Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment

Peter Swire

SOCIAL NETWORKS, PRIVACY, AND FREEDOM OF ASSOCIATION: DATA PROTECTION VS. DATA EMPOWERMENT*

PETER SWIRE**

This Article examines the tension between social networks as enablers of political mobilization (sharing information is good) and as threats to privacy (sharing information is bad). A central theme is that social networks are platforms to create associations. Linguistically, "networks" and "associations" are close synonyms; they both depend on "links" and "relationships." This Article introduces the idea that limits on such networks can deeply implicate the freedom of association.

Part I sets forth the facts of the tension between mobilization and association (Arab Spring, 2008 Obama campaign) and privacy (enforcement actions against social networks in Europe and the United States). Part II introduces the doctrinal structure in the United States for addressing the tension. If and when state action limits information sharing in social networks, individual users, political associations, and the networks themselves may have valid claims for violation of First Amendment freedom of association rights.

** C. William O'Neill Professor of Law at the Moritz College of Law of the Ohio State University and a Senior Fellow at the Center for American Progress and the Future of Privacy Forum. Special Assistant to the President for Economic Policy from 2009 to 2010, serving in the National Economic Council. Chief Counselor for Privacy in the U.S. Office of Management and Budget, from 1999 to early 2001.

Thanks for comments on an earlier draft by Neil Richards, Katherine Strandburg, and Eugene Volokh, and for comments on earlier versions of this Article presented at the Privacy Law Scholars Conference, the Telecommunications Policy Research Conference, the Governance of Social Media Conference, and the University of North Carolina Law Review Symposium titled *Social Networks and the Law*. Thanks for research assistance to Kenesa Ahmad, Scott Bent, and Lindsay Gladysz. Research funding for this Article comes from the Moritz College of Law and the Future of Privacy Forum. An earlier version of portions of this Article was published as PETER SWIRE, CTR. FOR AM. PROGRESS, SOCIAL NETWORKS, PRIVACY, AND FREEDOM OF ASSOCIATION: HOW INDIVIDUAL RIGHTS CAN BOTH ENCOURAGE AND REDUCE USES OF INFORMATION (2011), *available at* http://www.americanprogress.org/issues/2011/02/social_networks_privacy.html.

Part III applies the proposed doctrine to three concrete examples of possible state action, including "Privacy by Design" and "Do Not Track" proposals that have been featured in recent privacy debates. Part IV moves beyond doctrine to examine more generally the tension between "data empowerment," which relies on sharing of information, and "data protection," which relies on limits to such sharing. As illustrated by our eagerness to use social networks, access to the personal data of others is often a benefit to individuals, rather than the threat assumed by the data protection approach. These benefits notably include our right to associate, to reach out to people to effect political change and realize ourselves as individuals. The old paradigm for debates about personal information was rights vs. utility; the discussion here shows that data empowerment increasingly makes the debate one of rights vs. rights.

INTRODUCTION

At Internet conferences that I have attended in the past few years, there have often been panels highlighting how social networks mobilize political change. Speakers on these panels often discussed the 2011 "Arab Spring," including the "Facebook Revolution" in Egypt that resulted in the overthrow of President Mubarak.[1] They also praised the 2008 Obama campaign, whose outreach and mobilization was led by a co-founder of Facebook.[2] In these panels, a key feature of social networks was their ability to foster political association at the grassroots level—sharing information among activists empowered them.[3]

Meanwhile, speakers from another panel often spoke about the privacy problems caused by social networks. In these discussions, sharing of information was a problem, and not a positive feature of political mobilization.[4] In the period that social networks have grown to prominence, government agencies have issued a flurry of privacy

1. *See, e.g.*, Pieter, *Facebook Revolution in Egypt: Pictures and Cartoons*, REFACE.ME (Feb. 2, 2011, 8:05 PM), http://reface.me/news/facebook-revolution-egypt/ (collecting pictures and cartoons about the Facebook Revolution); *The Facebook Revolution: The Role of New Media in Egypt and the Middle East*, HERITAGE FOUND. (Feb. 17, 2011), http://www.heritage.org/events/2011/02/facebook-revolution (discussing, on a panel, the role of social media in the Egyptian uprising and its effect on the Middle East). For background discussion of the role of Facebook and social networks in the Arab Spring, see Malcolm Gladwell & Clay Shirky, *Response, From Innovation to Revolution, Do Social Media Make Protests Possible? An Absence of Evidence*, 90 FOREIGN AFF. 153, 153–54 (2011), *available at* http://www.foreignaffairs.com/articles/67325/malcolm-gladwell-and-clay-shirky/from-innovation-to-revolution.

2. *See infra* Part I.A (discussing the 2008 Obama campaign).

3. *See* Pieter, *supra* note 1; *The Facebook Revolution*, *supra* note 1.

4. *MENA Beyond Stereotypes: Technology of Good and Evil Before, During and After Revolutions*, 21ST ANN. CONF. COMPUTERS, FREEDOM & PRIVACY (June 15, 2011), http://www.cfp.org/2011/wiki/index.php/Video#MENA_Beyond_Stereotypes:_Technology_of_Good_and_Evil_Before.2C_During_and_After_Revolutions (panelists deconstructed the role of social media in the local and foreign policy of the Middle East and North Africa, pre- and post-revolutions).

policy initiatives, such as the Obama Administration's call for Internet privacy legislation,[5] the Federal Trade Commission's report on online privacy,[6] and the European Union's proposed revision to the Data Protection Directive.[7] Major social networking companies have also been the target of high-profile enforcement actions in the United States and Europe.[8]

Notably lacking from these conferences was an integrated understanding of when the sharing of personal information was good (Arab Spring) and when it was bad (privacy problems). This Article tries to help with that integration. To do so, the analysis here highlights the profound connection between social networking and freedom of association. A basic tension exists between information sharing, which can promote the freedom of association, and limits on information sharing, notably for privacy protection. Although many writers have written about one or the other, my research has not found any analysis of how the two fit together—how freedom of association interacts with privacy protection.[9]

---

5. For the Administration's initial approach to privacy policy, set forth in a report by the Department of Commerce Internet Policy Task Force, see generally INTERNET POLICY TASK FORCE, DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (2010), *available at* http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf. For further comments, see generally Peter Swire, *Why the Federal Government Should Have a Privacy Policy Office*, 10 J. TELECOMM. & HIGH TECH. L. (forthcoming 2012) (calling for a federal privacy office).

6. *See generally* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS, PRELIMINARY FTC STAFF REPORT (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (proposing a framework for consumer privacy). Note that an earlier version of this Article was submitted as a comment to that Federal Trade Commission preliminary staff report.

7. *See generally* EUROPEAN COMM'N, PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA (2011), *available at* http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf (proposing a new data protection regulation).

8. *See infra* Part I.B (discussing enforcement actions).

9. I have conducted a number of searches such as: "freedom of association" & "social network"; and "freedom of association" & "Facebook." With the exception of the academic work along the lines of that written by Katherine Strandburg, discussed *infra*, my research has turned up no analysis of how freedom of association fits together with privacy for social networks. The lack of discussion is even more striking because of the considerable attention given to the role of social networks in empowering freedom of association as a political check on authoritarian regimes. *See, e.g.*, *The Facebook Revolution*, *supra* note 1 (discussing the Egyptian revolution). The power of social media in this way is a theme of the U.S. State Department's project on Internet Freedom. *See generally Internet Freedom*, U.S. DEP'T OF STATE, http://www.state.gov/e/eb/cip

At the most basic level, linguistically, "networks" and "associations" are close synonyms. They both depend on "links" and "relationships." If there is a tool for lots and lots of networking, then it also is a tool for how we make lots and lots of associations. In this respect, social networks such as Facebook and LinkedIn are simply the latest and strongest associational tools for online group activity, building on e-mail and the web itself.[10] Indeed, the importance of the Internet to modern political and other group activity is highlighted in a 2011 study by the Pew Foundation, which finds that a majority of online users in the United States have been invited through the Internet to join a group, and a full thirty-eight percent have used the Internet to invite others to join a group.[11]

I stumbled into this tension between association and privacy due to a happenstance of work history. I have long worked and written on privacy and related information technology issues, including as the Chief Counselor for Privacy under President Clinton. Then, during the Obama transition, I was asked to be counsel to the New Media team. These were the people who had done such a good job at grassroots organizing during the campaign. During the transition, the team was building New Media tools for the transition website and an overhaul of whitehouse.gov.[12]

/netfreedom/ (last visited May 6, 2012) (describing the Internet Freedom program at the U.S. State Department). For an insightful article discussing the interaction between political shifts and the impact technology has upon them, see generally Clay Shirky, *The Political Power of Social Media: Technology, the Public Sphere, and Political Change*, 90 FOREIGN AFF. 28 (2011).

10. The focus of the discussion here is on social networks, which have emerged very recently, where the name "social network" shows an especially strong relationship to freedom of association. The analysis, however, does not turn on whether a service is called a "social network" or not; instead, the ways that associations are formed online will be crucial to the relevance of freedom of association.

11. LEE RAINIE, KRISTEN PURCELL & AARON SMITH, PEW RESEARCH CTR., PEW INTERNET & AM. LIFE PROJECT, THE SOCIAL SIDE OF THE INTERNET 24–25 (2011), *available at* http://www.pewinternet.org/~/media//Files/Reports/2011/PIP_Social_Side_of_the_Internet.pdf.

12. For a set of my materials about Web 2.0 and the federal government, see PETER SWIRE, CTR. FOR AM. PROGRESS, SIX NEW MEDIA CHALLENGES: LEGAL AND POLICY CONSIDERATIONS FOR FEDERAL USE OF WEB 2.0 TECHNOLOGY *passim* (2009), *available at* http://www.americanprogress.org/issues/2009/06/web2.0_challenges.html. I first publicly discussed the importance of "data empowerment," including the freedom of association, at the Computers, Freedom, and Privacy conference in June 2009. *See* Saul Hansell, *The Obama Administration's Silence on Privacy*, N.Y. TIMES (June 2, 2009, 12:28 PM), http://bits.blogs.nytimes.com/2009/06/02/the-obama-adminstrations-silence-on-privacy/. I spoke in greater detail about data empowerment at the Organization for Economic Cooperation and Development Conference on data privacy guidelines, in Jerusalem, in October 2010. *See Swire's Speeches and Public Appearances 2010*, PETERSWIRE.NET, http://www

My own engagement in privacy protection is consistent with the view of a large majority of people, who, when asked whether they support privacy protection, at least at a general level say they do.[13] Many people believe that "they"—meaning big corporations or law enforcement—will grab our personal data and put "us" at risk. The Obama New Media folks, by contrast, often had a different intuition. They saw personal information as something that "we" use. Modern grassroots organizing seeks to engage interested people and go viral, to galvanize one energetic individual who then gets his or her friends and contacts excited.[14]

In this New Media world, "we" the personally motivated use social networks, text messages, and other outreach tools to tell our friends and associates about the campaign and remind them to vote. We may reach out to people we don't know or barely know but who have a shared interest—the same college club, rock band, religious group, or whatever. In this way, "our" energy and commitment can achieve scale and effectiveness. The tools provide "data empowerment," meaning ordinary people can do things with personal data that only large organizations used to be able to do.[15]

To explain the interaction between data sharing and limits on data sharing, this Article has four parts. Part I sets forth the facts of the tension between association (share data) and privacy (limit sharing) in social networks. Part II introduces the doctrinal structure in the United States for addressing this tension. If and when state action limits information sharing in social networks, individual users, political associations, and the networks themselves may have valid claims for violation of First Amendment freedom of association rights. Part III applies the proposed doctrine to three concrete examples of possible state action, including "Privacy by Design" and "Do Not Track" proposals that have been featured in recent privacy debates. Part IV moves beyond doctrine to examine more generally the tension between "data empowerment," which relies on sharing of

---

.peterswire.net/psspeeches2010.htm (last visited May 6, 2012).

13. For additional materials on the history of public support for information privacy protection, see *Public Opinion on Privacy*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/survey/#polls (last visited May 6, 2012).

14. *See* Jacqueline D. Lipton, *From Domain Names to Video Games: The Rise of the Internet in Presidential Politics*, 86 DENV. U. L. REV. 693, 693 (2009) (analyzing how the 2008 Obama campaign "converged with the features of this new Internet").

