Fulfilling Government 2.0's Promise with Robust Privacy Protections

Danielle Keats Citron*

Abstract

The public can now friend *the White House and scores of agencies on social networks, virtual worlds, and video-sharing sites. The Obama Administration sees this trend as crucial to enhancing governmental transparency, public participation, and collaboration. As the President has underscored, government needs to tap into the public's expertise because it does not have all of the answers.*

To be sure, Government 2.0 might improve civic engagement. But it also might produce privacy vulnerabilities because agencies often gain access to individuals' social-network profiles, photographs, videos, and contact lists when interacting with them online. Little would prevent agencies from using and sharing individuals' social-media data for more than policymaking, including law enforcement, immigration, tax, and benefits matters. Although people may be prepared to share their views on health care and the environment with agencies and executive departments, they may be dismayed to learn that such policy collaborations carry a risk of government surveillance.

This Essay argues that government should refrain from accessing individuals' social-media data on Government 2.0 sites. Agencies should treat these sites as one-way mirrors, where individuals can see government's activities and engage in policy discussions but where government cannot use, collect, or distribute individuals' social-media information. A one-way mirror *policy would facilitate democratic discourse, enhance government accountability, and protect privacy.*

Table of Contents

Introduction 823
I. What Is Government 2.0? 827
II. The Privacy Risks of Government 2.0 829

---

* Professor of Law, The University of Maryland School of Law. I owe special thanks to Richard Boldt and Paul Ohm for helping me think through this project in its earliest stages. I also received helpful comments from Annie Antón, Steve Bellovin, Woody Hartzog, Geoff Kravitz, James Grimmelmann, Toby Levin, Frank Pasquale, Joel Reidenberg, Ari Schwartz, Dan Solove, Jay Stanley, Kathy Strandburg, David Super, Peter Swire, and the participants of the Department of Homeland Security's "Privacy and Government 2.0" conference and New York University School of Law's "Federal Online Privacy" conference. Kaveh Saba, Alice Johnson, and Susan McCarty did superb research. I am grateful to Mark Taticchi, Paul Stepnowsky, Andrew Welz, and the Editors at *The George Washington Law Review* for their insightful comments. I also appreciate Dean Phoebe Haddon and The University of Maryland School of Law for supporting my research.

A. Privacy Harms 831
B. Individuals' Privacy Expectations for Government 2.0 834
C. Absence of Robust Legal Protections..... 837
III. Protecting Privacy and Enhancing Civic Engagement with a One-Way Mirror Policy 839
A. The One-Way Mirror Proposal 839
B. Promoting Democratic Participation and Transparency..... 841
C. Objections 843
Conclusion 845

Introduction

President Barack Obama has 1,867,060 MySpace friends,[1] and Andy is one of them.[2] After the 2008 election, Andy hoped that his MySpace friendship with the President would help him keep up with the Administration's policy endeavors. Andy's profile included a variety of personal information, including his hometown, birthday, political views, friends, and interests. It featured photos of Andy's recent trip to Tijuana, Mexico, and noted his enthusiasm for sales and gangster movies.

Unbeknownst to Andy, the Drug Enforcement Administration was investigating a drug ring in his hometown that maintains ties with dealers in Tijuana, Mexico. In connection with the investigation, a data mining program analyzed the profiles of the executive branch's social network of friends and identified Andy as a person of interest. Agents included Andy in a drug-trafficking and terrorist watchlist.[3] Although Andy had no connection to the drug ring, his inclusion on various watchlists cost him a job offer and prevents him from traveling by airplane.

Although Andy's predicament is hypothetical, the privacy risks attendant to government's use of social media are not. In January 2007, Connecticut police arrested Ken Krayeske, a freelance journalist

---

1 MySpace—Barack Obama, http://www.myspace.com/barackobama (last visited Nov. 13, 2009).

2 Although Andy's story is of my imagination, it may soon be routine if we permit Government 2.0 to proceed unchecked.

3 Federal agencies share intelligence and information with state and federal agencies and law enforcement through fusion centers, which facilitate the "information sharing environment" mandated by Congress in the Intelligence Reform and Terrorism Prevention Act of 2004. *See* Danielle Keats Citron & Frank Pasquale, Fixing Fusion Centers: Restoring Liberty and Enhancing Security in the Post-9/11 World 10 (unpublished manuscript, on file with author).

and law student, during the gubernatorial inaugural parade.[4] Police officers recognized Mr. Krayeske from a Connecticut Intelligence Center security bulletin. Law enforcement identified Mr. Krayeske as a potential threat based on his blog postings encouraging protests of the Governor's inaugural ball, his service as a Green Party candidate's campaign manager, and his previous arrest at an antiwar rally.[5] After Mr. Krayeske spent thirteen hours in jail, prosecutors dropped the charges.[6] State legislators and the Governor roundly criticized Mr. Krayeske's arrest and appearance on a threat list.[7]

Civic engagement could increasingly entail the risk of domestic surveillance as government learns more about individuals' online activities. Unfortunately, Government 2.0 is no exception. In January 2009, President Obama's "Transparency and Open Government" memorandum ordered executive departments and agencies to adopt new technologies that would enhance governmental transparency, public participation, and collaboration.[8] True to this policy, the White House "stay[s] connected" with the public through social-network sites, microblogging, and video-sharing sites.[9] The Centers for Disease Control and Prevention provides health information to the public via Facebook, YouTube, Flickr, and Twitter.[10] National Oceanic and Atmospheric Administration officials interact with the public on a virtual island in Second Life.[11]

Government's use of social media[12] offers great promise. It allows agencies and executive departments to reach millions of individu-

---

4 Gerri Willis, *Are You on the List?*, CNN, Sept. 30, 2009, http://www.cnn.com/video/#/video/crime/2009/09/30/willis.fusion.centers.cnn.

5 Gregory B. Hladky, *Arrest Exposes State's Threats List: Activist's Rights Trampled*, *Rell, State Lawmakers Say*, New Haven Reg., Jan. 9, 2007, at A1.

6 *Id.*

7 Jennifer Medina, *Arrest of Activist Troubles Hartford Officials*, N.Y. Times, Jan. 9, 2007, at B6.

8 Transparency and Open Government, 74 Fed. Reg. 4685 (Jan. 21, 2009).

9 The White House, http://www.whitehouse.gov/ (last visited Nov. 13, 2009) (urging the public to connect with the White House on MySpace, Facebook, Twitter, iTunes, YouTube, Vimeo, LinkedIn, and Flickr).

10 Social Media at CDC, http://www.cdc.gov/socialmedia/ (last visited Nov. 13, 2009).

11 Outreach at Earth System Research Laboratory, http://www.esrl.noaa.gov/outreach/ (last visited Nov. 13, 2009).

12 This Essay focuses on government's use of social media, i.e., networked technologies that enable the production and sharing of digital content in mediated social settings. This characterization includes social-network sites where users post personal information, view their network of relations to others, and communicate with others in their network. *See* danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. Computer-Mediated Comm. 210, 211 (2008) (discussing social-network sites like MySpace, Facebook,

als at trivial cost. It permits them to broadcast updates on pressing matters[13] and to post research data.[14] It has the potential to facilitate discussions between agencies and citizen-experts on policy matters[15] and will surely entice people who might otherwise not engage with government to join those discussions.[16] Indeed, the Administration has been successful in translating the public's embrace of networked technologies during the 2008 presidential campaign into an interest in interacting with the Administration online.[17]

Government 2.0 sites depart from the traditional model of public participation. In the past, individuals interacted with government in ways that had little connection to their personal lives. They commented on rulemakings, offered expert testimony, and participated in town hall meetings. At present, people engage with government in networked environments organized around social connections.[18] As James Grimmelmann has explored with great insight, social-network

---

YouTube, Flickr, Bebo, LinkedIn, etc.); Frederic D. Stutzman & Woodrow N. Hartzog, Boundary Regulation in Social Media 5–6 (Oct. 9, 2009) (unpublished manuscript, on file with author).

