hold that the benefits of social media greatly outweigh the privacy risks that come with it. The threat of reduced privacy does little, if anything, to deter Millennials' usage of social media. In taking advantage of the social media tools at hand, Millennials express themselves through the information they share over the internet. They do not wish to restrict their social interactions to people in close proximity. As one Millennial blogger remarks, "getting a reaction from the masses – instead of from your couch buddy – can be more addictive than settling down for a real conversation with only one person" [4]. In this

respect, Millennials could be considered a socially exhibitionistic generation. A certain amount of public approval confers a boost in self-esteem and personal validation. "Millennials are more visible on the Web," reports Douglas MacMillan of *Businessweek*. "Respondents aged 18 to 29 were the most likely to say they'd posted photos of themselves and other personal data for others to see on such Web sites as Facebook and MySpace" [5]. Many Millennials live a significant part of their lives online, and to ask them to relinquish that way of life out of concern for their privacy would not only be unthinkable, but also detrimental to their concept of identity.

2.2 Strict Privacy Controls

While their mentality may seem reckless from an outside perspective, Millennials have a different way of seeing the privacy issue. Heather West, writing at *Wired* explains, "Digital immigrants tend to think about privacy as the ability to conceal information from others. Digital natives instead share information within certain contexts, and with granular privacy controls on that information" [6]. Older generations tend to see privacy as keeping as much of their personal information off the internet as possible, but Millennials are different in this respect. Millennials, in a sense, want to be found, but they want to be found in ways for which they themselves are responsible. Julian Sanchez from *Cato @ Liberty* points out, "Privacy is not just a function of the raw quantity of information available about each of us, but of the control we exercise over that information" [7]. It is precisely because Millennials rely so heavily on social media that many are so self-conscious regarding the information displayed about themselves.

To preserve the integrity of their online identities, Millennials take advantage of built-in privacy controls to regulate the visibility of their information. Most major social media tools offer a range of settings that can be changed to control which groups of people can access an individual's information, and to what depth. Macmillan reports findings that "seventy-one percent of social networking users aged 18 to 29 said they'd adjusted privacy settings on social networks in order to make some information private" [5]. In contrast to common assumptions, researchers have found that Millennials are the most vigilant managers of online information among the generations of social media users studied [5]. Privacy controls in social media give Millennials an attractive compromise in choosing between privacy and connectivity. These controls allow information to be distributed selectively and thereby enable some advantages of both privacy and connectivity. Not only do Millennials take advantage of privacy controls to personalize their networking experience, but they have also come to expect them as a standard feature to protect their personal information.

2.3 Distrust of Social Media

A significant and unexpected finding from these online social media studies is that Millennials do not trust social networking websites. The Millennial generation is the

least trusting age group of social networking websites. One of the more surprising examples of this trend was found in a 2010 survey of young women, the most extensive users of social media. These female social media users, ages 18-24, displayed a surprising level of cynicism towards Facebook. 89% of them knew not to post content that they want to hide from their parents, 72% felt that information put on Facebook will remain there forever, and 54% said that they did not trust Facebook with their private information [3]. With such a level of distrust towards social networking sites, Millennials are significantly more likely than older users to hide certain comments or photos that they feel threaten their online identities. Many Millennial social media users are constantly pruning their online interactions in order to maintain a pristine online reputation. A majority of online Millennials now use search engines to check what kinds of information are available on them across the internet [5].

2.4   Comments on the Findings

The loosening of privacy values by large online services is not the result of a growing apathy towards privacy by the Millennial generation. Rather, nearly the opposite is true. The Millennial generation is reacting skeptically to a changing commercial approach towards information management. Millennials do not want to make any mistakes in exposing too much of their information, so they have learned to exercise a degree of caution when dealing with social media. "Many teens and certainly most young adults make thoughtful decisions about what information to share, and in what context," says West at *Wired* [6]. Millennials may have learned this caution from the mistakes of their predecessors. In the earlier days of social networking websites, several reckless privacy blunders caused serious trouble for the first users of such services. The consequences of these exhibitionistic behaviors ranged from employment difficulties to political resignations. The incidents shattered the initial illusion of online behavioral impunity, sending a wake-up call to those who would next discover social media, but also burning an expectation of online recklessness into the minds of older generations [8]. The youth of every generation have always been seen as rash and indiscreet by those that preceded them. The perception of Millennials' online recklessness is possibly an extension of this trend.