15. To read more about the democratization of digital campaigns and networks, see generally Robert Faris & Bruce Etling, *Madison and the Smart Mob: The Promise and Limitations of the Internet for Democracy*, FLETCHER F. WORLD AFF., Summer 2008, at 65.

information, and "data protection," which relies on limits to such sharing. As illustrated by our eagerness to use social networks, access to the personal data of others is often a benefit to individuals, rather than the threat assumed by the data protection approach. These benefits notably include our right to associate, to reach out to people to effect political change and realize ourselves as individuals. The old paradigm for debates about personal information was rights vs. utility; the discussion here shows that data empowerment increasingly makes the debate one of rights vs. rights.

I. THE TENSION BETWEEN ASSOCIATION AND PRIVACY IN SOCIAL NETWORKS

This Part lays out basic factual background for how social networks are platforms to create associations, thus supporting greater data flows. It then discusses the extensive critiques of the privacy practices of social networks, supporting limits on data flows. Later parts analyze the conflict, as a doctrinal matter and more broadly.

A. Social Networks as Platforms To Create Associations

It is intuitive to most readers that social networks are powerful creators and facilitators of associations. Networks such as Facebook serve as platforms for users to do things jointly. To bolster this intuition, this Part examines the linguistic connection between "networks" and "associations," points out that networks are used for professional as well as personal reasons, and looks briefly at how the networks are platforms generally to create associations. The emphasis is on how social networks serve as platforms for what freedom of association doctrine calls "expressive" associations, such as political groups, religious organizations, and other groups in civil society.[16]

Linguistically, as mentioned in the Introduction, "networks" and "associations" are close synonyms. They both depend on "links" and "relationships." "Social networks" link together people in their social capacity—their associations with other people. The linguistic convergence of "social networks" and "associations of people" offers a simple and powerful argument that legal rules about social networks will implicate legal rules about freedom of association.

For individuals, some of the associations are primarily social, such as when we share only with personal "friends" on Facebook or

16. The categories of "expressive" and "intimate" association were set forth in *Roberts v. U.S. Jaycees*, 468 U.S. 609, 617–18 (1984), discussed in the text accompanying notes 65–72.

our "circles" of friends on Google+. On the other hand, social networks often also have a professional component. LinkedIn is a social network that described itself, as of late 2011, as the "world's largest professional network on the Internet with more than 135 million members in over 200 countries and territories."[17] A person's "circles" on Google+ can be based on professional affiliations,[18] and a 2011 study found that eighteen- to twenty-nine-year-olds had an average of sixteen professional colleagues among their Facebook "friends."[19] Individuals often use social networks to achieve their professional goals; for individuals engaged in politics or nonprofit work, this means that they are using social networks in the service of these sorts of expressive activities.

Along with these efforts by individuals to foster association, associations themselves are making social networks an increasingly prominent part of their overall strategy. Charities came early to social media; a 2009 study found that ninety-seven percent of charities in the United States already used some form of social media.[20] Nonprofit organizations "are using social media tools to connect with the communities they serve. They are attracting donations, volunteers, media coverage, and employees."[21] The emphasis is on engagement, in contrast to traditional one-way communications from the organization to members or possible donors: "Online communities are becoming the center of member engagement strategies at both nonprofit and for-profit membership organizations."[22] The

17. *About Us*, LINKEDIN, http://press.linkedin.com/about (last visited May 6, 2012). At the end of the day of its initial public offering, LinkedIn was worth $8.9 billion. Stu Woo, Lynn Cowan & Pui-Wing Tam, *LinkedIn IPO Soars, Feeding Web Boom*, WALL ST. J., May 20, 2011, at A1, *available at* http://online.wsj.com/article/SB10001424052748704816604576333132239509622.html.

18. GOOGLE+, *New Ways of Sharing the Right Things with the Right People* https://www.google.com/intl/en-US/+/learnmore/index.html#circles (last visited May 6, 2012).

19. Jorgen Sundberg, *INFOGRAPHIC: How Generation Y Use Facebook for Professional Networking*, THE UNDERCOVER RECRUITER (Jan. 9, 2012), http://theundercoverrecruiter.com/content/infographic-how-generation-y-use-facebook-professional-networking.

20. Nora Ganim Barnes, *Social Media Usage Now Ubiquitous Among US Top Charities, Ahead of All Other Sectors*, U. MASS. DARTMOUTH, CENTER MARKETING RES., http://www.umassd.edu/cmr/studiesandresearch/socialmediatopcharities/ (last visited May 6, 2012).

21. Amy Southerland, *Why Every Nonprofit Needs a Social Media Strategy*, SPURSPECTIVES (Jan. 15, 2009), http://spurspectives.com/why-every-nonprofit-needs-a-social-media-strategy/. Researchers have found large increases in fundraising from such approaches. Anthony Sicola, *Using Social Media Increases Fundraising by 40%*, NETWITSTHINKTANK (May 12, 2011), http://www.netwitsthinktank.com/friends-asking-friends/using-social-media-increases-fundraising-by-40-percent.htm.

22. Joshua Paul, *Most Popular Member Engagement Posts of 2011*, SOCIOUS (Dec. 27,

importance of the Internet to modern associational activity is highlighted in the previously mentioned 2011 study by the Pew Foundation, which finds that a majority of online users in the United States have been invited through the Internet to join a group, and a full thirty-eight percent have used the Internet to invite others to join a group.[23] The Pew study also found different patterns of association for the online and offline worlds. For instance, online groups appear to have greater entry and exit—people both join and leave groups more often—so that the rules for forming groups, and recruiting new members, are likely more important to group formation and retention than in the offline world.[24]

Consistent with the idea that social networks are general-purpose platforms for associational activity,[25] there has been strong recognition of the importance of such networks to politics, both globally and in the United States. The political protests in Egypt that led to the ouster of President Mubarak were dubbed the "Facebook Revolution,"[26] and the empowerment offered by social media has been credited more broadly for Arab Spring movements in other countries.[27] In the United States, Facebook co-founder Chris Hughes joined the Obama campaign in 2007 as its "online organizing guru."[28] The centrality of social networking to the campaign was widely recognized, such as in this *New York Times* profile of Hughes: "The campaign's new-media strategy, inspired by popular social networks like MySpace and Facebook, has revolutionized the use of the Web as a political tool, helping the candidate raise more than two million donations of less than $200 each and swiftly mobilize hundreds of thousands of supporters before various primaries."[29] The lessons from

---

2011, 8:11 AM), http://info.socious.com/bid/51173/Most-Popular-Member-Engagement-Posts-of-2011.

23. RAINIE ET AL., *supra* note 11, at 24–25.

24. *See id.* at 34 ("Compared with group members who go online but do not use these services, Twitter and social networking site users are significantly more likely to say that they discovered some of their groups online, that the internet helps them participate in a greater number of groups, and that they spend more time participating in group activities thanks to the internet.").

25. *See infra* Part II.A (discussing the role of social networks as "platforms").

26. *See, e.g.*, Pieter, *supra* note 1; *The Facebook Revolution*, *supra* note 1.

27. For more background discussion of the role of Facebook and social networks in the Arab Spring, see Gladwell & Shirky, *supra* note 1, at 153–54. *See generally* Shirky, *supra* note 9 (discussing how social media has served as a tool for nearly all of the world's political movements).

28. Brian Stelter, *The Facebooker Who Friended Obama*, N.Y. TIMES, July 7, 2008, at C1, *available at* http://www.nytimes.com/2008/07/07/technology/07hughes.html.

29. *Id.*; *see also* David Carr, *How Obama Tapped into Social Networks' Power*, N.Y. TIMES (Nov. 9, 2008), http://www.nytimes.com/2008/11/10/business/media/10carr.html

the Obama campaign have spread across the political spectrum, playing an important role in the rise of the Tea Party[30] and the 2010 campaign of Republican Scott Brown to win the Massachusetts Senate seat previously held by Ted Kennedy.[31] Experts believe social networks will play a large and growing role for the 2012 election and beyond.[32]

In assessing the convergence of associations with social networks, it is of course true that a tremendous amount of social networking activity consists of playing games, linking to cute or funny videos, posting pictures of children and pets, and all the other stuff of social life. Politics and other expressive associational activity may be only a modest fraction of all social networking. On the other hand, the discussion here has shown that social networking is an increasingly vital aspect of how political and other expressive associations work. As discussed below, legal rules that restrict or govern social networks will thus be subject to scrutiny under the First Amendment rules that apply to expressive associations.

B. Social Networks as Privacy Threat

Social networks share personal information. From their inception, therefore, there have been concerns that they create privacy problems.[33] Facebook, as the largest social network, has

---

(analyzing the importance of social networks to Obama's election).

30. Corbin Hiar, *How the Tea Party Utilized Digital Media To Gain Power*, PBS.ORG (Oct. 28, 2010), http://www.pbs.org/mediashift/2010/10/how-the-tea-party-utilized-digital-media-to-gain-power301.html.

31. Sophia Yan, *How Scott Brown's Social-Media Juggernaut Won Massachusetts*, TIME (Feb. 4, 2010), http://www.time.com/time/nation/article/0,8599,1960378,00.html.

32. *See, e.g.*, Matt Hamblen, *Social Networking Mobile Campaigns To Rule 2012 US Presidential Race*, COMPUTERWORLDUK (Jan. 3, 2012), http://www.computerworlduk.com/news/applications/3327402/social-networking-mobile-campaigns-rule-2012-us-presidential-race/ (emphasizing role of mobile devices that access social networks); Jay Samit, *Three Ways Social Media Will Make or Break 2012 Election Campaigns*, ADAGEDIGITAL (June 23, 2011), http://adage.com/article/digitalnext/social-media-make-break-2012-election-campaigns/228367/ (explaining reasons for growing importance of social networks).

33. For a very early discussion dating from when Facebook served only select college campuses, see generally Harvey Jones & José Hiram Soltren, Facebook: Threats to Privacy (Dec. 14, 2005) (unpublished student paper, Massachusetts Institute of Technology), *available at* http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf; *see also Facebook Privacy*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/facebook/ (last visited May 6, 2012) (showing history of privacy criticisms of Facebook). As one defense of many social network data practices, it is helpful to consider that individuals voluntarily post information to the networks, so the people who post do disseminate this data with a significant degree of "opt in" consent. That defense is significant but incomplete, because users may not realize how data will be

drawn the most attention. In a 2010 interview before a large audience, Facebook CEO Mark Zuckerberg literally broke out in a sweat when asked repeated questions about privacy.[34] Symbolically as well, privacy is an issue that can make social network executives sweat.

These privacy concerns are arising at a time when privacy is once again becoming a more prominent policy issue. Privacy was a relatively prominent issue in the United States in the late 1990s, when the Internet bubble occurred, the European Directive on Data Protection went into effect, and the United States promulgated rules for medical, financial, and children's online privacy protection.[35] After the attacks of September 11, 2001, Congress passed the USA-PATRIOT Act, and we entered a period where anti-terrorism and security concerns outweighed privacy concerns.[36] As I have written elsewhere, a confluence of factors, including the rise of social networks, is once again making privacy a more prominent issue in the United States.[37] Other factors include: location and other privacy issues that accompany the skyrocketing use of mobile devices;[38] revelations in the press about intensive data collection online for behavioral advertising;[39] the growth of cloud computing, with a bigger range of personal data held remotely;[40] proposed revisions in the European Union to the Data Protection Directive (which has not been changed since 1995);[41] and new privacy legislation enacted by

---

used, and they may post pictures or other information about other people, without those people's consent.

34. Bianca Bosker, *Mark Zuckerberg Sweats in Privacy Hot Seat at All Things Digital*, HUFFINGTON POST (June 3, 2010, 9:36 PM), http://www.huffingtonpost.com/2010/06/03/mark-zuckerberg-all-thing_n_598834.html.

35. *See* Peter P. Swire, *Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy*, 54 HASTINGS L.J. 847, 860–64 (2003) (describing a period of heavy privacy activity in late 1990s).

36. *See* Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 VILL. L. REV. 951, 953–59 (2006) (discussing privacy policy in the wake of the September 11 attacks).

37. Peter Swire, *Why Privacy Legislation Is Hot Now*, THE HILL (June 23, 2011, 7:50 PM), http://thehill.com/component/content/article/72-opinion/168267-why-privacy-legislation-is-hot-now.

38. *See Location Based Services Forum*, FCC (June 28, 2011), http://www.fcc.gov/events/location-based-services-forum (multi-stakeholder public education forum on location-based services in response to the rapid growth of those services).