13 *See* Hilton Collins, *Emergency Managers and First Responders Use Twitter and Facebook to Update Communities*, EMERGENCY MGMT., July 27, 2009, http://www.emergencymgmt.com/safety/Emergency-Managers-and-First.html.

14 *See, e.g.*, Data.gov, http://www.data.gov/ ("The purpose of Data.gov is to increase public access to high value, machine readable datasets generated by the Executive Branch of the Federal Government.").

15 BETH SIMONE NOVECK, WIKI GOVERNMENT: HOW TECHNOLOGY CAN MAKE GOVERNMENT BETTER, DEMOCRACY STRONGER, AND CITIZENS MORE POWERFUL 20–21, 40–42 (2009); Eric E. Holdeman, Opinion, *Twitter: Five Lessons for Emergency Managers from Iran*, GOV'T TECH., June 23, 2009, http://www.govtech.com/gt/697201; *see also* Danielle Keats Citron, *Open Code Governance*, 2008 U. CHI. LEGAL F. 355, 358 (arguing that an open code model for governance can encourage public participation in the administrative state, improve political accountability, and marshal expertise).

16 Many individuals might not have interacted with government about policy due to the considerable transaction costs associated with writing letters, calling agency staffers, and submitting comments on rulemaking. They also may have declined to do so due to their age and life experiences. In the past, younger Americans may not have engaged with executive agencies and the White House because government may have seemed too remote or disinterested in their concerns. As the 2008 presidential election demonstrates, today's youth has become increasingly involved with political campaigns and government decisionmaking, both offline and online.

17 The Pew Internet and American Life Project recently reported that thirty-seven percent of social-network site users expect updates from the Obama Administration via social-network sites and thirty-four percent expect to hear from the Administration via email. AARON SMITH, PEW INTERNET & AM. LIFE PROJECT, PEW INTERNET PROJECT DATA MEMO 1 (2008), *available at* http://www.pewinternet.org/~/media//Files/Reports/PIP_Voter_Engagement_2008.pdf; *see also* AARON SMITH, PEW INTERNET & AM. LIFE PROJECT, THE INTERNET'S ROLE IN CAMPAIGN 2008 (2009), *available at* http://www.pewinternet.org/~/media//Files/Reports/2009/The_Internets_Role_in_Campaign_2008.pdf (documenting the public's avid involvement in the 2008 campaign).

18 *See* danah boyd, *Friends, Friendsters, and Top 8: Writing Community into Being on Social Network Sites*, FIRST MONDAY, Dec. 4, 2006, http://firstmonday.org/htbin/cgiwrap/bin/ojs/

sites are inherently *social*—individuals create their identities, cement relationships, and accumulate social capital by revealing a wealth of personal information.[19] This imbues their interactions with a sense of trust and confidentiality.[20]

Bringing government into these socially driven spaces presents new challenges for privacy.[21] Social-network sites facilitate two-way interactions—agency "friends" have access to individuals' profiles, musings, photographs, videos, and miniblogs just as individuals can view agencies' postings.[22] Nothing prevents agencies from collecting, analyzing, and distributing individuals' *social-media data*[23] for law enforcement, immigration, benefits determinations, and other purposes. Nonetheless, individuals like Andy may be dismayed to learn that their collaboration with the White House or a federal agency entailed the risk of persistent government surveillance.

Some might attribute this problem to the convergence of the public and private spheres and seek to resolve it with these concepts in mind.[24] Yet doing so may complicate matters more than it illuminates them. Because the terms *public* and *private* lack intrinsic meaning, the

---

index.php/fm/article/view/1418/1336 (suggesting that social-network sites create a community through the process of "friending").

19 James Grimmelmann, *Saving Facebook*, 94 Iowa L. Rev. 1137, 1159 (2009).

20 *Id*. at 1159–60. Social-network sites like MySpace and Facebook are less about networking as they are about socializing inside of preexisting networks. danah boyd, *Social Media Is Here to Stay . . . Now What?*, Feb. 26, 2009, http://www.danah.org/papers/talks/MSRTechFest2009.html.

21 Although this Essay refers to microblogging sites like Twitter in passing, it does not focus on them, as they may engender privacy norms that differ from social-network sites and the like. *Compare* danah boyd, *supra* note 20 (explaining that Twitter users see their activities as involving the "public square" and hope to garner the attention of the wider public), *with* Stutzman & Hartzog, *supra* note 12, at 13 (explaining that individuals often maintain separate work and personal Twitter accounts due to privacy concerns).

22 As Part I explains, social-media providers treat agencies like any other users of their service, thus permitting them to access their friends' social-media information if their privacy settings permit. To date, only Facebook does not follow this model; instead, agencies generate "fans," not friends, there. While agency Facebook "fans" can comment on an agency's postings and interact on live chats about policymaking, government cannot view their fans' profiles in their entirety.

23 This Essay uses the terms *social-media data*, *social-network information*, and *social-network data* interchangeably to refer to information revealed on social-media sites that does not involve feedback on policy matters.

24 *See* Aristotle, *Book 1*, *in* Politics 3–13 (H. Rackham trans., Harvard Univ. Press 1944) (1932) (explaining his concept of the public state and the private family); John Stuart Mill, On Liberty 68–74 (Gertrude Himmelfarb ed., Penguin Books 1974) (1859) (discussing the interaction between the struggle of liberty—the private self—and authority—the public sphere).

boundary between them is not sharp.[25] As a result, discourse about public and private spheres focuses on a multitude of concepts, some overlapping, making it difficult to categorize many circumstances.[26] A public/private binary also may not accord with our lived experiences—individuals routinely carve out zones of privacy in so-called public spaces.[27] Thus, notions of the public and the private may not provide an effective tool to resolve Government 2.0's privacy dilemma.

This Essay argues that government should refrain from accessing individuals' social-media data. It contends that government should view Government 2.0 sites as one-way mirrors, where individuals can see government's activities and engage in policy discussions but where government cannot use, collect, or distribute individuals' social-media information. This would advance the goals of open government. Strong privacy rules enhance deliberative democracy by encouraging participation and by discouraging self-censorship.

I. What Is Government 2.0?

President Obama is widely known as the "first tech president,"[28] and his "Open Government" initiative demonstrates this moniker's accuracy.[29] On January 21, 2009, the President ordered executive departments and agencies to adopt "new technologies" that would "put information about their operations and decisions online" and improve the public's ability to participate and collaborate in policymaking.[30] The President has urged the adoption of social media because "government does not have all the answers and public officials need to

---

25 Duncan Kennedy has explained that the public/private distinction is so incoherent that it cannot help us describe, explain, or justify anything. Duncan Kennedy, *The Stages of the Decline of the Public/Private Distinction*, 130 U. PA. L. REV. 1349 (1982).