   It will take a compelling crisis to separate the Millennial generation from its social media. Since the technology is so tightly integrated with their lives, Millennials will not abandon social media out of distrust. They would rather accept the risks of online connectivity and counter the consequences themselves. Because they have made such a decision, they are forced to manage their online footprints carefully. This self-consciousness leads to a level of online vigilance that contradicts outside opinions on today's youth. Since many Millennials have built their lives around social media, they treat the technology seriously. And this seriousness is what motivates Millennials to take control of their online information. Generally speaking, older generations seek privacy by avoiding the internet, while Millennials seek privacy by controlling it. Modern adults have the right to be concerned for today's youth, but online social networks are the Millennials' home turf. They have demonstrated that they take their own game seriously.

3 Consequences of Privacy Concession

3.1 Worst Case Scenarios

Millennials have proven themselves generally concerned for their online privacy, but they undeniably concede a certain amount of it to large database services and the public eye. And these concessions, willing or not, will have an impact on Millennials' lives in the future. This concern provokes a myriad of differing predictions. And it would be almost natural to spiral into the prognosis of a dystopic worst case scenario. George Orwell's social science fiction novel *1984* is a frequently cited metaphor for a society deprived of individual privacy. The novel presents a dystopia in which totalitarianism and uniformity are enforced by invasive surveillance technology and political propaganda. The ruling Party, represented by the enigmatic figurehead "Big Brother," can erase all evidence of a person's existence at the first sign of observable deviance. The fictitious regime serves as a powerful illustration of how people's private information can be collected and abused in terrifying ways.

The Orwellian Big Brother metaphor is powerful and popular, but it does not adequately capture the kind of privacy issues that Millennials will have to face. In the 2004 book, *The Digital Person*, Daniel J. Solove acknowledges the merits of this metaphor, but also points out its limits in accounting for current concerns with large, online databases. "Certainly, monitoring is an aspect of information collection, and databases may eventually be used in ways that resemble the disciplinary regime of Big Brother. However… the goal of much data collection by marketers aims not at suppressing individuality but at studying it and exploiting it" [9]. Information is being collected from internet users at all times, but at present, the character of the collectors is vastly different from that of a totalitarian state. In this respect, the Big Brother metaphor falls short in its relevance to the Millennial privacy concern. Therefore, it should be more constructive to explore the consequences that are already emerging with the technology. A cautionary notion to keep in mind is not to think of these consequences as strictly positive or negative, but rather as changes – possible transitions in human social behavior for the new millennium.

3.2 Privacy Ignorance

The first of these possible consequences could be termed "privacy ignorance." Data suggest that Millennials do indeed care about their online privacy, but this attitude has only a partial effect on the precision Millennials exhibit when controlling their information. Their outlook does not necessarily improve the knowledge Millennials possess about what information is available about themselves. A study of college students at Columbia University suggests that most Facebook users do not fully understand the privacy settings that the service presents to them. The study found that each of the 65 interviewed Millennials was sharing or restricting some personal information unintentionally [10]. While Millennials certainly bear the responsibility for controlling their own information in this age, the study finds that a great deal of confusion can be attributed to poor conveyance on the part of Facebook itself. The

study concludes that Facebook's current approach to privacy settings is fundamentally flawed, and must be redesigned so that a user's expectations of privacy regularly match the level of privacy achieved.

Given the number of large corporations like Facebook beginning to dominate the trafficking of personal information, Facebook's lack of privacy clarity may be indicative of a larger trend. In *The Digital Person*, Solove discusses the issue of privacy ignorance in regard to what he calls "the database problem." In seeking an alternative to the *1984* allegory, Solove presents the novel *The Trial* by Franz Kafka as a more plausible metaphor for the database problem. In *The Trial*, the protagonist, Joseph K., is bewildered to find himself accused of an unknown crime by a nonspecific party. The story follows K's efforts to uncover the details of his accusation as he deals with an apathetic judicial bureaucracy which monitors his life from afar, and which denies him any information regarding the decisions it makes. "*The Trial* captures the sense of helplessness, frustration, and vulnerability one experiences when a large bureaucratic organization has control over a vast dossier of details about one's life. At any time, something could happen to Joseph K.; decisions are made based on his data, and Joseph K. has no say, no knowledge, and no ability to fight back" [9]. From this perspective, *The Trial* resonates powerfully with the treatment of user information by large database corporations.

