Center for American Progress

Social Networks, Privacy, and Freedom of Association

How Individual Rights Can Both Encourage and Reduce Uses of Personal Information

Peter Swire February 2011

Center for American Progress

Social Networks, Privacy, and Freedom of Association

How Individual Rights Can Both Encourage and Reduce Uses of Personal Information

Peter Swire February 2011

Contents

Introduction and summary

The ongoing political transformation in Egypt highlights the crucial role that social networks play in helping individuals organize politically. Facebook was central to the initial sweep of Egyptians onto the streets of their nation's main cities, allowing dispersed individuals to organize effectively.[1] And democracy protesters could fear, if the popular movement to displace President Hosni Mubarak had not been successful, that the regime would be able to track them down individually, in part through their Facebook accounts.

At precisely the same time that everyday Egyptians were pouring out of their homes in protest, the U.S. Federal Trade Commission was receiving comments on how new online technologies, including social networks, affect privacy.[2] The FTC request obviously did not spark protests across American cities but many here in the United States share the worries of those Egyptian protesters when it comes to privacy, including privacy of their political views but not just political privacy. These deeply held worries about information sharing must be considered given the growing role of social networking in our society—from Barack Obama's successful online political campaign that helped propel him into the presidency in 2008 to the Tea Party's successful social networking activism beginning a year later.

This report explores the tension between information sharing, which can promote the freedom of association, and limits on information sharing, notably for privacy protection.[3] Although many experts 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.[4] My analysis here, which I offer as a "discussion draft" because the issues have not been explained previously, highlights the profound connection between social networking and freedom of association.

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 do 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 email and the Web itself.[5] Indeed, the importance of the Internet to modern political and other group activity is highlighted in a new 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 38 percent have used the Internet to invite others to join a group.[6]

This new intensity of online associations through social networks is occurring at the same time as social networks and other emerging online activities receive increasing scrutiny from policymakers for privacy reasons, including the Federal Trade Commission, a recent report on privacy from the U.S. Department of Commerce, and a process underway in the European Union to update its Data Protection Directive. All these government efforts are concerned about protecting the privacy of users of social networks and other online activities, yet a previously unaddressed question is precisely how to create privacy rules without jeopardizing the freedom of association inherent in these networks' very existence.

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 into the overhaul of whitehouse.gov.[7]

My experience historically had been that people on the progressive side of politics often intuitively support privacy protection.[8] They often 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.

In this new media world, "we" the personally motivated use social networks, texts, 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.

This shift from only "them" using the data to "us" being able to use the data tracks the changes in information technology since the 1970s, when the privacy fair information practices were articulated and the United States passed the Privacy Act. In the 1970s, personal data resided in mainframe computers. These were operated by big government agencies and the largest corporations. Today, by contrast, my personal computer has more processing power than an IBM mainframe from 30 years ago.[9] My home has a fiber-optic connection so bandwidth is rarely a limitation. Today, "we" own mainframes and use the Internet as a global distribution system.

To explain the interaction between privacy and freedom of association, this discussion draft has three sections. The first section explains how privacy debates to date have often featured the "right to privacy" on one side and utilitarian arguments in favor of data use on the other. This section provides more detail about how social networks are major enablers of the right of freedom of association. This means that rules about information flows involve individual rights on both sides, so advocates for either sort of right need to address how to take account of the opposing right.

The second section shows step by step how U.S. law will address the multiple claims of right to privacy and freedom of association. The outcome of litigation will depend on the facts in a particular case but the legal claims arising from freedom of expression appear relevant to a significant range of possible privacy rules that would apply to social networks.

The third section explains how the interesting arguments by New York University law professor Katherine Strandburg fit into the overall analysis. She has written about a somewhat different interaction between privacy and freedom of association, where the right of freedom of association is a limit on the power of government to require an association to reveal its members. As discussed below, her insights are powerful but turn out to address a somewhat different issue than much of the discussion here.

From rights vs. utility to rights vs. rights

The role of data empowerment

In the mainframe era, the right to privacy was significantly at risk while the right to freedom of association by users was not usually implicated. Today, by contrast, new social networking tools both raise serious privacy issues and also are a major platform for the freedom of association. As discussed here, arguments previously have been rights vs. utility—arguments about how the right to privacy compares to utilitarian arguments in favor of use of personal information. Now the debate much more becomes about rights vs. rights—how to fit the right of privacy with the right of freedom of association. The right of freedom of association, in turn, is part of a broader change in the relationship of data and individuals: Instead of personal data often being a threat to individuals, individuals benefit from "data empowerment."