26 Alan Freeman & Elizabeth Mensch, *The Public-Private Distinction in American Law and Life*, 36 BUFF. L. REV. 237, 247–50 (1987) (arguing that the public/private distinction collapses on itself, has no objective content, and is incoherent). For example, the economy involves the public arena for some; it implicates the private sphere for others. *Id.* at 250–52.

27 *Cf.* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 66–70 (2001) (noting that employees create privacy spaces in public workplaces). Stutzman and Hartzog argue that social-network sites defy the public/private categorization—users have privacy expectations that instead fall along a continuum, from complete anonymity, to practical obscurity, to complete transparency. Stutzman & Hartzog, *supra* note 12, at 14.

28 Chris Snyder, *Government Agencies Make Friends with New Media*, WIRED, Mar. 25, 2009, http://www.wired.com/epicenter/2009/03/government-agen/.

29 Transparency and Open Government, 74 Fed. Reg. 4685 (Jan. 21, 2009); *see also* Macon Phillips, *WhiteHouse 2.0*, posting to The White House Blog (May 1, 2009, 14:03 EDT), http://www.whitehouse.gov/blog/09/05/01/WhiteHouse/.

30 Transparency and Open Government, 74 Fed. Reg. 4685 (Jan. 21, 2009).

draw on what citizens know."[31] Social media provides government with an inexpensive way to garner the expertise and feedback of millions of individuals.[32]

Government 2.0 permits a "two-way interaction between government and its citizens" through online comments, live chats, and message threads.[33] For instance, the President's Facebook page asks: "Have thoughts on the President's priorities on science and technology? Join the live chat."[34] The Federal Emergency Management Agency ("FEMA") explains to subscribers and friends on its YouTube video channel that it hopes to provide the public with a chance "to see how FEMA operates in communities across America, comment on disaster response and recovery, and learn how to prepare homes and communities for all hazards."[35] The State Department connects with the public on LinkedIn[36] and maintains an embassy in Second Life.[37]

States, municipalities, and emergency responders have embraced social media as well.[38] For instance, the Los Angeles Fire Department distributes videos to friends and subscribers on YouTube, befriends citizens on MySpace, and urges users to share photos and videos on Facebook.[39]

---

31 Beth Noveck, *Enhancing Citizen Participation in Decision-Making*, posting to The White House Blog (June 10, 2009, 13:08 EDT), http://www.whitehouse.gov/blog/Enhancing-Citizen-Participation-in-Decision-Making/.

32 Facebook now has over 250 million members. Caroline McCarthy, *Facebook Hits a Quarter Billion Users*, CNET News (July 15, 2009), http://news.cnet.com/8301-13577_3-10287336-36.html. MySpace has over 100 million members. Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 851 n.8 (W.D. Tex. 2007); *see also* Jon Swartz, *MySpace Cranks Up Heat in Facebook Turf War*, USA Today, Dec. 23, 2007, at 1B. They have different audiences in these networked environments—MySpace and Facebook communities tend to have different socioeconomic backgrounds, ages, nationalities, etc. *See* danah boyd, *supra* note 20.

33 Saul Hansell, *The Nation's New Chief Information Officer Speaks*, posting to The New York Times Bits Blog (Mar. 5, 2009, 14:57 EST), http://bits.blogs.nytimes.com/2009/03/05/the-nations-new-chief-information-officer-speaks/.

34 The White House, posting to Facebook—The White House (Aug. 6, 2009, 14:20 EST), http://www.facebook.com/WhiteHouse.

35 YouTube—FEMA's Channel, http://www.youtube.com/user/fema?blend=1&ob=4 (last visited Nov. 13, 2009). The Federal Trade Commission has a YouTube channel as well. YouTube—FTCvideo's Channel, http://www.youtube.com/user/FTCvideos (last visited Nov. 13, 2009).

36 U.S. Department of State Company Profile, LinkedIn, http://www.linkedin.com/companies/u.s.-department-of-state (last visited Nov. 13, 2009).

37 L. Gordon Crovitz, Opinion, *From Wikinomics to Government 2.0*, Wall St. J., May 12, 2008, at A13.

38 *See* Hilton Collins, *Emergency Managers and First Responders Use Twitter and Facebook to Update Communities*, Gov't Tech., July 27, 2009, http://www.govtech.com/gt/701799.

39 *Id.*

Generally, the government interacts with social-media users just as any individual participant would. Social-network sites like MySpace provide agencies access to individuals' personal information (assuming their privacy settings permit) and vice versa. Agencies might be able to view individuals' videos, photographs, political and religious affiliations, and revealing commentary. Video-sharing sites like YouTube operate in a similar way. Agencies can see information and videos that friends and subscribers share with others.[40] By contrast, the social-network site Facebook designates the friends of government agencies and corporations as fans whose social-media information cannot be accessed.[41]

Government 2.0 certainly has potential to heighten the public's awareness of, and ability to provide feedback on, policymaking. Caution is, however, in order. Social-media scholar Clay Shirky warns that government's rush to adopt Web 2.0 technologies may end in "catastrophe."[42] The next Part addresses what Shirky may have been alluding to—the privacy risks of Government 2.0.

II. The Privacy Risks of Government 2.0

Civic engagement and privacy have long enjoyed an uneasy relationship. Working for a political advocacy group might expose one's policy views to interested agencies, but it also might unexpectedly lead to the release of sensitive personal information to the government. This phenomenon was true during the 1950s and 1960s when officials in the South sought the names and addresses of NAACP members[43] and when the Federal Bureau of Investigation spied on activists in the civil rights and anti–Vietnam War movements whom it viewed as threats to national security.[44]

This risk has continued into the twenty-first century. In 2005 and 2006, Maryland State Police officers conducted surveillance of human rights groups, peace activists, and death penalty opponents to identify

---

40 Saul Hansell, *Should the White House Be a Place for Friends?*, posting to The New York Times Bits Blog (May 4, 2009, 10:24 EDT), http://bits.blogs.nytimes.com/2009/05/04/should-the-white-house-be-a-place-for-friends/.

41 *Id.*

42 Interview with Clay Shirky by Meet the Innovators (June 15, 2009), http://media.bonnint.net/wtop/15/1560/156071.mp3 (available online in mp3 format).

43 NAACP v. Alabama, 357 U.S. 449, 453, 466 (1958) (striking down Alabama court order requiring NAACP to produce list of its members on the grounds that privacy in group association is indispensable to preserving the freedom to associate).

44 WARD CHURCHILL & JIM VANDER WALL, THE COINTELPRO PAPERS 95, 165–66 (1990).

potential "threats."[45] The investigation resulted in the classification of fifty-three nonviolent political activists as "terrorists," including two Catholic nuns and a former Democratic candidate for local office.[46] More recently, the Missouri fusion center[47] issued a report discussing the modern militia movement in which it suggested to law enforcement officials that these "extremists" are supporters of third-party candidates like Ron Paul and Bob Barr.[48] Individuals labeled as extremists did little more than affiliate with groups opposed to government policy.[49]

Government 2.0 could contribute to this trend. While social media permits individuals to provide feedback to government on policymaking, it also provides government access to their social-media data, including their group affiliations and other sensitive information. Unlike the civil rights activists of the 1950s, who surely would not have willingly provided Southern officials access to their personal information, individuals today establish online connections with government that make them vulnerable to surveillance. Government could, in fact, learn more about individuals from Government 2.0 sites than it could from traditional law enforcement tactics given the breadth of personal information that individuals voluntarily reveal online.[50] This Part explores the nature of Government 2.0's privacy risks and why individuals often fail to appreciate them. It concludes by exploring current law's inability to adequately address these concerns.