Facebook and Google both collect and exploit information about its users. Both companies reportedly monitor keyword and hyperlink usage to make decisions about the ads and search results a user sees while using their products. Additionally, Facebook has voiced its bold intentions to share users' phone numbers and home addresses with certain third-party companies, regardless of user privacy settings [11]. A user may be able to take down or block online information from the public, but these acts rarely remove the information itself. Once a company like Facebook acquires information, it is that company's decision how it is put to use, assuming no third-parties have siphoned the same information. In some cases, invisible third-party trackers can acquire personal information through larger online services, independently of the first-party company's permission. "For example," an NSDI web tracking paper begins to explain, "Facebook's [tracking] cookie is a first-party cookie when the user visits facebook.com, but it is a third-party cookie when a Facebook 'Like' button is embedded on another webpage" [12]. These third-party cookies can report browsing behavior to third-party trackers. Underhanded data aggregation practices could steadily undermine the very control that Millennials depend on to regulate their exposure – leaving Millennials with a hidden vulnerability and only the illusion of control. But the degree of vulnerability Millennials will ultimately experience could range from the level of Kafka's *The Trial* to something almost nonexistent. Facebook's plan to release information has been heavily criticized by privacy experts, its user base, and the United States Congress [11]. Database companies require the compliance of their user base to function, but ultimately, users have little control over the hidden management of their own online information.

3.3 Social Media Background Checks

Following privacy ignorance, the second type of consequence pertains to background checking. Personalized social media provide people and organizations with an efficient means to investigate others from afar. Such investigations of character can range from legitimate background checks to personal snooping. Already, the Department of Homeland Security has admitted to monitoring social media services like Facebook and Twitter for suspicious postings [13]. Police, too, have checked Facebook pages to help confirm accusations of criminal activity. With the expanding popularity of Facebook and other social media, official background checks via social media may become not only common, but expected. A Facebook page may one day serve a purpose similar to that of a government file, in that it is kept on hand for emergencies. If these online background checks become so thorough, anonymous usernames should retain their value in an otherwise personalized internet. For instance, a blogger of harmless yet controversial material may prefer to write under a pseudonym to escape personal accountability. The fact that authorities can view public information should not come as a shock, nor an outrage. People's identities are simply becoming bigger, bleeding out into a larger world, becoming more noticeable to everyone with an interest. In the future, it may become commonplace for new acquaintances to know some personal information about each other before ever communicating directly.

3.4 Social Media Culture

The third kind of consequence from privacy concession involves the emerging importance of the online reputation. In the Columbia University study, the primary reason that Millennial college students valued online privacy was to protect their online reputation. This reason outweighed their concerns for identity theft, economic risks, and personal safety [10]. The Millennials are developing in a new world, in which everyone has a reputation. Everyone has a page or six to his or her name, displaying personal interests, videos, friends, and photographs. Everyone acts like a celebrity, whose unique thoughts, experiences, and talents are worth broadcasting to all who may listen. It is an emerging new culture of mass exhibitionism – a paradoxical collective individualism. Yet the culture itself is not necessarily harmful. What earlier generations may refer to as "concessions of privacy," Millennials might call "the telling of one's self." Some behaviors that would traditionally "degrade the value of privacy" might be reinterpreted as "reaching out to new people." Millennials have pioneered the social media culture because they grew up with the technology to facilitate its expansion. Social interaction takes on a new meaning with Millennials. They consider less of their information to be private because they have evolved to see personal disclosure as a form of meaningful interaction and interpersonal validation. So while the Millennial attitude did not produce this culture, Millennials' habitual concession of privacy will certainly reinforce the culture as it continues to spread. And a change in privacy values could have significant harmful and beneficial effects on future values in general.