The "right to privacy" is a complicated term. I will try to clarify how arguments about privacy rights fit into a discussion of the practices of social networks. To begin with, I am not referring 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. 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 and implemented in the 1995 Data Protection Directive. A human rights approach to privacy is also embodied in the widely cited 1980 privacy guidelines from the Organisation for Economic Co-operation and Development.

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

In many policy debates, these rights to privacy are contrasted with utilitarian arguments, which essentially state that the benefits of some sorts of data sharing outweigh the privacy costs. 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 participants
- The utilitarian effects more generally

Let's consider each of these categories in turn.

The utility of users

Some arguments focus on the benefits that individuals themselves get from social networking. People apparently like social networks a lot—more than half a 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 do social networking.

Cost-benefit analysis for other participants

Economists and policymakers often turn to the utilitarian approach of cost-benefit analysis to assess alternative rules and policies. In addition to any costs and benefits for individual users, participants in social networking include nonindividual users (such as 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.

Utilitarian effects 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. In some instances, privacy rules and other 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. In other instances, however, strict rules can chill innovation. An overall cost-benefit assessment of a potential regulation should therefore consider these indirect effects on innovation and other goals, in addition to the effects on the participants themselves.[10]

Sorting out the arguments

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. Rights arguments in many settings take precedence over ("trump") a utility argument. The right to vote, for instance, should be upheld even if it costs more 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: "We'll make a higher return on our ad spending with greater use of personal data." The advocate says: "That approach will violate a fundamental human right."

The structure of this debate favors the rights argument, especially in places such as the European Union where fundamental rights in informational privacy are established in law. 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 they are proven safe. 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.

This clarification of the rights vs. utility debate helps us see the importance of considering the freedom of association in our overall assessment of social networks. 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. In the discourse of human rights, people using a social network are exercising their right to freedom of association.

In short, 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 the debates are also rights vs. rights. For each new use of data, there are possible violations of the right to privacy. For each 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 ways 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. Nonprofits today that seek to engage their membership already rely heavily on social networks and other new media technology. If social networks loom large for politics and civil society organizations, then restrictions on social networks can have serious implications for the freedom of association.

As rights vs. rights arguments thus become more important to the debate about privacy regulation, a related insight is the new importance of "data empowerment." The focus of the discussion thus far has been about how social networks augment the freedom of association for politics and nonprofit activities. Social networks

also augment other abilities for individuals. The mainframe world was hierarchical and vertical—large organizations had the computers and information technology managers dictated what could be done with information.

Social networks, by contrast, are person-to-person and far more horizontal. I have written previously about the ways that "consumers" today can also be "producers" because current technologies enable individuals from home to be important economic actors.[11] Individuals are empowered in the cultural realm, creating and distributing photos, videos, blog posts, and other creations. With social networks, they also create new communities and other social groupings.

"Data empowerment" provides a more general framework for analyzing the tradeoffs between rights of privacy and rights associated with the use of information. Simply from the viewpoint of the individual—without consideration of benefits or costs for advertisers, the networks themselves, or others—the facts in a particular setting may favor either sharing or limits on use of personal information.

Privacy regulators and others have long supported the concept of "data minimization"—that holders of personal information should minimize the collection and use of personal information to protect privacy rights. The analysis here shows why the collection and use of personal information also supports "data empowerment," or the ways that personal data can advance an individual's rights and achievement of goals in the political, economic, cultural, social, or other realms.

When it comes to personal data, then, new uses should not trigger a presumption of violation of privacy rights. In a given factual setting, those uses may actually advance individual rights. So how does U.S. law apply? To this we now turn.

U.S. law applied to privacy and freedom of association

The discussion thus far has helped show in general how freedom of association and other rights may be implicated by privacy rules about social networking. Getting more specific on the facts, the government might set privacy rules for what names and other data "friends" or "friends of friends" get to see. Or the government might set standards for what a political party, nonprofit, or other organization can see about individuals who "like" the organization, or set limits on how organizations can communicate with relevant individuals, including members, those who "like" the group, or people with shared interests but who are not yet members of a group.