---

45 Nick Madigan, *Spying Uncovered*, BALT. SUN, July 18, 2008, at 1A.

46 Bob Drogin, *Spying on Pacifists: Greens and Nuns*, L.A. TIMES, Dec. 7, 2008, at A18, *available at* http://articles.latimes.com/2008/dec/07/nation/na-cop-spy7; Lisa Rein, *Maryland Police Surveillance Listed Some Activists as Terrorists*, WASH. POST, Oct. 8, 2008, at B1.

47 *See supra* note 3.

48 MO. INFO. ANALYSIS CTR., MIAC STRATEGIC REPORT: THE MODERN MILITIA MOVEMENT (2009), *available at* http://www.firearmscoalition.org/images/news/miac-militia-2009.pdf.

49 Chad Livengood, *Agency Apologizes for Militia Report on Candidates*, SPRINGFIELD NEWS-LEADER (Mo.), Mar. 25, 2009, at 1A. The fusion center intended the report only for the eyes of police officers—it was made public after being leaked on the Internet. *Id.* The fusion center apologized to former presidential candidates Ron Paul, Bob Barr, and Chuck Baldwin for linking them to the modern militia movement in the report. *Id.* The Missouri fusion center has ceased distribution of the February 20, 2009 report. Chad Livengood, *State Retracts Militia Report*, SPRINGFIELD NEWS-LEADER (Mo.), Mar. 26, 2009, at 1A.

50 While a traditional investigation might require police to obtain a warrant to gain access to sensitive personal information residing on a person's computer, for instance, there is no such requirement for Government 2.0 sites, which may give government access to similarly revealing personal information that individuals voluntarily post.

A. Privacy Harms

Government 2.0 sites can interfere with individuals' privacy in various ways. Agencies may use individuals' social-media information for purposes other than garnering feedback on policy. A party can intrude on another's privacy by using information for "purposes unrelated to the purposes for which the data was initially collected without the data subject's consent."[51] Daniel Solove's insightful taxonomy of privacy problems describes this as a "secondary use" privacy intrusion.[52]

Rather than using a person's social-media data for policymaking purposes, executive departments and agencies could share it with law enforcement, immigration, and tax authorities.[53] This possibility is not remote. Law enforcement regularly analyzes social-network information to identify criminals, terrorists, and other threats.[54] Police departments reportedly have a constant presence on MySpace and Facebook to identify sex offenders, murderers, and other criminals.[55] For instance, detectives in Auburn, Maine, explain that they obtain "photos of crimes" that suspects post on their social-network profiles.[56] Denver's Joint Information Center monitored social-network sites and blogs during the 2008 Democratic National Convention to gain intelligence on potential saboteurs.[57]

---

51 DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 131 (2008).

52 *Id*. at 129–33; *see* Danielle Keats Citron & Leslie Meltzer Henry, *Visionary Pragmatism and the Value of Privacy in the Information Age*, 108 MICH. L. REV. 1107, 1114 (2010) (reviewing Daniel J. Solove's *Understanding Privacy*).

53 It is crucial to note that nothing suggests that agencies have already engaged in such secondary use of their friends' social-media data. This Essay urges government to adopt policies that would preclude this possibility, which the law, to date, largely does not.

54 Citron & Pasquale, *supra* note 3, at 12–13.

55 Jim McKay, *The New Neighborhood Watch*, GOV'T TECH., Sept. 2009, at 24. In The Netherlands, law enforcement agencies use social-network data to learn about criminal activity and to monitor affiliates of known criminals. Joseph Bonneau et al., Prying Data Out of a Social Network (2008) (unpublished manuscript), *available at* http://www.cl.cam.ac.uk/~jra40/publications/2009-ASONAM-prying-data.pdf.

56 McKay, *supra* note 55, at 28. I use this example not to suggest that law enforcement may never use social-network data in their investigations. Quite the contrary. As Part III discusses, the one-way mirror policy ought to be cabined to instances where government uses social-network sites to garner feedback on government policy and to engage citizens in democratic discourse. Government could use other social-network data for investigative purposes if the law so permits.

57 Jeannette Sutton, *The Public Uses Social Networking During Disasters to Verify Facts, Coordinate Information*, GOV'T TECH., July 30, 2009, http://www.govtech.com/gt/706523. It appears that the Denver fusion center obtained social-media data from the Internet, i.e., information that individuals released to the public through blogging and social-network sites. This

The intelligence community has expressed interest in following law enforcement's lead. The National Security Agency has funded research on the production of intelligence from social-network data.[58] Although individuals may be prepared to tell the White House their views about health care or the environment, they may not expect the agency to collect and distribute their social-media data for other purposes.

An agency's secondary use of social-media data could have harmful consequences. Individuals may face erroneous arrests.[59] For example, British police mistakenly arrested the host of a birthday party after he invited seventeen friends to an "all-night party" on Facebook.[60] Officers identified the Facebook posting as important evidence that the party might turn into an illegal rave or music festival.[61] Individuals could also be incorrectly placed on watchlists.[62] They might be denied government benefits or asylum if the government mistakenly determines that their social-media data contradicts information provided on their applications.

To make matters worse, law enforcement could distribute such erroneous designations to countless other public and private actors through the information-sharing environment, compounding the error in ways that are difficult to detect and eliminate.[63] Once social-media data makes its way to other entities' databases, it can be used in disadvantageous ways. This is especially likely as the information has been taken out of its original context and thus is subject to misinterpretation.[64]

---

example demonstrates law enforcement's use of social-media data generally, not the sharing of Government 2.0 data with fusion centers and the like.

58 Paul Marks, *Pentagon Sets Its Sights on Social Networking Sites*, NEW SCIENTIST, June 9, 2006, http://www.newscientist.com/article/mg19025556.200-pentagon-sets-its-sights-on-social-networking-websites.html?full=true.

59 *See supra* notes 5–7 and accompanying text (discussing the arrest of Ken Krayeske at a gubernatorial inaugural parade in Connecticut because law enforcement identified him as a potential threat due to his blog posts urging others to protest the parade, his work on Green Party campaigns, and his prior arrest at an antiwar rally).

60 *Police Pay Flying Visit to Halt 30th Birthday Party*, TIMES (London), July 17, 2009, at 27.

61 *Id.* According to the host, the police arrived in a helicopter to "stop 15 people eating burgers." *Id.*

62 *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1274–75 (2008) (discussing the misidentifications that occur because of the "No Fly" computer matching system).

63 Citron & Pasquale, *supra* note 3.

64 *See* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. (forthcoming 2010) (exploring the reputational damage inflicted when information is read online out of its original context).