39. *See, e.g.*, *See What They Know*, WALL ST. J., http://blogs.wsj.com/wtk/ (last visited May 6, 2012) (analyzing tracking files installed on users' computers by fifty popular websites).

40. NICOLE A. OZER & CHRIS CONLEY, ACLU OF N. CAL., CLOUD COMPUTING: STORM WARNING FOR PRIVACY? 2 (2010), *available at* http://dotrights.org/sites/default/files/Cloud%20Computing%20Issue%20Paper.pdf.

41. *See* EUROPEAN COMM'N, *supra* note 7, at 2.

important trade partners, such as Mexico and India.[42]

Both the Federal Trade Commission ("FTC"), an independent agency, and the Obama Administration have launched major privacy initiatives. The FTC released a privacy report late in 2010 that received the most attention for its discussion of a possible Do Not Track approach to online behavioral advertising.[43] The U.S. Department of Commerce released a "green paper" on privacy shortly thereafter,[44] and the Obama Administration has become the first to explicitly support comprehensive privacy legislation in the United States.[45] As of the date of writing in early 2012, follow-on reports by both the FTC and the Department of Commerce are expected soon.

New attention to enforcement has accompanied this privacy policy debate. In 2010 and 2011, the FTC entered into privacy consent decrees with social media company Twitter,[46] Google (operator of the Google+ social network),[47] and Facebook itself.[48] The FTC consent

---

42. *See* Ley de Transparencia y Acceso a la Información Pública del Distrito Federal [LTAIPDF][Transparency and Access to Public Information Law for the Federal District], *as amended*, Diario Oficial de la Federación [DO], 7 de Mayo de 2010 (Mex.); Graham Greenleaf, *India's U-Turns on Data Privacy*, *in* PRIVACY LAWS & BUS. INT'L REP., ISSUES 110–14 (2011), *reprinted in* USNW LAW RESEARCH PAPER No. 42 (2011), *available at* http://ssrn.com/abstract=1964013.

43. *See* FED. TRADE COMM'N, *supra* note 6, at 63–69.

44. *See generally* INTERNET POLICY TASK FORCE, *supra* note 5 (setting forth the Obama Administration's approach to online privacy, recommending articulation of core principles followed by subsequent discussion of issues as they become apparent). For further comments, see Swire, *supra* note 5 (calling for a federal privacy office).

45. *See The State of Online Consumer Privacy: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 112th Cong. 5–13 (2011) (prepared statement of Lawrence E. Strickling, Assistant Secretary for Communications and Information, National Telecommunications and Information Administration, U.S. Department of Commerce), *available at* http://commerce.senate.gov/public/?a=Files.Serve&File_id=9e90bd89-dcb9-42c3-a8b7-e59c126b8fad.

46. Press Release, Fed. Trade Comm'n, Twitter Settles Charges That It Failed To Protect Consumers' Personal Information; Company Will Establish Independently Audited Information Security Program (June 24, 2010), *available at* http://www.ftc.gov/opa/2010/06/twitter.shtm (announcing that the FTC had entered into a consent agreement with Twitter resolving privacy and security complaints about Twitter's security system and unauthorized access to its users' non-public information).

47. Press Release, Fed. Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), *available at* http://www.ftc.gov/opa/2011/03/google.shtm (announcing that the FTC had entered into a consent agreement with Google resolving privacy complaints about the company's Buzz social networking service).

48. Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges That It Deceived Consumers by Failing To Keep Privacy Promises (Nov. 29, 2011), http://ftc.gov/opa/2011/11/privacysettlement.shtm (announcing that the FTC had entered into a consent agreement with Facebook resolving complaints that Facebook made deceptive

decree highlighted concerns that Facebook had changed its data policies over time without clear notice to users and did not provide users with a way to opt out from having their data processed when privacy practices changed.[49] The Google and Facebook consent decrees included the first agreements by companies to establish a "comprehensive privacy program," which in part requires that, for the next twenty years, the companies have independent third-party audits every two years to assess their privacy practices.[50] In Europe, there have been additional complaints about social networks and privacy. An Austrian law student examined data about his own use of Facebook and filed a complaint with twenty-two separate allegations of violation of European data protection law.[51] The Data Protection Commissioner for the German State of Schleswig-Holstein ordered state institutions to shut down their Facebook pages and remove the "Like" button from their websites, or face fines.[52] In late 2011, the Data Protection Commissioner in Ireland, where Facebook has its largest European operations, issued a major report that criticized a number of the company's privacy practices, and the company promised to make a number of changes.[53]

In conclusion on privacy, the short discussion here shows substantial public concerns about privacy and social networks, growing policy discussions about possible regulatory limits, and increased enforcement actions. We next turn to the implications of government privacy actions for the legal doctrine of freedom of association.

II. SOCIAL NETWORKS UNDER U.S. LAW OF FREEDOM OF ASSOCIATION

The discussion in Part I showed that social networks both provide a platform for creating desirable associations and create privacy risks that have drawn public and government attention.

---

representations to consumers regarding Facebook's privacy practices).

49. *Id.*

50. *See supra* notes 47–49 (describing the FTC consent decrees with Google and Facebook).

51. *See* David Cohen, *Facebook Privacy Policies Challenged by Austrian Law Student*, ALLFACEBOOK (Oct. 26, 2011, 4:45 PM), http://www.allfacebook.com/facebook-privacy-policies-2011-10.

52. Sarah Kessler, *German State Bans Facebook's "Like,"* MASHABLE (Aug. 19, 2011), http://mashable.com/2011/08/19/germany-like-button/.

53. DATA PROT. COMM'R, FACEBOOK IRELAND LTD: REPORT OF AUDIT 5–20 (2011), *available at* http://dataprotection.ie/documents/facebook%20report/final%20report/report.pdf.

Facebook, Google, and Twitter have already faced privacy enforcement actions in the United States, and the Irish Data Protection Commissioner has concluded a major privacy audit of Facebook.[54] Although privacy laws tailored to social networks have not been enacted to date in the United States, my experience with privacy debates in other emerging sectors leads me to conclude that such state and federal laws quite likely will be proposed going forward. This Part discusses how the First Amendment freedom of association doctrine would intersect with privacy laws in general. Then, Part III applies the doctrine to specific possible examples of privacy law.

My research has found no previous analysis of how freedom of association doctrine would apply to privacy laws in the social networking context. In my view, the strongest constitutional arguments will apply to state action that limits the ability of individuals, political campaigns, and others to learn about and reach out to others in order to create and deepen associations. This Article will analyze three possible government actions. The first would be a state or federal law that prohibits all use of social networking sites for political campaigns. I consider such a law unlikely to be proposed, but it serves a useful role here as a thought experiment for how government regulation could affect freedom of association. The second and third examples draw on prominent features of the FTC's privacy policy efforts. One would be a Privacy by Design rule that requires default settings to share as little personal data as possible. The other would be a Do Not Track requirement that applies to the activities of political campaigns, charities, or other nonprofit activities. These three examples are intended as useful tools for considering, in concrete settings, how courts might analyze the tradeoffs between privacy and freedom of association. I undertake this analysis not with the aim of exalting one goal over the other; instead, the analysis arises from my genuine puzzlement (which I believe is widely shared) about how to reconcile the two goals.

Under U.S. law, a preliminary issue is that the First Amendment applies only to "state action." State action exists, for instance, where a statute, regulation, or enforcement action creates a privacy limit on how personal information is used. By contrast, an individual generally has no First Amendment rights with respect to decisions by a private company.[55] Thus, the First Amendment itself does not apply to

54. *See supra* Part I.B.

55. There are minor exceptions, such as in a "company town" where the local coal

decisions by social networking companies. The analysis here may nonetheless be helpful as social networks decide how to build and configure their systems. Non-state actors are free to consider both privacy and freedom of association as they operate their systems, and those decisions can be informed by the same normative arguments that apply to state actors.

This Part discusses the current doctrine of freedom of association. It then explains the main categories of free speech doctrine, shows how speech doctrine could apply to association, and contends that using speech doctrine in this way would be a good idea. It concludes with a discussion of how freedom of association doctrine can support privacy and limits on data flows, rather than supporting such data flows.

A. The Current Freedom of Association Framework

Association is central to a vast array of human affairs.[56] Americans belong to diverse civic, social, and political associations, and the importance of these associations has long been recognized. Alexis de Tocqueville, regarded by some as "the philosophical father of the right of association,"[57] observed that "Americans of all ages, all conditions, all minds constantly unite."[58] According to de Tocqueville, there is nothing that deserves more attention than "the intellectual and moral associations of America."[59]

Yet, despite the prevalence and importance of association, the freedom of association has received far less legal attention than other freedoms, such as the freedom of speech. According to some, "the value and limits of free association in the United States have not received the attention they deserve."[60] Accordingly, freedom of association doctrine is incomplete as it applies to the new domain of

---

mine owns all the property and limits speech in the town. For an in-depth treatment, see generally DAWN C. NUNZIATO, VIRTUAL FREEDOM: NET NEUTRALITY AND FREE SPEECH IN THE INTERNET AGE (2009) (exploring implications that most speech over the Internet is controlled by private actors, rather than in public spaces).

56. *See* Roberts v. U.S. Jaycees, 468 U.S. 609, 622 (1984) ("An individual's freedom to speak, to worship, and to petition the government for the redress of grievances could not be vigorously protected from interference by the State unless a correlative freedom to engage in group effort toward those ends were not also guaranteed.").

57. David Cole, *Hanging with the Wrong Crowd: Of Gangs, Terrorists, and the Right of Association*, 1999 SUP. CT. REV. 203, 229.

58. ALEXIS DE TOCQUEVILLE, DEMOCRACY IN AMERICA 489 (Harvey C. Mansfield & Delba Winthrop eds. & trans., Univ. of Chi. Press 2000) (1840).

59. *Id.* at 492.

60. Amy Gutmann, *Freedom of Association: An Introductory Essay*, *in* FREEDOM OF ASSOCIATION 3, 3 (Amy Gutmann ed., 1998).

social networks, which are platforms for creating and expanding associations.

The freedom of association was not explicitly recognized by the Supreme Court until 1958, when the Court held that the State of Alabama could not compel the NAACP to disclose its membership list in *NAACP v. Alabama ex rel. Patterson*.[61] In so holding, the Court asserted that "[i]t is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech."[62] The Court said: "[S]tate action which may have the effect of curtailing the freedom to associate is subject to the closest scrutiny."[63] Thus, the state must point to a compelling interest to justify a law that burdens the freedom to associate.[64]

The Court later developed and clarified the freedom of association framework in *Roberts v. United States Jaycees*.[65] The Court in *Roberts* stated that there are two forms of constitutionally protected association: intimate association and expressive association.[66] Intimate association "receives protection as a fundamental element of personal liberty."[67] Expressive association, on the other hand, is protected "as an indispensable means of preserving other individual liberties," such as "speech, assembly, petition for the redress of grievances, and the exercise of religion."[68]

According to the Court in *Roberts*, "the nature and degree of constitutional protection afforded freedom of association may vary depending on the extent to which one or the other aspect of the constitutionally protected liberty is at stake in a given case."[69] The Court articulated only one standard of review, however, even while acknowledging the possibility of more. Under this standard, "[i]nfringements on [the freedom to associate for expressive

61. 357 U.S. 449, 466 (1958).

62. *Id.* at 460.

63. *Id.* at 460–61.

64. *Id.* at 463 ("Such a . . . 'subordinating interest of the State must be compelling . . . .' " (quoting Sweezy v. New Hampshire, 354 U.S. 234, 265 (1957) (Frankfurter, J., concurring))).

65. 468 U.S. 609 (1984).

66. *Id.* at 617–18.

67. *Id.* at 618.

68. *Id.* This Article deals primarily with expressive association, as legally mandated privacy protections on social networks such as Facebook are less likely to interfere with the ability to form intimate associations with people such as family members and close friends.

69. *Id.*

purposes] may be justified by regulations adopted to serve compelling state interests, unrelated to the suppression of ideas, that cannot be achieved through means significantly less restrictive of associational freedoms."[70] Thus, the Court's doctrinal statements to date apply a strict scrutiny standard for freedom of association doctrine that tracks the strict scrutiny standard for content-based restrictions on speech.[71] While this approach may have been workable in the past, the development of social networks as platforms for association poses new challenges for the doctrine of free association. If courts continue to apply only strict scrutiny, then a wide range of possible state actions would likely be considered unconstitutional.[72] If courts do not apply strict scrutiny, then new doctrinal structures will be needed for freedom of association. As shown by the relatively recent and sparse Supreme Court precedent, freedom of association law is relatively undeveloped—the dichotomy of strict scrutiny or no scrutiny is not well suited to the clash of strong state interests that we see for social networks.