3.5 Coercion by Corporation

The last kind of consequence to consider here is how companies can potentially control the social media culture. The wide adoption of social media suggests that its providers hold some power over society's values. Mark Zuckerberg makes the claim that Facebook evolves to reflect the social norms that have emerged "naturally" over time. But to a certain degree, Facebook is also responsible for creating, or at least influencing these norms. "…We decided that these [privacy behaviors] would be the social norms now and we just went for it," said Zuckerberg in regard to a recent privacy change [2]. Time and time again, users have expressed discontent with changes to Facebook's layout, behavior, and appearance. Yet despite these complaints, the number of Facebook users continues to grow by the millions, and is rapidly approaching its first billion [14]. The trend suggests a certain level of generational dependence on social media, which Facebook can easily exploit for various purposes. A 2012 survey of American and Norwegian college students found Facebook the fourth most preferred mode of communication for social purposes, behind face-to-face, telephone, and texting [15]. With such popularity, Facebook has become an integral part of many people's lives, along with other online services. Google has also made some recent privacy changes. And because Google provides the most instrumental and popularly used search engine on the internet, with an expanding scope of additional services and features, a minor privacy change is rarely seen as a compelling reason to abandon the product. Because of this emerging dependence on online services, these companies have demonstrated the power to make nonconsensual changes to their functionality, with the implicit assurance that the public will rapidly adapt to the concessions required.

4 The Millennials' Defense

Millennials have a few unique weapons to defend against this kind of exploitation. The same individualistic outlook that makes their connectivity exploitable by social media companies also makes Millennials disloyal to the companies themselves. Millennials' individualism makes them less than willing to contribute to a hierarchical, corporate machine. To put trust into a large, faceless corporation is an unsettling idea to Millennials, who favor management structures that are more compatible with their individualistic values. According to *Millennial Inc*, a study of U.S. and U.K. Millennials, this generation prefers flattened leadership structures, in which responsibilities are shared and collaborative, and decisions are made by popular consensus [16]. From a Millennial perspective, most companies are out of touch with emerging modern values. A 2010 study of French Millennials indicates they possess a strong sense of corporate defiance. They do not sympathize with the tedious, hierarchical structure of a corporation, nor do they trust in its decisions. Even commercial advertisements are seen as corporate ploys, which Millennials will often try to outsmart [17]. Much of the online privacy concern involves the unscrupulous usage of information by large scale data aggregators like Google and Facebook, but Millennials are reluctant to trust corporations in general, let alone hand them their

personal information. Even if modern corporations continue to enjoy Millennials' compliance, the Millennial generation will not make a willing target for corporate deception.

Corporate decisions that affect the lives of Millennials are frequently met with a degree of skepticism, so a Millennial's compliance with ethically questionable privacy changes is often hesitant as well. The moment a more effective approach is discovered, many Millennials will be able to switch products easily. This attitude has been particularly evident in the rapidly changing online world. From around 2008 to 2010, the popular social media network MySpace was abandoned in favor of the much more convenient Facebook. Some particularly non-Millennial systems contributed to the collapse of MySpace, including a stagnant corporate structure and a poor privacy policy. Then when a preferable alternative presented itself, social media users began leaving MySpace by the millions, crippling the revenue stream it required to remain a lucrative business [18]. And it is not unreasonable to imagine future repetitions of this Millennial mass exodus. Many Millennials utilize their increased connectivity to stay informed of brand reputations. According to Edelson and StrategyOne's international study of brand behavior, nearly a quarter of surveyed Millennials indicated they would lose respect for a company that exhibited questionable practices. About a third said they would boycott a product or service on the basis of personal values, and a majority said they would encourage others to boycott a company they found untrustworthy [19]. Millennials are certainly becoming dependent on social media for connectivity, but the future of their privacy is not necessarily in the hands of any one brand. Millennials have a strong capacity for change and a strong desire to choose for themselves. So if a popular online service betrays the generation's trust while a clear, preferable alternative is available, Millennials have the ability to sever old attachments swiftly and decisively. Poor privacy would have to become a universal epidemic within all convenient available technologies in order for it to become an inescapable liability for the future.

5 Concluding Remarks

The situation that Millennials face regarding online privacy is a complicated issue. Many conflicting opinions are circulating around what the future holds for this generation. Perhaps the only conclusion that can be drawn from the available evidence is that Millennials will be living in a different world – a digital world – filled with digital problems and possibly digital solutions. At first glance, the Millennials' shameless adoption of social media at the cost of privacy may seem like a mistake. But given their strong stance on privacy control, their generally serious attitude toward personal information, and their wariness of corporate tactics, it would also be a mistake to underestimate their resourcefulness.