Government could also use social-media data to identify sensitive information about individuals, including their group associations and sexual orientation.[65] Although individuals might deliberately avoid including this information in their profiles, the government could infer these excluded details by looking at the information imparted by others in their social network.[66] For instance, a student experiment at the Massachusetts Institute of Technology demonstrated the ease with which a person's sexual orientation can be identified by examining a person's online friends.[67] Using publicly available data from Facebook, a software program determined if a person was gay based on the gender and sexuality of that person's friends.[68] Although the student researchers had no way of checking all of their predictions, their computer program appeared accurate based on their outside knowledge.[69]

Even if individuals decline to reveal sensitive information online, agencies could employ computer algorithms that infer such information about them based on their social contacts. Agencies could identify a person's involvement in unpopular groups.[70] They could also make assumptions about individuals that are incorrect. As Katharine Strandburg explores in her insightful work, individuals might face surveillance based on their legitimate associations.[71] They might, in turn, refrain from joining certain groups and causes to avoid arousing suspicion.[72] The possibility of government surveillance might chill identity-forming and expressive activities.[73]

---

65 This concern might apply to social-network sites that permit users to become fans of government agencies if government can access the names of their fans' friends, which it appears that Facebook does. *See* Facebook Help Center, http://www.facebook.com/help/?faq=12277 (last visited Nov. 13, 2009) ("Pages cannot see the profiles of their fans. They can only see the profile photo and the name of each of their fans."); *see also* Bonneau et al., *supra* note 55.

66 Grimmelmann, *supra* note 19, at 1174.

67 Carolyn Y. Johnson, *Project 'Gaydar,'* Boston Globe, Sept. 20, 2009, at K1, *available at* http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy?mode=PF.

68 *Id.*

69 *Id.*

70 Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. Rev. 741, 759–60 (2008).

71 *Id.*

72 Individuals may find it easier to censor themselves than to de-friend an agency or executive department. Individuals also may be unaware that they could de-friend an agency.

73 Daniel J. Solove & Paul Schwartz, Information Privacy Law 525–26 (3d ed. 2009). Christopher Slobogin has argued that governmental surveillance of expressive activities, such as a speech at a park rally, can chill conduct, even though it takes place in public and is meant to be seen by others. Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 Miss. L.J. 213, 253–55 (2002). As Solobogin recog-

Furthermore, an agency's friendship with one user may have privacy consequences for others.[74] Agencies could gain access to social-network data of their contacts' contacts.[75] James Grimmelmann explains this phenomenon: "[i]f Hamlet and Gertrude are contacts, then when Gertrude accepts Claudius's contact request, she may compromise Hamlet's privacy from Claudius."[76] Such privacy spillover may result in government's use, collection, and distribution of someone's contacts' social-network information. This spreads the web of individuals whose privacy loss may lead to a false arrest, inclusion on a watchlist, or denial of government benefits.[77]

Finally, the government's use of social-media data may defy the privacy norms of Web 2.0 site users. Helen Nissenbaum's theory of contextual integrity bases privacy protections on the norms of particular contexts.[78] It assesses the kind of information that users share in certain arenas and the typical flow of information there.[79] As the next Part explores, government's use of individuals' social-media data for nonpolicy purposes would transgress the norms of information flow in social-network sites.

B. Individuals' Privacy Expectations for Government 2.0

Individuals who interact with government on social-media sites fail to appreciate their privacy risks and do not expect government to pay attention to, let alone use, their social-media data. People participate in social-network sites for *social* reasons.[80] They reveal personal

---

nized, the Supreme Court rejected a similar assertion in *Laird v. Tatum*, 408 U.S. 1 (1972). *Id.* Nonetheless, *Laird* might not foreclose a First Amendment argument against automated surveillance if social-network site users appreciated the risk, as it might present a direct "compulsion" against speech acts that the First Amendment would prohibit. *Id.*

74 *See* Grimmelmann, *supra* note 19, at 1174–75.

75 This is true if the privacy settings of government's contacts' contacts permit. Many people allow friends of friends to see their profiles. *See id.* at 1174. Indeed, some permit anyone living in their geographic area to see their profiles. On the other end, some only allow friends to do so. Research suggests that some users do not use these settings at all, *id.* at 1185, meaning that the social-network site's default privacy rules govern who can view their profile (which is often not protective of users' privacy).

76 *Id.* at 1174.

77 *See id.* at 1174–75.

78 HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 6–7 (2009); Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 138–40 (2004) [hereinafter Nissenbaum, *Privacy as Contextual Integrity*]. Daniel Solove offers a comprehensive, pragmatic theory of privacy that requires decisionmakers to balance the multitude of interests at stake in a given situation. SOLOVE, *supra* note 51, at 87–88.

79 Nissenbaum, *Privacy as Contextual Integrity*, *supra* note 78, at 138–40.

80 Grimmelmann, *supra* note 19, at 1151.

information as a means to say who they are, make new friends, and cement personal connections.[81] In doing so, people underestimate social media's privacy risks because social-network sites engender feelings of trust.[82] Seeing contacts' names and pictures conveys the notion that users are engaging in "a private space, closed to unwanted outsiders."[83]

People also have a sense that their social-network information will be kept private because they feel anonymous amidst the millions of social-network users.[84] As noted social-media researcher danah boyd explains, social-network participants "live by security through obscurity, where they assume that as long as no one cares about them, no one will come knocking."[85] They operate under the assumption that only close friends will pay close attention to their online activities.[86] Notably, social-network users fail to appreciate how many people can, and do, access their information.[87] For this reason, the possibility of future employers, government, or corporations reading their profiles seems remote.[88] As James Grimmelmann explains, the design of social-network environments effectively impairs individuals' ability to appreciate their privacy risks.[89]

---

81 *Id.*; *see also* danah boyd & Jeffrey Heer, Profiles as Conversation: Networked Identity Performance on Friendster (Jan. 2006) (unpublished manuscript), *available at* http://vis.berkeley.edu/papers/friendster_profiles/2006-Friendster-HICSS.pdf.

82 Grimmelmann, *supra* note 19, at 1160–64.

83 *Id.* at 1162.

84 *Id.* at 1161–62. My previous work *Cyber Civil Rights* explores how an online group's feeling of anonymity breeds destructive behavior online. Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. Rev. 61, 81–84 (2009).

85 danah boyd, *Social Network Sites: Public, Private, or What?*, 13 The Knowledge Tree 4, 7 (2007), http://kt.flexiblelearning.net.au/tkt2007/wp-content/uploads/2007/05/edition_13.pdf.

86 Grimmelmann, *supra* note 19, at 1161.

87 *Id.* at 1168.

88 Zeynep Tufekci, *Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites*, 28 Bull. Sci., Tech. & Soc'y 20, 31 (2008). This view is, of course, mistaken—more than half of all employers check a person's social-network activities in making interviewing and hiring decisions. A 2006 survey of 100 executive recruiters reported that 77% of recruiters used search engines to find background data on candidates and 35% eliminated a candidate based on what they uncovered. *Casting a Digital Shadow; Your Reputation Precedes You*, Brian Solis, July 17, 2009, http://www.briansolis.com/2009/07/casting-a-digital-shadow-your-reputation-precedes-you. Ralph Gross attributes people's willingness to divulge a wealth of personal information on social-network sites to a herd effect—they see others doing so and follow their lead. Ralph Gross et al., Information Revelation and Privacy in Online Social Networks (The Facebook Case) 80 (Nov. 7, 2005) (unpublished manuscript), *available at* http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf.

89 Grimmelmann, *supra* note 19, at 1162. Because Government 2.0 is so new, social scientists have yet to study individuals' privacy expectations associated with it.