B. Three Categories of Free Speech Doctrine

This Article proposes that freedom of speech doctrine offers a good model for a more nuanced doctrine of freedom of association.[73] The Supreme Court has created three relevant categories for free speech analysis: content-based rules; rules affecting commercial speech; and time, place, and manner restrictions. The remainder of this Part outlines the Court's basic freedom of speech framework and

---

70. *Id.* at 623.

71. Compare the standard of review applied in *Roberts* to that applied in *United States v. Playboy Entertainment Group*, 529 U.S. 803, 813 (2000) ("If a statute regulates speech based on its content, it must be narrowly tailored to promote a compelling Government interest.").

72. *See* Cole, *supra* note 57, at 203–04 ("As a matter of democratic theory, the right of association is something we cannot live without; but as a matter of social governance, the right, if uncontained, is something we cannot live with.").

73. According to Justice O'Connor's concurring opinion in *Roberts*, the distinction between content-based and content-neutral restrictions already applies to the freedom of association. *Roberts*, 468 U.S. at 634 (O'Connor, J., concurring) ("Reasonable, content-neutral state regulation of the time, place, and manner of an organization's relations with its members or with the State can pass constitutional muster, but only if the regulation is 'narrowly drawn' to serve a 'sufficiently strong, subordinating interest' 'without unnecessarily interfering with First Amendment freedoms.'" (quoting Vill. of Schaumburg v. Citizens for a Better Env't, 444 U.S. 620, 636–37 (1980))). However, the Court in *Village of Schaumburg v. Citizens for a Better Environment* never mentioned the phrase "freedom of association," and research has not found an explicit judicial holding that less than strict scrutiny applies to the freedom of association. *See* Vill. of Schaumburg v. Citizens for a Better Env't, 444 U.S. 620 *passim* (1980).

then explains why it makes sense to apply this framework to the freedom of association.

First, the strictest scrutiny of state action occurs for content-based regulation: "If a statute regulates speech based on its content, it must be narrowly tailored to promote a compelling Government interest."[74] In addition, "[i]f a less restrictive alternative would serve the Government's purpose, the legislature must use that alternative."[75] Commercial speech is subject to a lower level of scrutiny. Commercial speech is defined as "expression related solely to the economic interests of the speaker and its audience."[76] The Court has stated: "The First Amendment's concern for commercial speech is based on the informational function of advertising."[77] Proposing a commercial relationship "furthers the societal interest in the fullest possible dissemination of information."[78] The often-followed test from *Central Hudson Gas & Electric Corp. v. Public Service Commission*[79] provides:

> The State must assert a substantial interest to be achieved by restrictions on commercial speech. Moreover, the regulatory technique must be in proportion to that interest. The limitation on expression must be designed carefully to achieve the State's goal. Compliance with this requirement may be measured by two criteria. First, the restriction must directly advance the state interest involved; the regulation may not be sustained if it provides only ineffective or remote support for the government's purpose. Second, if the governmental interest could be served as well by a more limited restriction on commercial speech, the excessive restrictions cannot survive.[80]

The third doctrinal category concerns content-neutral restrictions on the time, place, and manner of speech.[81] Such restrictions are valid if they "are narrowly tailored to serve a significant governmental interest" and "leave open ample alternative channels for

74. *Playboy*, 529 U.S. at 813.

75. *Id.*

76. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 561 (1980).

77. *Id.* at 563.

78. *Id.* at 561–62.

79. 447 U.S. 557 (1980).

80. *Id.* at 564.

81. Clark v. Cmty. for Creative Non-Violence, 468 U.S. 288, 293 (1984) ("Expression, whether oral or written or symbolized by conduct, is subject to reasonable time, place, or manner restrictions.").

communication of the information."[82] As with restrictions on commercial speech, the "narrow tailoring" element of this analysis requires only a reasonable fit between legislative ends and means—it is not a least-restrictive-means requirement.[83]

There are a number of justifications for these analytical distinctions. The distinction between commercial and noncommercial speech is justified in large part by the fact that commercial transactions occur in "an area traditionally subject to government regulation."[84] Moreover, "[t]o require a parity of constitutional protection for commercial and noncommercial speech alike could invite dilution, simply by a leveling process, of the force of the [First] Amendment's guarantee with respect to the latter kind of speech."[85] The Court has also stated that commercial speech holds a "subordinate position in the scale of First Amendment values,"[86] acknowledging by implication that political speech sits atop this scale of values.[87]

The distinction between content-based restrictions and content-neutral time, place, and manner restrictions is based on two justifications. First is the idea that "[a]ll speech, regardless of its content, must be treated the same by the government. To allow the government to target particular views or subjects permits the government to greatly distort the marketplace of ideas."[88] Because time, place, and manner restrictions pose less danger of government censorship, there is less need for close judicial scrutiny. Second, "strict scrutiny of these restrictions would hamstring the government in its ability to pursue legitimate objectives."[89]

---

82. *Id.*

83. Bd. of Trs. of State Univ. of N.Y. v. Fox, 492 U.S. 469, 477–78 (1989) ("We have refrained from imposing a least-restrictive-means requirement . . . in assessing the validity of so-called time, place, and manner restrictions.").

84. Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978).

85. *Id.*

86. *Id.*

87. *See, e.g.*, Morse v. Frederick, 551 U.S. 393, 403 (2007) ("Political speech, of course, is 'at the core of what the First Amendment is designed to protect.' " (quoting Virginia v. Black, 538 U.S. 343, 365 (2003) (plurality opinion))); *see also* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 269 (1964) (stating that the First Amendment "was fashioned to assure unfettered interchange of ideas for the bringing about of political and social changes desired by the people" (quoting Roth v. United States, 354 U.S. 476, 484 (1957))).

88. ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 934 (3d ed. 2006).

89. Kimberly K. Smith, Comment, *Zoning Adult Entertainment: A Reassessment of* Renton, 79 CALIF. L. REV. 119, 122 (1991).

C. *How the Speech Framework Could Apply to Association*

In the context of speech, a restriction is content-based if it prohibits speech because of the subject matter or viewpoint expressed in the speech.[90] For example, the Court in *United States v. Playboy Entertainment Group, Inc.*[91] held that a law that exclusively regulated sexual speech was a content-based restriction.[92] On the other hand, a restriction is content-neutral "if it applies to all speech regardless of the message."[93] In *Turner Broadcasting System, Inc. v. FCC*,[94] for example, the Court held that a law requiring companies to carry local broadcasting stations was content-neutral because the companies had to carry all stations, no matter the content of their programming.[95]

The concept of "content-based," and the accompanying strict scrutiny, fits nicely with the freedom of association, particularly expressive association.[96] A restriction on the freedom of expressive association is clearly content-based if it is targeted at the subject matter or viewpoint expressed by the association. A related insight concerns membership in an organization. The *Roberts* majority said: "There can be no clearer example of an intrusion into the internal structure or affairs of an association than a regulation that forces the group to accept members it does not desire."[97] Justice O'Connor, in her concurrence in that case, stated that "an association engaged exclusively in protected expression enjoys First Amendment protection of both the content of its message and the choice of its members."[98] An organization's speech and its ability to choose its members thus are core associational rights subject to strict scrutiny protection.

The concept of "commercial association" can apply for organizations themselves and for the social network platforms that facilitate association formation and maintenance.[99] A wide range of organizations use social networks to recruit new members and do

90. *See* Hill v. Colorado, 530 U.S. 703, 722–23 (2000); Consol. Edison Co. of N.Y. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 530, 538 (1980).

91. 529 U.S. 803 (2000).

92. *Id.* at 811.

93. CHEMERINSKY, *supra* note 88, at 936.

94. 512 U.S. 622 (1994).

95. *Id.* at 643.

96. *See supra* Part II.A (distinguishing intimate and expressive association).

97. Roberts v. U.S. Jaycees, 468 U.S. 609, 623 (1984). Forced membership implicates freedom of speech as well: "Such a regulation may impair the ability of the original members to express only those views that brought them together." *Id.*

98. *Id.* at 633 (O'Connor, J., concurring).

99. My research has not found any previous discussion of "commercial association."

associational activities with members. Some of these organizations are exclusively or primarily commercial in nature, such as a consumer product company that forms a "club" for individuals who buy the product regularly or engage in sponsored activities. Individuals in the club may get discounts on products or special invitations to events. A famous early example was the "Mickey Mouse Club" of Walt Disney, but innumerable companies now encourage social network users to "like" the company or its products, and participate in sponsored activities. These purely commercial activities seem closely analogous to advertising and other commercial speech, and they would seem to be good candidates to be upheld if they meet intermediate scrutiny along the lines of the *Central Hudson* test. Other organizations, however, are political and charitable rather than primarily commercial. For these associations, the *Central Hudson* test would not seem to apply, given that "commercial" in the speech context concerns "expression related solely to the economic interests of the speaker and its audience."[100] As discussed below, associational rights of these political and charitable organizations may be subject to stricter scrutiny than for commercial associations.

A novel issue raised by social networks is how the networks themselves may be able to assert commercial associational rights in the face of state action. One theme of this Article is that social networks should be understood as platforms for creating associations. I use "platform" here the way the term is used in the information technology industry, where software developers and others outside of the company build their applications and businesses on the platform.[101] Facebook and other social networks clearly qualify as platforms—game providers and numerous other businesses have created business models that rely entirely or largely on Facebook.[102] As discussed above, political parties and nonprofits already rely heavily on social networks for member recruitment and engagement. An interesting issue, then, is the extent to which Facebook and other social networking sites could themselves challenge state action as a

100. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557, 561 (1980).

101. *See* Scott Cleland, *Why Google's Not a "Platform,"* FORBES (Oct. 19, 2011, 11:39 AM), http://www.forbes.com/sites/scottcleland/2011/10/19/why-googles-not-a-platform (defining "platform" and calling Facebook a "social platform").

102. Facebook itself offers the "Facebook Platform" to enable this use of its site. *Facebook Platform*, FACEBOOK, http://www.facebook.com/platform (last visited May 6, 2012). For discussion, see Nick O'Neill, *The Facebook Platform, Three Years Later*, ALLFACEBOOK (May 25, 2010, 1:05 AM), http://www.allfacebook.com/the-facebook-platform-three-years-later-2010-05.

restriction on their right of commercial association. The Supreme Court recognized the value of commercial speech under the First Amendment due to "the informational function of advertising."[103] The analogous argument is that social networks should have the right of commercial association, including making information available about possible group members, due to what one might call the "informational function of networking." The social networks achieve their commercial goals by facilitating associations among people, so Facebook or other social networks would appear to have a basis for challenging regulations that restrict association, much as advertisers can challenge regulations that restrict speech.

Along with regulation of association based on content and regulation of commercial association, there can be time, place, and manner restrictions on association. Classic examples of time, place, and manner restrictions on speech are limits on the hours where a sound truck or parade can go through a residential neighborhood.[104] The issue for social networks is whether certain state actions can be upheld under the more deferential standard used for time, place, and manner restrictions—narrow tailoring to a significant state interest, with ample alternative means for associating. As discussed below, the doctrine for time, place, and manner restrictions on associations may turn out to be a crucial issue for the permissibility of possible privacy limits as applied to social networks. This is especially true for limits on the associational rights of political and charitable organizations, which may be subject to strict scrutiny if there is not a time, place, and manner justification for a state action.

D. Why the Speech Framework Should Apply to Association

The Court's freedom of speech framework clearly *could* apply to the freedom of association, but why *should* it?[105] There are at least

103. *Cent. Hudson*, 447 U.S. at 563.

104. Kovacs v. Cooper, 336 U.S. 77, 87 (1949) (upholding regulation of sound trucks); Cox v. New Hampshire, 312 U.S. 569, 576 (1941) (upholding regulation of parades); *see also* C. Edwin Baker, *Unreasoned Reasonableness: Mandatory Parade Permits and Time, Place, and Manner Regulations*, 78 NW. U. L. REV. 937, 937 (1983) (arguing that the reasonableness aspect of time, place, and manner restrictions is neither necessary or desirable); Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. CHI. L. REV. 46, 67, 98 (1987) (discussing regulations on soundtrucks and parades as time, place, and manner restrictions).