Because social networks are still so new (Facebook had its seventh birthday recently and has

grown in that time from a college site to more than half a billion users), the ways that associations are formed may evolve rapidly, as might government efforts to regulate for privacy or other purposes. In addition, the recent Pew Foundation study shows that patterns of association seem to differ 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 the rules for forming groups and recruiting new members are likely more important than in the offline world.[12]

The next question is how the law would handle the multiple rights at issue. Fortunately, there are well-established methods in American law for how judges examine conflicting rights. The discussion here explains the basic legal doctrine and then examines three hypotheticals: a state or federal law that prohibits all use of social networking sites for political campaigns; a "privacy by design" rule that requires default settings to share as little personal data as possible; and a "do not track" requirement that applies specifically to the activities of political campaigns, charities, or other nonprofit activities.

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.[13] Although the First Amendment does not itself apply to decisions by social networking companies, there may well be strong policy and normative arguments that companies should consider privacy rights, freedom of speech and association, and other constitutional rights as they decide how to build and configure their systems.

The focus of my discussion is on how state action could limit data empowerment—how rules about data sharing could limit the ability of individuals, political campaigns, and others to reach out to others in order to create and deepen associations. The text of the First Amendment does not mention the "freedom of association" but instead states that Congress shall make no law "prohibiting the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

The freedom of association is deeply established in U.S. constitutional law, however. The Supreme Court has said: "we 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."[14] The Court has identified two categories of associational rights. One is "intimate" association, such as the right to choose who lives with you. The other is "expressive" association, such as the right to join with others for political, moral, or other reasons.

State action that infringes on the freedom of association may be permitted but only after careful judicial scrutiny. The Supreme Court has found that infringements on the right "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."[15] For instance, the Supreme Court has found it constitutional to limit the rights of members of a private club to exclude women or blacks. A court in such instances must make two key findings: that there is a compelling state interest, such as reducing sex or race discrimination; and that the state action is well tailored, so the infringement on the freedom of association is no more than necessary to achieve the state interest.

This test for freedom of association is similar to the test for state action that regulates based on the content of speech. Under the "strict scrutiny" standard

for content-based regulation, the state action is permissible only if it is narrowly tailored to a compelling state interest and is the least-restrictive means for protecting that interest. For both speech and association, there must be a compelling state interest that justifies the state action, and careful tailoring of the state action to that state interest.

There is a looser judicial test for state action that governs only the "time, place, and manner" of speech and not its content. The classic example is a limit on the hours that a sound truck can use its loudspeaker in a residential neighborhood. The Supreme Court has said that restrictions of this kind are valid provided that "they are narrowly tailored to serve a significant governmental interest, and that they leave open ample alternative channels for communication of the information."

This test is easier to meet than the rule for content. It requires only a "significant" rather than a "compelling" state interest, and instead of requiring the law to be narrowly tailored, the law need merely permit ample alternative channels for communication. I am not aware of any clear precedent on whether this sort of "time, place, and manner" approach would apply to the freedom of association.[16]

With these legal precepts in mind, we are in a position to see the structure of how an American judge would assess the interaction of privacy and freedom of association for state action affecting social networks. The first hypothetical is a state or federal law that prohibits the use of social networking sites for political campaigns.[17] Under constitutional challenge, the state would argue that privacy is the compelling state interest. The law, for instance, could reduce unwanted and intrusive messages and reduce the ability of third parties to gain access to sensitive information about a person's political beliefs.

In addition, intensive information use about an individual's political reading and views, as discussed further below, might itself chill a person's freedom of association. Evidence from a social network, for instance, might reveal individuals' participation in unpopular political causes, such as a small and unpopular political party. Targeted advertisements about those unpopular causes can be embarrassing if they appear as a person is using the computer, such as if a workplace colleague looks over the user's shoulder and learns, "Oh, you're one of those." These sorts of privacy concerns have been prominent in the current debates about rules for behavioral advertising, including advertising on social networks.

In response to the state interest in privacy protection, the First Amendment challenger would argue that privacy is not a compelling enough state interest to justify infringement on the fundamental rights of freedom of association and freedom of speech. One relevant factual issue would be how effective the law would be at protecting privacy, in light of the restriction on freedom of information and the content-based restriction on speech. The challenger could also say that the law is not well tailored and could suggest less restrictive ways to achieve the state interest.