The public's initial reaction to Facebook's adoption of "News Feed" seems to illustrate the point. The News Feed feature permitted users to see every act taken by all of their friends—who befriended whom, what someone wrote on another's wall, the new groups someone joined, etc.—when signing onto the site.[90] Immediately thereafter, over 700,000 users joined the *Students Against Facebook News Feed* group.[91] Although Facebook users could discover this information by visiting their friends' profiles, they opposed News Feed because it made them feel exposed, much like a person in a room with loud music would feel if someone turned the music off unexpectedly and others could hear her talking loudly.[92] Facebook users disliked how News Feed informed *all* of their friends about their activities.[93] News Feed felt like an intrusion—individuals did not expect, or want, acquaintances to check their profiles closely.[94] It also offended users' senses of control over their information, and Facebook's refusal to notify them before its adoption no doubt angered them further.[95]

This research provides insight into individuals' privacy expectations for Government 2.0. When individuals see President Barack Obama's smiling face on MySpace, they may experience feelings of trust. This is true not only because people feel that they know politicians,[96] but also because Government 2.0 sites suggest that agencies are only interested in the public's policy views. When the President tells social-network users that their views matter to him, he sends the message that government wants their policy feedback. Nothing informs individuals that government desires their social-media data for purposes other than policymaking, such as law enforcement.

Online commentary provides anecdotal support for this notion. In describing Government 2.0, a commentator wrote: "While the UK Home Office is planning to gain access to social-networking sites to snoop on its citizens, the Obama administration seeks to use the same technology to engage with voters [and] find out what they want."[97]

---

90 danah boyd, *Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence*, 14 CONVERGENCE 13, 13 (2008).

91 *Id.*

92 *Id.* at 14–15.

93 *Id.* at 15.

94 *Id.* at 13–14. In an ironic but perhaps expected turn of events, News Feed is now one of Facebook's most popular features.

95 I thank Woody Hartzog for this insightful point.

96 Lawrence M. Friedman, *The One-Way Mirror: Law, Privacy, and the Media*, 82 WASH. U. L.Q. 319, 327 (2004).

97 Anonymous, posting to eParticipation (Mar. 27, 2009, 19:54 EDT), http://eparticipation.com/content/government-agencies-use-social-networking-sites.

Moreover, social-network users may believe that the President and government agencies will not scrutinize their profiles because they expect nonintimate friends to refrain from monitoring their online activities.

To be sure, users might anticipate the possibility that a government friend might randomly notice their personal data while assessing their feedback on policy. But they would not expect government to collect, use, and distribute it systematically to law enforcement, immigration, tax, and other government authorities. Individuals share personal information on social-network sites to develop relationships, not because they want government to use it for law enforcement, taxation, and beyond. This distinction is crucial to understanding individuals' privacy expectations in Government 2.0.

Moreover, social-network sites do little to counteract individuals' mistaken impressions—they hide any mention of privacy and underscore the benefits of disclosing personal data.[98] They make privacy less salient to maximize information disclosure on their sites.[99] This may explain why individuals fail to change a social-media site's default privacy settings, which are designed to maximize the visibility of users' profiles.[100] In short, individuals may be unable to appreciate the great differences between befriending individuals and government agencies and may fail to understand the privacy risks engendered by Government 2.0.

C. Absence of Robust Legal Protections

Our current legal framework cannot adequately address these privacy concerns. In May 2009, the General Service Administration ("GSA") entered into terms-of-service agreements with social-network sites, such as MySpace, Facebook, and YouTube.[101] GSA officials explain that they had no opportunity to raise privacy concerns in

---

98 Joseph Bonneau & Soren Preibusch, The Privacy Jungle: On the Market for Data Protection in Social Networks 29–30 (2009) (unpublished manuscript), *available at* http://preibusch.de/publications/Bonneau_Preibusch__Privacy_Jungle.pdf; Bruce Schneier, *Facebook Should Compete on Privacy, Not Hide It Away*, GUARDIAN (U.K.), July 15, 2009, http://www.guardian.co.uk/technology/2009/jul/15/privacy-internet-facebook.

99 Richard Goettke & Joseph Christiana, Privacy and Online Social Networking Websites 2 (May 14, 2007) (unpublished manuscript), *available at* http://www.eecs.harvard.edu/cs199r/fp/RichJoe.pdf. Privacy information does not appear anywhere on the MySpace homepage, and although it allows users to change their settings, it is not user-friendly. *Id.* at 4. Social-network sites also discourage users from invoking restrictive privacy settings; they tell users that doing so would "make it more difficult for [them] to network with their friends." *Id.* at 2.

100 Gross et al., *supra* note 88.

101 Jeff Chester, *Federal Gov't (GSA) Refuses to Make Public Agreements with Facebook,*

their negotiations, as they had so little bargaining power vis-à-vis social-network providers who had little desire to host government sites.[102] The agreements only tackled issues that, if omitted, would have precluded the government from using social-network sites, such as indemnification, jurisdiction, intellectual property, and advertising.[103]

Federal law provides little protection from Government 2.0's privacy risks. The Privacy Act of 1974 sets the basic conditions under which the federal government collects, uses, and discloses personally identifiable information.[104] It covers "systems of records" under agency control,[105] including those administered by private companies on the government's behalf.[106] The Privacy Act, however, does not apply if the government accesses information gathered by third parties, such as commercial data brokers.[107] Because the government would retrieve individuals' network data from third-party sites in a manner akin to its retrieval of information from data-broker databases, the Privacy Act may not apply here.

Conversely, the Privacy Act would apply to social-media data incorporated into an agency's own system of records. That protection, however, may provide little help to individuals like Andy, as the Privacy Act largely exempts information used, collected, and distributed for intelligence and criminal investigations from its requirements.[108] In that case, individuals enjoy limited access, accuracy, and correction rights vis-à-vis their personal information.[109]

MySpace, etc., posting to Digital Destiny (Apr. 30, 2009, 13:38 EDT), http://www.democraticmedia.org/jcblog/?p=801; Snyder, *supra* note 28.

102 David Temoshok, Presentation at the U.S. Dep't of Homeland Security, Government 2.0: Privacy and Best Practices Workshop 157 (June 22, 2009), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_gov20_June2009_transcripts_day1.pdf.

103 *Id.* at 157–59.

104 5 U.S.C. § 552a (2006).

105 *See* Letter from Daniel J. Chenok, Chairman of Info. Sec. & Privacy Advisory Bd., to Peter Orszag, Dir. of Office of Mgmt. & Budget 11 (May 27, 2009), *available at* http://csrc.nist.gov/groups/SMA/ispab/documents/correspondence/ispab-report-may2009.pdf.

106 5 U.S.C. § 552a(m).

107 Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 595–97 (2004).

108 5 U.S.C. § 552a(k).

109 *Id.* The Privacy Act precludes agencies from collecting information that exclusively concerns individuals' First Amendment activities. That restriction does not, however, apply when the information gathered addresses more than just the person's speech acts. In turn, its protections, in practice, reach too few scenarios, as law enforcement routinely collects, uses, and distributes information relevant to far more than a person's political, religious, and other expressive activities. Andy's story demonstrates the point.