105. For alternative suggestions as to how the freedom of association doctrine should develop, see generally Cole, *supra* note 57 (proposing an approach to protection of association that focuses on the right of symbolic expression); John D. Inazu, *The Unsettling "Well-Settled" Law of Freedom of Association*, 43 CONN. L. REV. 149 (2010)

two reasons why the speech framework should apply to the freedom of expressive association: (1) the freedom of expressive association derives from the freedom of speech, and (2) the Court has already applied this framework to the freedom of association *sub silentio*.

1. The Freedom of Expressive Association Derives from the Freedom of Speech

Explaining the basis for constitutionally protecting the freedom of association, the Court in *Roberts* stated, "[t]he Constitution guarantees freedom of association of this kind as an indispensible means of preserving other individual liberties."[106] These "other individual liberties" include speech, religion, and petition for the redress of grievances.[107] Thus, the freedom of association is to some degree an extension or an instrumentality of the freedom of speech.

According to the Court, the freedom of association derives from more than one individual liberty. However, in developing the doctrine of free association, it makes the most sense to borrow from freedom of speech because speech is more similar to association than any of the other liberties. First, speech and association are equally ubiquitous. Second, "all of the arguments traditionally advanced to justify protecting speech also apply to association."[108] Third, the specific type of association being protected is "expressive" association, so freedom of speech principles are directly implicated. Thus, because the freedom of association is seen by the Court as a means to preserving other liberties such as the freedom of speech, and because the freedoms of association and speech are so similar, it is justifiable to apply freedom of speech principles to the freedom of association.

2. The Court Has Applied the Freedom of Speech Framework to Association *Sub Silentio*

While the Court has never explicitly stated that the distinction between content-based and content-neutral or between commercial and noncommercial applies to the freedom of association, some of the Court's past decisions appear to imply as much.[109] For instance, the

(urging that the Court abandon the distinction of intimate and expressive association and instead turn to the right of assembly).

106. Roberts v. U.S. Jaycees, 468 U.S. 609, 618 (1984).

107. *Id.*

108. Cole, *supra* note 57, at 228.

109. *See, e.g.*, Vill. of Schaumburg v. Citizens for a Better Env't, 444 U.S. 620, 636–37 (1980); *Cox*, 312 U.S. at 574–76.

Court in *Cox v. New Hampshire*[110] upheld the enforcement of a state statute that prohibited parades or processions on public streets without a special license.[111] According to the Court in *Cox*, "[c]ivil liberties, as guaranteed by the Constitution, imply the existence of an organized society maintaining public order without which liberty itself would be lost in the excesses of unrestrained abuses."[112] *Cox* was decided before the freedom of association was explicitly announced by the Court, but nonetheless, the Court's deferential analysis is telling. The *Cox* Court's analysis would have to be repudiated or substantially modified if content-neutral time, place, and manner restrictions on association are properly subject to strict scrutiny.[113]

In different contexts than social networks, the Court has also implicitly applied a lower level of scrutiny to commercial associations. Commercial associations are common, such as when an employer recruits an employee, a company solicits a customer, or two people partner up in business. These sorts of association are often expressive, such as when advertising gives reasons for customers to come to an event or when an employee decides to work for an organization due to its mission. Yet, the Court has not applied strict scrutiny to restrictions on activities such as this. As Justice O'Connor stated: "The Constitution does not guarantee a right to choose employees, customers, suppliers, or those with whom one engages in simple commercial transactions, without restraint from the State. A shopkeeper has no constitutional right to deal only with persons of one sex."[114]

The Court has long applied a lower level of scrutiny to content-neutral restrictions on association and restrictions on commercial association—it just hasn't done so explicitly. Importing freedom of speech doctrine into the context of free association would simply make explicit what has long been implicit in the Court's First Amendment jurisprudence.

E. When Freedom of Association Protects Privacy

The discussion thus far has focused on ways that social networks

110. 312 U.S. 569 (1941).

111. *Id.* at 576.

112. *Id.* at 574.

113. *See id.* at 576 ("If a municipality has authority to control the use of its public streets for parades or processions, as it undoubtedly has, it cannot be denied authority to give consideration, without unfair discrimination, to time, place and manner in relation to the other proper uses of the streets.").

114. Roberts v. U.S. Jaycees, 468 U.S. 609, 634 (1984) (O'Connor, J., concurring).

can enhance association by creating platforms for more effective recruitment and maintenance of membership. This discussion has highlighted how greater information flows can foster association. Previous work, however, has emphasized instead how the freedom of association is advanced by protecting privacy and restricting information flows.

This line of argument has been developed most fully by New York University School of Law Professor Katherine Strandburg.[115] Her analysis begins with a famous case from the civil rights era, discussed earlier, when the State of Alabama tried to require the NAACP to reveal the identity of its members.[116] The NAACP objected to this request. In 1958, the Supreme Court unanimously agreed with the NAACP, finding that freedom of association would be chilled if the group were forced by the state to reveal its member list.[117] The *NAACP* case reminds us of the potentially overwhelming power of the state to harass unpopular groups and force supporters to be subject to bad publicity, social pressure, and possible prosecution. As was shown in 2010 when Iran shut down protesters who used social media and other online sites, governments can trample on freedom of association by making intrusive demands on such sites for personal information.[118] Similar concerns existed in Egypt until President Mubarak stepped down.[119] Strandburg builds on the *NAACP* case to argue that freedom of association rights should be considered along with Fourth Amendment rights in assessing when it is lawful for the government to compel companies to turn over personal information.

As a matter of legal doctrine, Strandburg's excellent analysis is quite distinct from the tradeoffs between privacy rights and freedom of association discussed in this Article. She addresses the freedom of association of those who do not wish their associations revealed, in the context of shielding individuals against intrusive government surveillance. The focus here, by contrast, is on how social networks can offer platforms to associate, such as for political campaigns, nonprofits, and politically engaged individuals. Strandburg's

115. *See* Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 741 (2008).

116. *Id.* at 786.

117. NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 466 (1958).

118. *See* Ian Black, *How Iran Is Filtering Out Dissent*, GUARDIAN (June 30, 2009), http://www.guardian.co.uk/technology/2009/jun/30/internet-censorship-iran.

119. *See* David Stanford, *Egypt Faces New Media Censorship*, AL JAZEERA (Aug. 7, 2008), http://www.aljazeera.com/focus/2008/08/200887919526179 74.html.

discussion and mine are entirely consistent at the doctrinal level. They actually reinforce each other, because both use the same Supreme Court precedents to underscore the importance of freedom of association.

Although there is no conflict at the level of doctrine, there is a specific way that Strandburg's analysis modifies the discussion thus far about how U.S. law addresses both privacy and freedom of association. The added wrinkle, this Article suggests, is to recognize that the type of freedom of association that Strandburg emphasizes can be a state interest that supports the case for privacy regulation. Recall that judges faced with a First Amendment claim must identify a state interest to uphold state action—a "compelling" interest under strict scrutiny, a "substantial" interest for commercial limits, and a "significant" interest for time, place, and manner analysis.[120] In previous free speech challenges to privacy laws, the stated government interest was privacy itself.[121] Strandburg's approach helps us to see another candidate for the state interest—limits on data use can protect the freedom of association of those who do not want their associations revealed.[122]

III. CONSTITUTIONAL ANALYSIS OF POSSIBLE SOCIAL NETWORKING PRIVACY RULES

With these legal precepts in mind, we are in a position to see the structure of how a United States judge would assess the interaction of privacy and freedom of association for state action affecting social networks. This Part analyzes three types of possible privacy rules introduced above: limits on the use of social networks for political campaigns; rules requiring Privacy by Design in social networks; and Do Not Track rules for social networks.

A. Limits on Use of Social Networks for Political Campaigns

The first hypothetical, not proposed so far as I know, is a state or federal law that prohibits the use of social networking sites for political campaigns. Such a law is not content-neutral; on its face, the

120. *See supra* notes 73–89 and accompanying text.

121. *See* U.S. West, Inc. v. FCC, 182 F.3d 1224, 1236 (10th Cir. 1999); Individual Reference Servs. Grp., Inc. v. FTC, 145 F. Supp. 2d 6, 18 (D.D.C. 2001).

122. A related legal point is that the "narrowly tailored" requirement could be affected by having two compelling state interests. Where both privacy and the Strandburg aspect of freedom of association are the state interests, then state action may have greater flexibility, because limits on data use could be tailored to meet either one of the state interests.

law applies more restrictively to political campaigns. Strict scrutiny would almost certainly apply. Such a law has a substantial and direct effect on individuals' freedom of association, cutting off a widely used channel for mobilizing politically. The law would almost certainly be struck down.

Such a law is unlikely to be enacted for any number of reasons, including because it so clearly and explicitly restricts political speech and association.[123] The simple hypothetical, however, is a useful thought experiment for two reasons: it underscores the point that freedom of association can be implicated by limits on social networks, and it illustrates the way that content-based limits on association would be analyzed.[124] In defending such a law, the state could try to argue that privacy is a compelling state interest. The law, for instance, could protect privacy by reducing unwanted and intrusive messages. Also, along the lines of *NAACP*, it could reduce the ability of third parties to gain access to sensitive information about a person's political beliefs. Whether in this setting protecting privacy and the *NAACP* version of freedom of association would qualify as "compelling," a court would almost certainly find that the interests could be achieved through a less restrictive alternative than a flat prohibition on using social networks for political association.

B. "Privacy by Design" Limits on Social Networks

The second hypothetical builds on the FTC's call for Privacy by Design, that is, for building privacy protection into the design and default settings of a product or service.[125] Suppose that Privacy by

123. Another reason such a law is unlikely to pass is that incumbent legislators are unlikely to cut off one of their own effective channels for communicating at low cost with potential voters. *See* Ari Shapiro, *Facebook Has Powerful Friends; Will Users Suffer?*, NPR (May 30, 2011), http://www.npr.org/2011/05/30/135783156/facebook-has-powerful-friends-will-users-suffer.

124. The hypothetical used here is especially subject to constitutional challenge because of its explicit rules restricting political speech and association. Less far-fetched laws that address content might include laws regulating dating sites for adults—First Amendment litigation has prominently involved "adult" commercial activity. *See, e.g.*, City of Renton v. Playtime Theatres, Inc., 475 U.S. 41, 43 (1986) (upholding zoning ordinance for adult theaters against First Amendment challenge). More nuanced legal discussion would be needed, but "association" in the form of dating has been a prominent feature of social networking sites. *See* Michael J. Rosenfeld & Reuben J. Thomas, *Searching for a Mate: The Rise of the Internet as a Social Intermediary*, AM. SOC. REV. (forthcoming 2012), *available at* http://www.stanford.edu/~mrosenfe/Rosenfeld_How_Couples_Meet_Working_Paper.pdf. Laws limiting dating sites might be struck down as violating the freedom of intimate association.

125. The FTC's preliminary report on online privacy supports greater use of Privacy by Design. *See* FED. TRADE COMM'N, *supra* note 6, at v.

Design were required by a U.S. law or regulation, or in a state enforcement action. For instance, a social networking site could be required to set the default to the more protective option for a new product or service. One example could be the setting on some sites that allows a "friend" to see either all of your friends or only those friends that you have in common. Showing only the friends you have in common is more privacy protective, and correspondingly makes it more difficult for your friends to learn about who shares your interests and belongs to the same associations.

The discussion above indicated that, to date, the Court has applied strict scrutiny to freedom of association claims.[126] If, as suggested above, the free speech doctrines are used to create a more nuanced set of tests for freedom of association, then three doctrinal tests in addition to strict scrutiny might apply: "commercial association," "time, place, and manner restrictions on association," and the more vaguely defined "heightened scrutiny" stated by the Court in 2011 in *Sorrell v. IMS Health, Inc.*[127] First, a challenge by the social network could be a test case for whether to have a "commercial association" doctrine. The social network would argue that it meets its commercial goals by facilitating associations among people and that the regulation disrupts the informational function of networking, much as limits on commercial speech disrupt the informational function of advertising. If a court then applied a *Central Hudson* approach, the state would argue that the regulation directly advanced a substantial state interest, and the interest could not be achieved with a more limited restriction on association. A court would then conduct a factual inquiry. The state interest in promoting privacy and *NAACP*-type association would be weighed against the social network's claim of disruption of the platform for achieving commercial association. Similarly, commercial participants on the social network could challenge the law as restricting their "commercial association" rights to reach out to possible members.