References

1. Millennials: Confident. Connected. Open to Change. *Pew Social & Demographic Trends.* Pew Research Center, http://www.pewsocialtrends.org/2010/02/24/millennials-confident-connected-open-to-change/, last accessed 14 Apr. 2012 (2010)
2. Kirkpatrick, M.: Facebook's Zuckerberg Says The Age of Privacy is Over. *ReadWriteWeb.com.* ReadWriteWeb, http://www.readwriteweb.com/archives/facebooks_zuckerberg_says_the_age_of_privacy_is_ov.php, last accessed 14 Apr. 2012 (2010)
3. Phillips, L.E.: Privacy Not a Problem for Savvy Millennials. *eMarketer.com.* eMarketer, http://www.emarketer.com/Article.aspx?R=1007887, last accessed 14 Apr. 2012 (2010)
4. Massa, J.: Privacy in the Millennial Age: Are We Oversharing or Undersharing? *TheHuffingtonPost.com.* The Huffington Post, http://www.huffingtonpost.com/jessica-massa/privacy-in-the-millennial_b_775215.html, last accessed 14 Apr. 2012 (2010)
5. MacMillan, D.: Millennials: Savvy on Privacy. *Businessweek.com.* Bloomberg, http://www.businessweek.com/technology/content/may2010/tc20100526_876848.htm, last accessed 14 Apr. 2012 (2010)
6. West, H.: Is Online Privacy a Generational Issue? *Wired.com.* Conde Nast Digital, http://www.wired.com/geekdad/2009/10/is-online-privacy-a-generational-issue/, last accessed 14 Apr. 2012 (2009)
7. Sanchez, J.: No Privacy Please, We're Millennials. *Cato @ Liberty.* Cato Institute, http://www.cato-at-liberty.org/no-privacy-please-were-millennials/, last accessed 14 Apr. 2012 (2010)
8. Clarke, R.: Privacy Attitudes of the iGeneration. *RogerClarke.com.* Xamax, http://www.rogerclarke.com/DV/MillGen.html, last accessed 17 Apr. 2012 (2011)
9. Solove, D.J.: *The Digital Person: Technology and Privacy in the Information Age.* New York UP, New York (2004)
10. Madejski, M., Johnson, M., Bellovin, S.M.: *The Failure of Online Social Network Privacy Settings.* Columbia University, https://mice.cs.columbia.edu/getTechreport.php?techreportID=1459, last accessed 20 June 2012 (2011)
11. Bosker, B.: Facebook to Share Users' Home Addresses, Phone Numbers with External Sites. *The Huffington Post.* TheHuffingtonPost.com, http://www.huffingtonpost.com/2011/02/28/facebook-home-addresses-phone-numbers_n_829459.html, last accessed 20 June 2012 (2011)
12. Roesner, F., Kohno, T., Wetherall, D.: Detecting and Defending Against Third-Party Tracking on the Web. In *Proceedings of the 9th USENIX Symposium on Networked Systems Design and Implementation.* USENIX Association, http://www.franziroesner.com/pdf/webtracking-NSDI2012.pdf, last accessed 18 July 2012 (2012)
13. Hosenball, M.: Homeland Security Watches Twitter, Social Media. *Reuters.* Thomson Reuters, http://www.reuters.com/article/2012/01/11/us-usa-homelandsecurity-websites-idUSTRE80A1RC20120111, last accessed 20 June 2012 (2012)
14. Key Facts. *Facebook Newsroom.* Facebook, http://newsroom.fb.com/content/default.aspx?NewsAreaId=22, last accessed 10 July 2012 (2012)
15. Robinson, S., Stubberud, H.A.: Communication Preferences Among University Students. *Academy of Educational Leadership Journal*, vol. 16, issue 2, DreamCatchers Group, http://www.freepatentsonline.com/article/Academy-Educational-Leadership-Journal/289620442.html, last accessed 10 July 2012 (2012)
16. *Millennial Inc.* Mr. Youth and Intrepid, http://millennialinc.com/viewPaper.html, last accessed 10 July 2012 (2010)

17. Filloux, F.: Understanding the Digital Natives. *Mondaynote.com*. Monday Note, 25 July, http://www.mondaynote.com/2010/07/25/understanding-the-digital-natives/, last accessed 11 July 2012 (2010)
18. Gillette, F.: The Rise and Inglorious Fall of Myspace. *Businessweek.com*. Bloomberg, http://www.businessweek.com/stories/2011-06-21/the-rise-and-inglorious-fall-of-myspace, last accessed 11 July 2012 (2011)
19. *The 8095 Exchange*. Edelman and StrategyOne, http://www.edelman.com/insights/special/8095/8095whitepaper.pdf, last accessed 10 July 2012 (2010)