The E-Government Act of 2002 updated the Privacy Act by requiring agencies to conduct privacy impact assessments ("PIAs") when developing or procuring information technology systems that include personally identifiable information.[110] The Office of Management and Budget ("OMB") guidelines allow agencies to exempt government's use of private sector databases from the requirement to conduct PIAs when the data is not "systematically incorporate[d] into existing information system databases."[111] The E-Government Act does not apply to information generated on social-network sites if agencies decline to incorporate individuals' social-network information into their databases. If, however, an agency systematically downloads the social-media data of more than ten people, it would be obliged to produce a privacy-impact assessment report.[112] This certainly could provide considerable protection for individuals *if* the agency made clear that it would not access or use individuals' social-media data for purposes other than getting feedback on policymaking. To date, no such privacy impact assessments exist.

III. Protecting Privacy and Enhancing Civic Engagement with a One-Way Mirror Policy

This Part begins by proposing a one-way mirror policy that would permit individuals to provide feedback to government but would prevent government from using, collecting, or distributing individuals' social-media information. Then, it demonstrates how this approach can protect privacy and advance the animating principles of the Open Government initiative—governmental transparency, participation, and collaboration. It ends by countering important critiques of this approach.

A. The One-Way Mirror Proposal

Government 2.0's privacy policy should resemble a one-way mirror.[113] This approach would allow individuals to see and talk to the

---

110 E-Government Act of 2002, Pub. L. No. 107-347, § 208(b), 116 Stat. 2899, 2921.

111 Memorandum from Joshua B. Bolten, Dir. of Office of Mgmt. & Budget, to the Heads of Executive Dep'ts & Agencies, at Attachment A, Part II.E.2.f (Sept. 26, 2003), *available at* http://www.whitehouse.gov/omb/memoranda_m03-22/.

112 *Id.*

113 This Essay uses the image of a one-way mirror to help guide our thinking about the government's ability to use, collect, and distribute individuals' personal information on social-network sites. I recognize that the precise image of a mirror may not map perfectly onto every nuance of the proposal. For instance, one could argue that government's ability to obtain individuals' policy advice means that it has glanced back into individuals' views. Nonetheless, the

government but ban the government from accessing individuals' social-media data. Individuals could examine government's postings, participate in policy discussions, and share their expertise with government. At the same time, a one-way mirror policy would forbid government from using, collecting, or distributing individuals' list of contacts, wall musings, videos, photos, and other social-media data.

Facebook's fan pages resemble this approach. On Facebook, agencies and corporations generate fans whose profiles remain largely inaccessible to them. Those entities cannot view fans' profiles, photographs, videos, political and religious affiliations, or commentaries. Unfortunately, agencies and corporations can, however, view an abridged list of a Facebook fan's social contacts.[114] A one-way mirror policy would prohibit government from using or distributing that abridged list for any purpose, such as the identification of a fan's group associations.[115]

In short, this proposal creates a presumption of openness as to policy-related matters and a presumption of privacy as to individuals' social-network information. Although it would require government to adhere to this policy, it would not mandate that third parties alter their sites in any way. This solution is a legal one, not a technical one.

This proposal could be pursued in various ways. Congress could adopt legislation enshrining the one-way mirror policy into law.[116] Alternatively, the OMB could incorporate this proposal into its regulations.[117] Agencies could adopt it through policy statements or rulemakings.[118] The Department of Homeland Security ("DHS") has already taken the lead on this issue, sponsoring an agency-wide conference on the privacy implications of Government 2.0 and soliciting

---

image provides a powerful way to understand the extent to which government can use its Government 2.0 sites to obtain personal information about individuals.

114 Government could not view a fan's entire list of contacts.

115 *See* notes 63–79 and accompanying text (discussing the privacy problems associated with government's use of social-media data to infer individuals' group associations).

116 *See* Geoffrey D. Kravitz, Short Essay and Book Note, *REAL ID: The Devil You Don't Know*, 3 HARV. L. & POL'Y REV. 431, 445–46 (2009). This might be a particularly fruitful time to consider legislative action, as privacy advocates such as the Center on Democracy and Technology have devoted much time to thinking of ways to update the Privacy Act to account for networked technologies. But, as Paul Schwartz notes, such legislative change may come at too steep a price—the preemption of state privacy laws and ossification of legislation. *See* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 929–30 (2009).

117 I thank Peter Swire for his helpful comments on how we might implement the one-way mirror proposal.

118 Of course, agencies should adopt technology-neutral policies to prevent obsolescence. The policy should provide means for individuals to protest an agency's infringement of its terms.

public feedback as well.[119] DHS could draft a privacy impact assessment incorporating the one-way mirror policy, which other agencies might follow.

The one-way mirror policy would not, however, extend beyond Government 2.0 sites, i.e., ones that aim to enhance governmental participation, collaboration, and transparency as the Open Government memorandum suggests.[120] In other words, law enforcement would only be prohibited from asking agencies for their Government 2.0 friends' social-media data in cases where law enforcement identified agency friends as criminal targets.[121] The one-way mirror policy would *not* prevent law enforcement from independently investigating publicly available social-network profiles and blogs. Intelligence and law enforcement could continue their efforts to infiltrate groups suspected of criminal activity through social media.[122] This policy only aims to commit Government 2.0 to its declared purpose—garnering public insight on policy matters. As the next Section demonstrates, strong privacy rules will, in fact, advance that effort.

Although this proposal looks to law to address Government 2.0's privacy risks, social-network sites have an important role to play here as well. Sites like MySpace would be wise to adopt analogs of Facebook's fan pages, even though law would by no means require it. A particular site's adoption of fan pages for Government 2.0 efforts would surely enhance user loyalty if stories like Andy's emerge regarding government's misuse of social-media data on other sites. Facebook's competitors will ultimately follow its lead if they believe that users have a taste for such fan pages.

B. Promoting Democratic Participation and Transparency

The one-way mirror policy is crucial to producing the kind of engaged citizenry that the President imagines in his Open Government initiative. Deliberative democracy cannot thrive without strong privacy rules.[123] Privacy allows speakers and listeners to feel that they

---

119 Public Workshop Government 2.0: Privacy and Best Practices, 74 Fed. Reg. 17,876 (Dep't of Homeland Sec. Apr. 17, 2009).

120 Transparency and Open Government, 74 Fed. Reg. 4685 (Jan. 21, 2009).

121 In other words, law enforcement cannot contact the White House or other agency to view a government friend's profile (now criminal target) without legal process.

122 Law enforcement agents could continue to pursue undercover operations online so long as those operations comported with law.

123 Paul M. Schwartz, *Internet Privacy and the State*, 32 Conn. L. Rev. 815, 837 (2000).

can express themselves without reprisal.[124] It permits them to experiment with ideas.[125] Neil Richards explains that private intellectual exploration and confidential communication protect our ability to develop new beliefs and to discover new truths.[126]

Without privacy protections, democratic participation in cyberspace may be elusive.[127] Paul Schwartz cautions: "[W]ho will speak or listen when this behavior leaves finely grained data trails in a fashion that is difficult to understand or anticipate?"[128] In other words, when "widespread and secret surveillance becomes the norm, the act of speaking or listening takes on a different social meaning."[129] As Joel Reidenberg contends, a citizen's right to participate in government depends upon the right to privacy in her personal information.[130]

With strong privacy rules, individuals may be more inclined to participate in Government 2.0. They might engage with government on social-media sites and continue to watch videos in an uninhibited way. Government's online friends may be less likely to censor their postings and would feel free to support unpopular groups or causes.[131] This ensures that individuals produce more informed discourse.[132] Without a one-way mirror policy, government may lose intelligent commentary from those who appreciate Government 2.0's privacy risks.