Next, the court might apply a standard for time, place, and manner restrictions on association. Following free speech doctrine, such restrictions would be upheld if there is narrow tailoring to a significant state interest, with ample alternative means of associating. The time, place, and manner test is generally understood as easier for the state to meet than the commercial speech standard. The argument for applying a time, place, and manner standard is that the Privacy by

126. *See supra* Part II.A (discussing strict scrutiny).
127. 131 S. Ct. 2653, 2664–68 (2011).

Design limit allows a wide range of association to occur on the network, just not in a certain "manner"—the manner that poses an undue risk to privacy. Social networks provide "ample alternative means" of associating, and the privacy rule thus could be upheld so long as it is narrowly tailored to the state interest in protecting privacy.

A court might also decide to follow *Sorrell v. IMS Health, Inc.*, where the Supreme Court stated that "heightened scrutiny" applied, but declined to announce what form of scrutiny applied to a state law that sought to limit the sale of information about doctors' prescribing habits.[128] Some language in *Sorrell* can be read broadly, to suggest that privacy laws will be difficult to defend in the face of heightened scrutiny under the First Amendment.[129] My own view is that, for multiple reasons, the broad language in *Sorrell* will not (or at least should not) be understood as a major change in the application of First Amendment rules to privacy laws, primarily because the law at issue there involved data about commercial actors rather than private individuals.[130]

In examining the multiple doctrines that might apply to a Privacy by Design law, the principle goal here is to elucidate the possible logic for applying each doctrine, rather than attempting to declare the correct answer for all situations. At least for most commercial social networking, I do not believe that the strict scrutiny standard properly weighs the multiple state interests, and so I advocate for a more nuanced approach. Possible legislation here quite possibly merits a time, place, and manner analysis, so long as ample alternative methods exist for associating. The concept of "commercial association" also seems potentially quite useful to highlight reasons for protecting a platform of association under freedom of association doctrine. Then, under any of the doctrines, a court would assess the facts supporting the state interests supporting the law as well as possible negative effects on protected First Amendment association.

---

128. *Id.*

129. *See generally, e.g.*, Thomas R. Julin, Sorrell v. IMS Health *May Doom Federal Do Not Track Acts*, 10 PRIVACY & SECURITY L. REP. 1262 (2011), *available at* http://www.hunton.com/files/Publication/86a85a32-bb2d-4176-8683-7e985093cb2f/Presentation/PublicationAttachment/be10be7a-b942-494d-8463-865e505fd7f6/Julin_BNA_Federal_Do_Not_Track_Acts.pdf (lead trial counsel for IMS Health, Inc. in *Sorrell v. IMS Health, Inc.* stating that the case has broad implications for limits on privacy laws).

130. Peter Swire, Professor of Law, Moritz Coll. of Law, Ohio State Univ., Economics and Privacy If Data = Speech, Presentation at the University of Colorado Law School Conference: The Economics of Privacy (Dec. 2, 2011), *available at* http://www.peterswire.net/psspeeches2011.htm.

When presenting earlier versions of this Article at conferences, some listeners objected at this point of the analysis. These listeners accepted the *NAACP v. Alabama*-type right of association, and saw how state action implementing Privacy by Design would protect individuals from the sort of intrusion that the state was imposing on NAACP members. They argued, however, that the "outside" political parties, nonprofits, or others did not have a right under freedom of association doctrine to find potential recruits by using social networks. In considering this objection, I have been able to imagine two versions. First, the objectors may factually believe that there are "ample alternative means for association," so that the state action would survive scrutiny under the time, place, and manner test. To me, this is a factual question that is suitable for development in the record of litigation in an as-applied challenge to a state action. As Facebook and other social networks form an increasingly important and effective portion of associational activity, strict default standards against sharing of associational interests may face constitutional difficulties.

A second version of the objection, however, would go to doctrine rather than facts. As I understand the objection, some have the view that the First Amendment protects "negative" rights, such as the right of the NAACP to shield its members from intrusion by the State of Alabama. By contrast, this view would doubt whether there is similar protection for "positive" rights, such as the right of a political party to use a social network to reach out to potential new members and motivate those new members to participate more actively.[131] My own (somewhat tentative) view is that the First Amendment would apply to these positive rights. The analogy would be to a state law that prohibited a shopping mall from permitting political parties and nonprofits from setting up tables in the mall or approaching shoppers to proselytize. In this example, the shopping mall is like the social network. State action limiting the right of the shopping mall to authorize political activity would seem clearly subject to First Amendment challenge, and the same would seem to apply to state action limiting association through social networks.

C. "Do Not Track" Limits on Social Networks

A third hypothetical involves the application of a Do Not Track

131. *See generally* David P. Currie, *Positive and Negative Constitutional Rights*, 53 U. CHI. L. REV. 864, 864–65 (1986) (discussing the distinction between positive and negative rights).

requirement to the activities of political campaigns, charities, and other nonprofit activities.[132] This hypothetical adds to the discussion thus far by focusing attention on when and whether any exception should apply for political parties and other expressive associations. Previously, federal law has made important exemptions in privacy rules for such associations. For instance, the "Do Not Call" list prohibits telemarketing calls to individuals who have chosen to get on the list, but permits political parties and nonprofit organizations to contact numbers on the Do Not Call list.[133] A direct mail opt-out was upheld by the Supreme Court as constitutional, on the understanding that the limits on mailing did not apply to political or religious organizations.[134] My view is that the exceptions have been important to the courts' acceptance of limits on contacting individuals, and that the risk of such laws being struck down would be significantly higher if they applied to political and other expressive associations. The importance of such exceptions to maintaining a law's constitutionality is heightened by the Court's recent campaign finance jurisprudence, such as *Citizens United v. FEC*,[135] which reiterated the First Amendment rights of corporations to support political candidates.

The analysis of a Do Not Track law would depend on how "tracking" is defined. Some proponents of the Do Not Track approach wish to have bans on collection of information about a person's surfing habits; others, however, envision Do Not Track as primarily a limit on display of targeted online advertisements.[136] The

132. In its report, the FTC staff supports a Do Not Track approach to behavioral advertising, which it defines as "a more uniform and comprehensive consumer choice mechanism for online behavioral advertising." FED. TRADE COMM'N, *supra* note 6, at 66. The staff's report does not discuss the extent to which any such Do Not Track mechanism would apply to having choice in connection with advertising by political campaigns, charities, and other nonprofit activities.

133. *See* Mainstream Mktg. Servs., Inc. v. FTC, 358 F.3d 1228, 1234 (10th Cir. 2004) (upholding Do Not Call regulation, containing exceptions for political organizations and other nonprofits, against First Amendment challenge).

134. *See* Rowan v. U.S. Post Office Dep't, 397 U.S. 728, 741–42 (1970) (Brennan, J., concurring) (expressing concern that an otherwise-constitutional opt-out from receiving mail would violate the First Amendment if the rule applied to political or religious materials).

135. 130 S. Ct. 876 (2010). For one set of commentaries on *Citizens United*, see generally Symposium, *An Intersection of Laws:* Citizens United v. FEC, 27 GA. ST. U. L. REV. 887 (2011).

136. At an April 2010 conference on Do Not Track hosted by the Princeton University Center for Information Technology Policy, participants seemed evenly split between those who thought limits should apply only to display or also to collection. *See W3C Workshop on Web Tracking and User Privacy, Workshop Report*, WORLDWIDE WEB CONSORTIUM (W3C) (Sept. 11, 2011, 4:55 PM), http://www.w3.org/2011/track-privacy/report. For the efforts of the World Wide Web Consortium to develop standards for Do Not Track, see

analogy to Do Not Call is stronger if Do Not Track applies only to display of targeted advertisements: just as political and other expressive organizations are allowed to make calls to those on the Do Not Call list, arguably they should be allowed to display targeted ads to those on the Do Not Track list. Administration of such an exception would seem manageable—exempted organizations could send targeted ads even to those who signed up for Do Not Track. Failure to have an exception for political and other expressive associations thus, in my view, could be a significant additional risk that any such state action would be found to violate the First Amendment.

Other proponents of Do Not Track, including FTC Commissioner Julie Brill, would place limits on the collection of information about a person's surfing habits.[137] This sort of collection limitation would overlap with the Privacy by Design discussion above—the law would adjust what sort of data is available for viewing. It would seem fairly difficult to administer an exception—how would one securely build a system that collected data for the excepted organizations, but blocked collection for commercial organizations? The discussion of Privacy by Design showed significant uncertainty about what doctrinal standard would apply. Building an exception into the basic collection systems, however, seems difficult to manage, and having a standard collection system (without the exception for associations) seems more likely to survive constitutional scrutiny than a limit on targeted advertising by associations.

IV. RIGHTS VS. RIGHTS: DATA EMPOWERMENT VS. DATA PROTECTION

The discussion of U.S. legal doctrine has shown strong arguments on the side of limiting flows of data to protect both personal privacy and the associational memberships that Strandburg emphasizes. It has

Thomas Roessler, *Do Not Track at W3C*, W3C BLOG (Feb. 24, 2011, 5:00 PM), http://www.w3.org/QA/2011/02/do_not_track_at_w3c.html.

137. In a speech at an International Association of Privacy Professionals conference on "The FTC and Consumer Privacy Protection," Commissioner Brill discussed the newly published FTC Green Paper and explicitly supported the adoption of a Do Not Track mechanism. *See* Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at the International Association of Privacy Professionals Second Annual Conference: The FTC and Consumer Privacy Protection (Dec. 7, 2010), *available at* www.ftc.gov/speeches/brill/101207iapp.pdf. At a linguistic level, this position seems a more accurate match with the term "Do Not Track," because it would limit tracking (collection of data) and not just display of targeted ads.

also shown strong arguments on the side of enabling flows of data, notably to empower freedom of association. This Part generalizes that discussion. It first analyzes data protection, showing how rights to privacy are used in the United States and especially European law, in contrast to utilitarian arguments that often favor data flows. This Part then turns to what I call "data empowerment," focusing on a broader change in the relationship of data and individuals. As illustrated by our eagerness to use social networks, access to the personal data of others is often a benefit to individuals, rather than the threat assumed by the data protection approach. These benefits notably include our right to associate, to reach out to people to effect political change and realize ourselves as individuals. The old paradigm for debates about personal information was rights vs. utility; the discussion here shows that data empowerment increasingly makes the debate one of rights vs. rights.

A. Data Protection

To understand the data protection approach, the first step is to analyze rights to privacy under U.S. and E.U. law. Arguments based on a right to privacy contrast with utilitarian arguments, which often favor uses of personal information.

1. Rights to Privacy

The "right to privacy" is a notoriously complicated term.[138] To begin, the discussion here does not refer to the right to privacy that has been so controversial in American law, such as in cases about abortion and contraception. That version of the right to privacy is about *decisional privacy*, and the limits on the state's ability to regulate intimate decisions about one's body.[139] Instead, the discussion here is about *informational* or *data privacy*, and especially about the rules that a government might set for how personal information is collected and used.

The scope of data privacy rights varies, both geographically and in the extent to which the rights are considered part of a constitution. In the European Union, fundamental rights in information privacy are recognized under the European Convention on Human Rights[140]

138. For one analysis of the varying definitions of right to privacy, see generally Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002).

139. The distinction between decisional and data privacy is discussed further in DANIEL SOLOVE & PAUL SCHWARTZ, INFORMATION PRIVACY LAW 1–2 (3d ed. 2009).

140. European Convention for the Protection of Human Rights and Fundamental

and implemented in the 1995 Data Protection Directive.[141] A human rights approach to privacy is also embodied in the widely cited 1980 privacy guidelines from the Organization for Economic Cooperation and Development.[142]

In the United States, the Fourth Amendment protects a person's home and papers against unreasonable searches.[143] U.S. courts have found no general constitutional right, however, for individuals in the realm of data privacy.[144] Statutes and case law do provide important individual rights. Individuals have a set of rights under the Health Insurance Portability and Accountability Act's[145] medical privacy rule,[146] for instance, and common law judges have upheld some

---

Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 221, *available at* http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf (entered into force Sept. 3, 1953).

141. Council Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT [hereinafter European Directive on Personal Data]. The similarities and differences between the E.U. and U.S. data protection regulation are discussed at length in PETER SWIRE & ROBERT LITAN, NONE OF YOUR BUSINESS 76–89 (1998). *See also Internet Privacy: The Impact and Burden of EU Regulation: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Energy & Commerce Comm.*, 112th Cong. (2011) (statement of Peter Swire, Moritz College of Law of the Ohio State University and the Center for American Progress), *available at* http://republicans.energycommerce.house.gov/Media/file/Hearings/CMT/091511/Swire.pdf (comparing and contrasting E.U. and U.S. privacy laws).

142. *See generally* ORG. FOR ECON. CO-OPERATION & DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *available at* http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00.html (displaying international guidelines setting forth individual rights concerning processing of personal information).

143. *See* U.S. CONST. amend. IV.

144. The U.S. Supreme Court discussed the possibility of a constitutional right to information privacy in *Whalen v. Roe*, 429 U.S. 589, 598–604 (1977). For a more recent discussion, see SOLOVE & SCHWARTZ, *supra* note 139, at 474–77. There are serious doubts, however, about the current existence of a constitutional right to information privacy. *See* Am. Fed'n of Gov't Emps. v. Dep't of Hous. & Urban Dev., 118 F.3d 786, 791 (D.C. Cir. 1997) (expressing "grave doubts" as to the existence of a constitutional right of privacy in the nondisclosure of personal information).

145. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, 42 U.S.C.).

146. Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. pts. 160, 164 (2006). Several provisions of HIPAA were amended in 2009 by the Health Information Technology for Economic and Clinical Health Act, which is Title XIII of the American Recovery and Reinvestment Act. *See* American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (codified as amended in scattered sections of 6, 19, 26, 42, 47 U.S.C.); Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified in scattered sections of 42 U.S.C.).

privacy rights, such as the tort of intrusion on seclusion.[147] In addition to these established rights in the United States, many authors and political leaders have advocated for greater legal protections for rights in personal information.[148]

2. Utilitarian Arguments About Data Use

In many policy debates, rights to privacy are contrasted with utilitarian arguments, which essentially state that the benefits of some sorts of data sharing outweigh the privacy costs.[149] Economists and policymakers often turn to the utilitarian approach of cost/benefit analysis to assess alternative rules and policies.[150] To understand how the right of freedom of association fits into these debates, it is useful to identify key categories of the utilitarian arguments: the utility of users; the cost/benefit analysis for other stakeholders in social networks; and the utilitarian effects more generally.

The simplest utilitarian points in favor of social networks are that so many people have voluntarily joined them and spend so much time on them. People apparently gain a lot of utility from social networks—over a half billion people around the globe have joined them in the past few years. It is certainly true that better privacy rules might be even better for users, but the way people have "voted with their feet" (or their mouse clicks) reveals strong preferences to engage in social networking.[151]

---

147. For the classic discussion of privacy torts, see generally William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).

148. *See Bipartisan Congressional Privacy Caucus*, MARKEY.HOUSE.GOV., http://markey.house.gov/issues/bipartisan-congressional-privacy-caucus-0 (last visited May 6, 2012) (listing members of caucus, co-led by a republican and a democrat). For academic and advocate writings, see generally ANITA L. ALLEN, PRIVACY LAW AND SOCIETY (2d ed. 2010) (collecting numerous sources supporting greater legal protections for privacy rights); SOLOVE & SCHWARTZ, *supra* note 139 (same).

149. Particularly clear statements of the utilitarian approach are expressed by former FTC Chairman Tim Muris and former FTC Director of the Bureau of Consumer Protection Howard Beales. *See* J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 116–17 (2008). For a more recent statement on this approach, see *Internet Privacy: The Impact and Burden of EU Regulation: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Energy & Commerce Comm.*, 112th Cong. (2011) (statement of Stuart K. Pratt, President, Consumer Data Industry Association), *available at* http://democrats.energycommerce.house.gov/sites/default/files/image_uploads/Testimony_CMT_09.15.11_Pratt.pdf.

150. In 2011, President Obama issued an updated executive order for conducting a cost-benefit analysis for proposed major regulations. *See* Exec. Order No. 13,563, 76 Fed. Reg. 3821 (Jan. 21, 2011), *available at* http://www.gpo.gov/fdsys/pkg/FR-2011-01-21/pdf/2011-1385.pdf.

151. In August 2011, the data protection commissioner in the German State of

Beyond the utility of users, stakeholders in social networking include non-individual users (including political campaigns and nonprofit groups), the social networking companies, and advertisers. For economists, the large market value of social networks is evidence of the economic value of the industry, and the discussion throughout this Article has highlighted their usefulness for political and other expressive associations.[152]

More generally, the rise of social networking is part of the broader growth and innovation in the information technology sector. Continuing innovation can bring a wide variety of benefits, including new efficiencies, increased macroeconomic growth, and emerging products and services that people and businesses want.[153] In some instances, privacy rules and other legal rules of the road enhance innovation and economic growth, such as by fostering consumer trust and providing certainty to innovators about what practices are permitted.[154] In other instances, however, strict rules can chill innovation.[155] An overall utilitarian assessment of a proposed data rule should therefore consider these indirect effects on innovation

---

Schleswig-Holstein declared Facebook's "Like" button illegal, triggering several additional inquiries into Facebook's data analytics practices in Germany. Despite criticism from the Data Protection Authorities about user privacy, the number of new Facebook users in Germany continues to grow at a fast rate. As of October 2011, Germany had the third highest level of new user growth, and it remains the country with the tenth largest number of Facebook users in the world. *See Germany Facebook Statistics*, SOCIALBAKERS.COM, http://www.socialbakers.com/facebook-statistics/germany (last visited May 6, 2012); Eric Mack, *Facebook's 'Like' Button Illegal in German State*, CNET.COM (Aug. 19, 2011, 5:23 PM), http://news.cnet.com/8301-1023_3-20094866-93/facebooks-like-button-illegal-in-german-state/; Jan Rezab, *Top 10 Countries with Fastest User Growth on Facebook - Brazil Moves to Top of List While United States Slips*, SOCIALBAKERS.COM, http://www.socialbakers.com/blog/299-top-10-countries-with-fastest-user-growth-on-facebook-brazil-moves-to-top-of-list-while-united-states-slips/ (last visited May 6, 2012).

152. At the beginning of 2011, Facebook's estimated value was $50 billion. *See* Susanne Craig & Andrew Ross Sorkin, *Goldman Offering Clients a Chance To Invest in Facebook*, N.Y. TIMES (Jan. 2, 2011), http://dealbook.nytimes.com/2011/01/02/goldman-invests-in-facebook-at-50-billion-valuation. LinkedIn, the professional social network, was valued at $9 billion in May 2011. *See* Evelyn M. Rusli, *LinkedIn's Surge Sets Stage for More Internet I.P.O.'s*, N.Y. TIMES (May 19, 2011), http://dealbook.nytimes.com/2011/05/19/linkedins-surge-sets-stage-for-more-internet-i-p-o-s/.

153. For one explanation of the economic impact of innovation, see generally ROBERT D. ATKINSON, THE PAST AND FUTURE OF AMERICA'S ECONOMY: LONG WAVES OF INNOVATION THAT POWER CYCLES OF GROWTH (2004) (describing the process of change over the last 150 years, as well as analyzing today's economy and its effect on society).

154. The interaction of trust-enhancing and innovation-reducing privacy rules is discussed generally in SWIRE & LITAN, *supra* note 141, at 197–260.

155. *Id.*

and other goals, in addition to the effects on the participants themselves.

3. Rights vs. Utility

In a debate between rights and utility, the rights side of the argument has important advantages. A right is a different category of argument than an argument based on utility.[156] Rights arguments in many settings take precedence over ("trump") a utility argument. The right to vote, for instance, should be upheld even if it is costly to establish polling places for remote locations. For property rights, homeowners can refuse to sell to a private developer, even if the developer would create greater utility for more people.

Even where the courts don't recognize a legal right, a rights argument has the moral high ground over a cost/benefit argument such as one based on economic growth. To illustrate, consider the sorts of arguments we see in the current debates about privacy and behavioral advertising. The advertiser says something like this: "We'll make a higher return on our ad spending with greater use of personal data."[157] The advocate says: "That approach will violate a fundamental human right."[158]

The structure of this debate favors the rights argument, especially in places such as the European Union where fundamental rights in informational privacy are clearly established in law.[159] From the perspective of a human rights advocate, new uses of personal information, by advertisers or others, equates to "lesser protection of human rights." Who wants to be on the side of reducing protection of fundamental human rights? The human rights advocate may grudgingly agree that certain data uses actually benefit users, but the protector of rights remains skeptical in general of new data uses until

156. For further discussion on rights vs. utility and the law, see George P. Fletcher, *Fairness and Utility in Tort Theory*, 85 HARV. L. REV. 537, 539–40 (1972); Richard A. Posner, *Utilitarianism, Economics, and Legal Theory*, 8 J. LEGAL STUD. 103, 116–18 (1979). *See generally* Lea Brilmayer, *Rights, Fairness, and Choice of Law*, 98 YALE L.J. 1277 (1989) (discussing a rights-based approach to choice of law problems).

157. Industry attorney Stu Ingis stated, "[b]usinesses are using information to deliver ads more relevant to consumers. . . . This will make it a more efficient process to deliver content and services that consumers want. And it provides transparency for consumers to know how this information is being used." Theresa Howard, *Online Advertisers Launch Sweeping Rules over Data Privacy*, USA TODAY (July 2, 2009), http://www.usatoday.com /tech/2009-07-01-ads-online-privacy_N.htm.

158. *See* JEFF CHESTER, DIGITAL DESTINY: NEW MEDIA AND THE FUTURE OF DEMOCRACY 47 (2007).

159. *See* European Directive on Personal Data, *supra* note 141.

they are proven safe.[160] Indeed, under the European Union Directive on Data Protection, the presumption is against the legality of processing personal information, unless there is a lawful basis for such processing.[161] Because social networking creates new data uses so pervasively, the protector of rights thus may regard the entire realm of social networking with grave doubt. Officials in countries with comprehensive privacy laws are often referred to as "data protection commissioners."[162] As their title suggests, their first responsibility is to protect against data flows, which can violate human rights.

B. Data Empowerment

Data empowerment offers a different perspective than data protection. The factual nature of computing has shifted drastically since data protection principles were developed in the mainframe era. Under today's facts, individuals often have rights to use data, creating a rights vs. rights debate in place of the earlier debates between privacy rights and utilitarian claims that data flows were beneficial. Beyond formal rights, a policy and psychological tension exists between our impulses both to share and to limit sharing of personal information.

1. From Vertical to Horizontal Relationships in Computing

Facts about computing have changed enormously since the Fair Information Practices for privacy were developed in the 1970s.[163] The mainframe world of that era was hierarchical and vertical—large

160. Adam Thierer has highlighted the way that some advocates of privacy rights at least implicitly adopt the "precautionary principle" that has been widely debated in environmental law, to err on the side of safety for new and potentially dangerous technologies. *See* ADAM THIERER, MERCATUS CTR., TECH. POLICY PROGRAM, PUBLIC INTEREST COMMENT ON FEDERAL TRADE COMMISSIONER REPORT, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE 3 (2011), *available at* http://mercatus.org/sites/default/files/publication/public-interest-comment-on-protecting-consumer-privacy-do-not-track-proceeding.pdf. For a defense of the precautionary principle in environmental law, see generally Noah M. Sachs, *Rescuing the Strong Precautionary Principle from Its Critics*, 2011 U. ILL. L. REV. 1285.

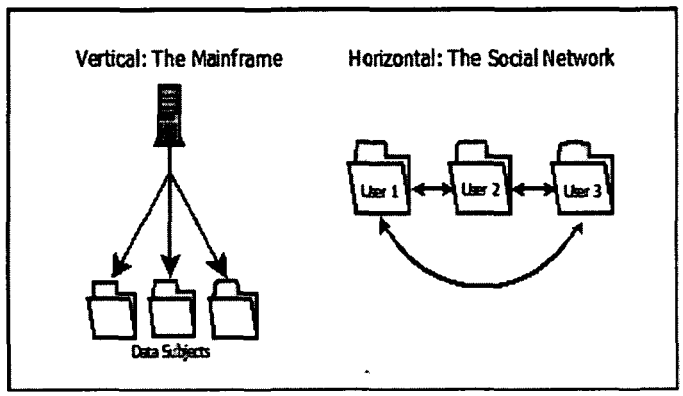
161. *See* European Directive on Personal Data, *supra* note 141, art. 7.

162. *See, e.g.*, *33rd International Conference of Data Protection and Privacy Commissioners, Privacy: The Global Age*, IFAI, http://www.privacyconference2011.org/index.php?lang=Eng (last visited May 6, 2012) (annual conference of "data protection and privacy commissioners" hosted in 2011 by Mexico's Federal Institute for Access to Information and Data Protection).