This proposal would play an expressive role as well. Beyond its coercive power, law establishes a public set of meanings and shared understandings between the state and the public.[133] It educates the

---

124 Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1651 (1999).

125 SOLOVE, *supra* note 51, at 79–80.

126 Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 416–17 (2008).

127 *See* Schwartz, *supra* note 123, at 837.

128 Schwartz, *supra* note 124, at 1651.

129 *Id.*

130 Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 497–98 (1995).

131 Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace*, 28 CONN. L. REV. 981, 1003–19 (1996) (arguing that digital copyright-management technologies violate First Amendment freedom of speech and thought).

132 Individuals' personal information seems out of place in any discussion of the Open Government initiative. Indeed, White House spokesperson Moira Mack remarked via email "we are focused on opening government to the people (and not the other way around)." *The White House Is Now Following You on Twitter . . .*, posting to The Podium (May 4, 2009), http://internetinnovation.org/blog/entry/the-white-house-is-now-following-you-on-twitter. This suggests that the White House and executive agencies have no interest in that information.

133 Elizabeth S. Anderson & Richard H. Pildes, *Expressive Theories of Law: A General Restatement*, 148 U. PA. L. REV. 1503, 1571 (2000).

public about the government's values and commitments.[134] In that way, the one-way mirror policy would express to the public that civic participation and collaboration is its highest priority. It would communicate that government will not compromise the goals of open government in pursuit of other aims. This message seems crucial to dispel the public's distrust in government, something the Obama Administration seems eager to combat.

C. Objections

Some will suggest that individuals have no privacy in information divulged on social-network sites because they have turned the private into the public by sharing it with others. The answer, however, is not that simple. As the Supreme Court has recognized, the fact that information is divulged to others "does not mean that an individual has no interest in limiting disclosure or dissemination of the information."[135] Scholars like Lior Strahilevitz have explored the pitfalls of drawing a sharp line between what is public and what is private.[136] Their criticism is particularly apt as to social-network sites where privacy is "not simply about zeros and ones; it is about how people experience their relationship with others and with information."[137]

Others will contend that people should know better, that once you friend the President or a government agency, you have opened yourself up to persistent surveillance.[138] But as social-network re-

---

134 Cass R. Sunstein, *On the Expressive Function of Law*, 144 U. PA. L. REV. 2021, 2022 (1996); *cf.* Danielle Keats Citron, *Law's Expressive Value in Combating Cyber Gender Harassment*, 108 MICH. L. REV. 373, 404–14 (2009) (exploring law's expressive power in conveying government's commitments).

135 U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 770 (1989); *see also* Woodrow Hartzog, *Promises and Privacy: Promissory Estoppel and Confidential Disclosure in Online Communities*, 82 TEMPLE L. REV. (forthcoming 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1473561, at 8–13 (describing the disclosure of personal information in online communities and its potential consequences).

136 Consider Lior Strahilevitz's critique of the public disclosure tort, where an individual's sharing of information with a few people or, in some jurisdictions, with one other person can waive a person's expectation of privacy. Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005). As Strahilevitz explains, a restrictive view of privacy fails to capture how information actually flows in given relationships. *Id.* In other words, a binary view of privacy—where disclosure to more than one person eviscerates any privacy protection—cannot capture the fact that something may be public vis-à-vis coworkers yet private vis-à-vis the outside world. *Id.* at 940. Strahilevitz's social-network theory would instead examine the actual structure of social networks and the "extent of dissemination the plaintiff should have expected to follow his disclosure of that information" to decide whether information would have become widely known. *Id.* at 921.

137 boyd, *supra* note 90, at 18.

138 Danielle Citron, *Why We Should Care About Privacy in a Government 2.0 World*, post-

search makes clear, individuals often do not know better.[139] They may be unable to distinguish government agencies from distant acquaintances who they believe are not watching their every move.[140]

Moreover, individuals may not appreciate the vastly different consequences of friend-ing government agencies and individuals. If an acquaintance sees something damning on an individual's page and discloses it to others, the individual might suffer reputational and emotional harm for which he can pursue civil damages. If, however, a government agency collects, uses, and distributes the information, the person may end up under investigation, be refused government benefits, or appear on a government watchlist. There may be no means to redress this breach of trust. Individuals will be unable to grasp these differences and the privacy risks that Government 2.0 poses.

Some may reject any attempt to limit government's access to social-media data on the grounds that law enforcement can simply obtain the information online from individuals whose privacy settings fail to protect the data. In other words, technology has already decimated users' privacy; the genie cannot be returned to the bottle. Such technological determinism, however, should not dictate policy. Warren and Brandeis rejected that sort of thinking in their seminal article, "The Right to Privacy."[141] As Jeffrey Rosen argues, we can make "social choices about how much privacy we as a society think it is reasonable to demand."[142]

Privacy officials have asked whether we should embrace a notice regime along the lines of the Privacy Act, rather than adopting a flat ban on the use, collection, and distribution of individuals' social-media data.[143] On this view, the sole responsibility of the government is to

---

ing to Concurring Opinions (June 20, 2009, 18:05 EDT), http://www.concurringopinions.com/archives/2009/06/why-should-we-care-about-the-privacy-implications-of-government-20.html (Comment by Jake) ("If you put stuff on the Internet, expect people to read it. Most folks who put stuff on the Internet probably expect this.").

139 *See supra* notes 80–100 and accompanying text (discussing social-network users' privacy expectations).

140 It may be more likely that individuals perceive government as more akin to distant acquaintances than corporations they friend online. Individuals may be more likely to appreciate that corporations have a profit motive to use their data. We expect Coca-Cola, Amazon, or Verizon not to act in our best interests. On the other hand, we may get confused as to the government's motives and whether they are aligned with our own. Social scientists have yet to study these nuances.

141 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

142 ROSEN, *supra* note 27, at 195.

143 Martha Landesberg, Presentation at the U.S. Dep't of Homeland Security, Government 2.0: Privacy and Best Practices Workshop 121, 140–41 (June 22, 2009), *available at* http://

make sure that the social-media sites that they use have clear policies that tell consumers what could be done with their information.[144] James Grimmelmann views this option as "completely unrealistic."[145] He suggests that people tend not to appreciate notice.[146] Although Facebook's privacy policy bears a TRUSTe seal, Facebook users "don't read it, don't understand it[, and] don't rely on it."[147] Thus, even if government agencies posted a well-written privacy policy on their Government 2.0 sites, users are not likely to be protected by it.

Conclusion

Government 2.0 presents exciting opportunities and serious challenges. While social-media sites could attract more members of the public to participate in agency policymaking, especially the digital-native generation, they could erode privacy in ways that undermine the participatory goals of open government. A one-way mirror policy would ameliorate that problem, facilitating democratic discourse without engendering privacy risks.

It also has potential uses beyond Government 2.0. Companies and nonprofit organizations might consider adopting one-way mirror policies, either through technology or practice, when interacting with individuals on social-network sites. This move would permit nongovernmental entities to get the public's feedback about their services while protecting their privacy.

---

www.dhs.gov/xlibrary/assets/privacy/privacy_gov20_June2009_transcripts_day1.pdf (asking panelists whether a notice regime might suffice to address privacy concerns of Government 2.0).

144 Grimmelmann, *supra* note 19, at 1181.

145 *Id.*

146 *Id.*

147 *Id.*