163. *See* SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS § VIII (1973), *available at* http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm.

organizations had the computers, and the managers there dictated what could be done with information.[164] The basic grammar of this period is shown by standard terms used in the E.U. Data Protection Directive, which was drafted with the mainframe in mind.[165] The large organization with the computer is the "controller"—the powerful organization that is in control. Individuals are passive "data subjects," under the control of the controllers. This factual setting, with its imbalance of power, helps an American reader further understand why "privacy law" in the United States is called "data protection law" in Europe. The E.U. Directive is designed to "protect" on at least two levels—the data subject has fundamental human rights against the controller, and data is considered presumptively risky, so the law protects against those risks.

Figure 1: Vertical vs. Horizontal Relationships



Modern computing, by contrast, is far more horizontal. Figure 1 shows the shift from the vertical (controller to data subject) to the horizontal (user to user). This insight is most popularly associated with Thomas Friedman, author of *The World is Flat: A Brief History of the Twenty-First Century*.[166] Friedman stresses the importance of

164. Prior to the personal computer, individuals could not realistically own a computer. Early "personal computers" came to market in the late 1970s, with the PC becoming far more common after IBM entered the market in the early 1980s. *See* Peter Swire, *Consumers as Producers: The Personal Mainframe and the Law of Computing*, LAW/TECH., 1st Quarter 2009, at 5, 5–9, *available at* http://www.peterswire.net/world%20jurist%20consumers.pdf.

165. *See generally* SWIRE & LITAN, *supra* note 141 (discussing how the Directive was designed for mainframe processing of personal information).

166. For economist Thomas Friedman's discussion of the horizontal, or "flat," nature of our modern information technology world, see generally THOMAS FRIEDMAN, THE

the personal computer in enabling effective economic competition from anywhere in the world, including by individuals and small businesses.[167] Individuals are also empowered in the cultural realm, creating and distributing photos, videos, blog posts, and other creations. With social networks, they create new communities and other social groupings. Linguistically, in my own writing, I have stressed the flattening of computing, that "consumers" today can also be "producers" because current technologies enable individuals to be important economic actors from home.[168] On a social network, Teenager A may comment about what Teenager B did in school that day, while Teenager C reads the post but says nothing. Adult A may post a photo from dinner about Adult B, which gets a thumbs up from Adult C. On these facts, there are no clear "controllers" or "data subjects." The vertical relationship of the mainframe era gives way to a more horizontal and equal relationship when each of us has what can be called a "personal mainframe."[169]

2. Rights vs. Rights

In the vertical world of mainframe computing, the legal focus was on the rights of the data subject to be protected from the powerful controller, to limit data flows. In the horizontal world typified by social networks, there are often individuals on both sides actively using personal information as well as passively being the subject of such data use. As discussed above, "association" is a synonym with "network"—the day-to-day stuff of social networking is about how people associate with each other.

The previous debates about privacy rules for social networks have been rights vs. utility. By recognizing the centrality of freedom of association to social networking, we realize that the debates are also rights vs. rights. For a new use of data, there are possible violations of the right to privacy. For a new restriction on data use, there are possible violations of the right to freedom of association.

One might object that the lofty term of "freedom of association" should not apply to the many mundane uses of social networking. Put another way, "freedom of association" is most importantly about political activity, and political activity is a small fraction of all the

---

WORLD IS FLAT 3.0: A BRIEF HISTORY OF THE 21ST CENTURY (3d ed. 2007).

167. *See id.*

168. *See* Swire, *supra* note 164, at 7–12.

169. *See id.* at 7. Facebook itself, however, would be more in the position of the classic controller, because it collects and manages personal information on many people as part of running its business.

ways that social networks are used. A strong version of this view could argue that political activity is such a small portion of social networking that privacy rules can safely ignore the issue.

That view is not convincing. To see why, consider social networks from the perspective of a political campaign, nonprofit leader, or individual who is seeking to mobilize friends and associates for a cause. Even if these activities are a small fraction of social networking, social networking is becoming an important and increasingly large fraction of political and nonprofit activity. The Obama campaign, the Tea Party, and political movements around the world such as in Egypt have made social networking an integral part of their strategy. As discussed previously, nonprofits today that seek to engage their membership already rely heavily on social networks and other new media technology.[170] If social networks loom large for politics and civil society organizations, then restrictions on social networks have serious implications for the freedom of association.

There can be a large impact from understanding debates as rights vs. rights rather than rights vs. utility. For privacy advocates and regulators, and others committed to human rights, there are both psychological and pragmatic advantages to conceiving the debate as rights vs. utility. The advantage from a psychological point of view is that the human rights advocate is literally on the side of right (or at least of rights). Compared with the mundane calculations of the utilitarian, the rights defender can take comfort from the clarity and simplicity of erring on the side of protecting fundamental rights. From a pragmatic point of view, rights arguments are also attractive. Where rights legally exist, there is a presumption against violating them. Alleged violators have to justify an exception in order to overcome the acknowledged legal right. In the absence of compelling facts, the utilitarian argument for an exception can easily lose to the assertion of right.

This tension between the right to privacy and the right to free association places the social networking privacy debate into broader conversations about the right to limit data vs. the right to use data. Eugene Volokh has written about how free speech rights can provide a legal basis to enable speaking truthfully about another person, despite the latter's wish for privacy.[171] Many of the free speech and

170. *See supra* Part I.A.

171. *See* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right To Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1054–57 (2000).

privacy cases to date have involved claims to use personal information by traditional news media and large marketing organizations. The increasingly horizontal nature of computing, however, makes individuals increasingly tempting targets for claims against publication of private information.[172] Copyright holders are another category of plaintiff seeking to enforce legal rights that limit flows of information. There is an extensive academic literature, however, supporting robust fair use rights in copyrighted work.[173] In each of these settings, individuals' rights to use information come into tension with individuals' rights to limit such use. The rights holder seeking to limit information flows cannot simply trump a utilitarian argument in favor of use, but must also show why one right outweighs another.

3. Data Empowerment and Data Minimization

I suggest the term "data empowerment" to describe how individuals use personal data in social networks and the many other horizontal relationships enabled by modern computing.[174] As discussed throughout this Article, the 2008 Obama campaign and the Arab Spring symbolize the political dimension of this empowerment. The discussion of nonprofit, religious, and other expressive associations shows that the empowerment goes well beyond the realm of political power. More broadly, individuals are empowered to reach out to others on many dimensions, from the cultural (writing, photos, music), to the economic (emphasized by Friedman in *The World is Flat*), to the everyday social interactions of the social networks themselves.

---

172. *See, e.g.*, Obsidian Fin. Grp., LLC v. Cox, No. CV1157HZ, 2011 WL 5999334, at *2 (D. Or. Nov. 30, 2011) (holding that "investigative blogger" was not protected under Oregon media shield law from having to reveal her sources in defamation case).

173. *See generally, e.g.*, Pamela Samuelson, *Unbundling Fair Uses*, 77 FORDHAM L. REV. 2537 (2009) (discussing fair use law and its utility when separating fair use cases into policy-relevant clusters).

174. My research has not found any use of the term "data empowerment" in any similar sense before publication of the early version of this Article. There is a different meaning for a similar-sounding term, "personal information empowerment." *See generally The Case for Personal Information Empowerment: The Rise of the Personal Data Store*, MYDEX.ORG (Sept. 27, 2010), http://mydex.org/wp-content/uploads/2010/09/The-Case-for-Personal-Information-Empowerment-The-rise-of-the-personal-data-store-A-Mydex-White-paper-September-2010-Final-web.pdf (exploring how individuals may exercise control over their own personal information through third-party "infomediaries" that manage a user's personal information); *see also generally* JOHN HAGEL III & MARC SINGER, NET WORTH: SHAPING MARKETS WHEN CUSTOMERS MAKE THE RULES (1999) (defining and discussing "infomediaries").

This data empowerment helps us understand a psychological tension that many of us have when considering how to participate in social networks. On the one hand, part of us is aware of the privacy risks and the importance of keeping parts of ourselves shielded from view from the few (anyone except our closest friends) and the many (the general public).[175] On the other hand, part of us intuitively understands data empowerment, the ways that we can meet our diverse goals by sharing information about ourselves, learning information about other people in our lives, and reaching out to those people in ways we never did before social networks made it easy to do so. The tension between data use and data limits is not simply the legal battle of rights vs. rights. It is an intensely personal tension within each of us.

This legal and personal tension also sheds new light on the important data protection concept of "data minimization."[176] Data minimization posits that holders of personal information should minimize the collection and use of personal information to protect privacy rights.[177] This concept is important in many settings, especially where the security and privacy risks are high. For example, only the minimum number of people should have access to your bank password, to prevent theft, and I have written previously about how data that acts like a key to a safe should be carefully controlled.[178] Data minimization is an important principle in wiretap law, where the state gains lawful access to the relevant conversations, but should not use the existence of the wiretap to trawl through the rest of the conversations on a phone line.[179] Minimization is used by systems administrators, to give privileges to access systems and records only as needed, in order to secure the system and prevent employees from

175. For one insightful new discussion of the reasons for shielding parts of ourselves from others, see generally JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012).

176. *See, e.g.*, EUROPEAN COMM'N, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS: A COMPREHENSIVE STRATEGY ON DATA PROTECTION IN THE EUROPEAN UNION 8 (2010), *available at* http://www.statewatch.org/news/2010/oct/eu-com-draft-communication-data-protection.pdf (discussing concept of data minimization).

177. *See id.*

178. Peter P. Swire, *Efficient Confidentiality for Privacy, Security, and Confidential Business Information*, *in* BROOKINGS-WHARTON PAPERS ON FINANCIAL SERVICES 273, 290 (Richard Herring & Robert E. Litan eds., 2003).

179. *See generally* Peter P. Swire, *A Reasonableness Approach to the* Jones *GPS Tracking Case*, STAN. L. REV. ONLINE (forthcoming Spring 2012) (discussing minimization).

inappropriately peeping into sensitive files.[180] More broadly, the idea of data minimization serves as a useful reminder, for those who process personal information, that data should not be collected, used, or retained where it can cause harm and is not needed.

We live in an information age, however. The goal simply cannot be to minimize and protect against uses of data. Data empowers individuals as well as risks the possibility of harm. Other stakeholders will push for access to personal data, such as corporations targeting advertisements, the state doing law enforcement, and medical and other researchers trying to make new discoveries. Those of us who have participated in privacy debates are familiar with these stakeholders and their usually utilitarian arguments for acquiring the data. The additional point here is that individuals themselves have the tension between data minimization and data empowerment. Regulators and advocates who focus on outcomes for the individual face difficult questions about when either empowerment or minimization will favor the individual. The tension within each of us is a tension facing regulators as well. I believe considerable further debate and research is needed to clarify the conditions under which data minimization and data protection are the correct concepts going forward, and when instead to consider explicitly the benefits to the individual from data empowerment.

CONCLUSION

Part of this Article is about doctrine, to explain the ways that the rights of both privacy and freedom of association should fit together for the association platforms that are social networks. In this analysis, I have not sought to pick sides—to be an advocate in general either for greater privacy protection or greater protection of the freedom of association. Instead, the work has been a bit like a law school exam: "The freedom of association affects how privacy can and should be regulated for social networks. Discuss." The work here is an effort to advance our understanding—to identify the issues and concerns that are likely to be more fully developed once skillful lawyers write briefs in future cases that involve both of the rights.

Perhaps the most fundamental point in this Article is that there are contrasting individual rights at issue in social networking—the right to privacy (usually pushing for limits on data sharing) and the right to freedom of association (often pushing for greater data

180. Peter P. Swire, *Peeping*, 24 BERKELEY TECH. L.J. 1167, 1183–85 (2009).

sharing). The huge privacy literature in recent decades has given many of us strong intuitions about the importance of privacy rights. I have spent years writing about ways to provide more effective privacy protections, and I stand by that body of work. But there has been no similar emphasis on the freedom of association. The idea of "data empowerment" seeks to capture the ways that individual rights are indeed enhanced by many developments in social networking and other current online tools. The Supreme Court has said: "[W]e have long understood as implicit in the right to engage in activities protected by the First Amendment a corresponding right to associate with others in pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends."[181]

The time has come to understand the implications for "association" in social "networks."

181. Roberts v. U.S. Jaycees, 468 U.S. 609, 622 (1984).