The first example is an easy case to show how the First Amendment can be the basis for striking down a privacy law. The hypothetical law directly addresses political associations and limits speech based on content. The structure of the argument, though, also applies to more realistic examples of limits on social networking sites. For the second hypothetical, suppose "privacy by design" (that is, building privacy protection into the initial designs of a product or service) is required by a U.S. law or regulation, or in a state enforcement action.[18]

In this example, imagine that a social networking site is required to set the default to the more protective option for a new product or service. A variation would be if there is a legal presumption of privacy by design, which allows the less privacy-protective setting only if the site meets various criteria. A current example might be the setting on some sites that allows a "friend" to see either all of your friends or only those friends you have in common. The more privacy-protective setting is the latter and a law or enforcement action might require such a default in order to protect the privacy of the friends who have chosen to be linked to one person but haven't made the same choice to be linked with others.

The challenger could claim that this privacy-by-design requirement would violate users' freedom of association and speech by disrupting the challenger's ability to find and contact individuals who would be interested in joining the association. The state would answer by saying that protecting privacy is a compelling state interest and that it cannot be achieved through means significantly less restrictive of associational freedoms. A court hearing the case would then likely need to develop a factual record, exploring effects on freedom of association and privacy and assessing alternative restrictions.

For instance, suppose the challenger came forward with evidence that the more restrictive setting substantially reduces the effectiveness of networking for political and civil society activities. In this potentially realistic example, one could

imagine a judge deciding that the rule violates the test for freedom of association—it does not "serve compelling state interests, unrelated to the suppression of ideas, that cannot be achieved through means significantly less restrictive of associational freedoms."

A third hypothetical involves the application of a "do not track" requirement to the activities of political campaigns, charities, and other nonprofit activities.[19] At a technical level, this question raises some novel questions. Previously, the Federal Trade Commission has made important exemptions in privacy rules for political campaigns and nonprofits. For instance, the "do not call" list prohibits telemarketing calls for individuals who have chosen to get on the list. The exception for politics and nonprofits is why, even if we're on the list, we still get phone calls at home from the Police Benevolent Association or a new candidate for Congress.

Now here's the tricky part. A social networking platform typically configures itself the same way for contacts with commercial companies and with political campaigns and other nonprofits. To the extent privacy laws shape the configuration of a social networking operation, it is not clear how or whether it is possible to create the same safe harbor for politics and nonprofits that we have traditionally had for telemarketing and door-to-door contacts.

The upshot: Freedom of association and freedom of speech require careful tailoring of the scope of the state action, and consideration of less restrictive approaches to meeting the state interest in protecting privacy. I have not seen any previous discussion of this interaction of the First Amendment and "do not track" laws and it deserves consideration as the FTC, Congress, and the Commerce Department consider their current privacy proposals.[20] A distinct but related issue is the subject of the next section.

When freedom of association protects privacy

The discussion thus far has shown ways in social networking that the right to freedom of association can be in tension with the right to privacy. There has previously been some discussion, developed most fully by New York University law professor Katherine Strandburg, that legal rules about freedom of association instead can protect rights in privacy, notably in restricting government searches and seizures of personal information.[21]

Strandburg's argument begins with a famous case from the civil rights era, when the state of Alabama tried to require the NAACP to reveal the identity of its members. 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 was forced by the state to reveal its member list.[22]

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 last year when Iran shut down protesters using social media and other online sites, governments can trample on freedom of association by making intrusive demands on the sites for personal information. Similar concerns existed in Egypt until President Mubarak stepped down. 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 different from the tradeoffs between privacy rights and freedom of association discussed in the previous section. 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. I have addressed the freedom of association of those who use social networks to enhance their ability to associate, such as for political campaigns, nonprofits, and politically engaged individuals. Strandburg's

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 earlier about how U.S. law addresses both privacy and freedom and association. The added wrinkle, I believe, is to recognize that the type of freedom of association Strandburg emphasizes can be a state interest that supports the case for privacy regulation. Recall that judges faced with a freedom-of-association claim must find a compelling state interest in order to uphold state action. The discussion earlier assumed privacy protection was the potentially compelling state interest. Strandburg's approach helps us 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.[23]

To conclude, three categories of individual rights can be implicated by the settings and practices of social networks:

- The right to privacy
- Freedom of association for those wishing to expand their network
- Freedom of association for those who do not wish their associations to be revealed

These three types of rights can operate at the legal level, such as in a federal trial court that would develop a factual record about the effects on these rights. The three types of rights can also operate at a policy and nonlegal level—the analysis identifies specifically what sorts of rights are at issue in the design and operation of social networks.

Conclusion

The online-inspired political transformation in Egypt, occurring at the same time U.S. and European government agencies are asking for comment about online privacy, shows the importance of having an integrated understanding of both privacy and the freedom of association. The events unfolding in Egypt concern revolutionary political moments but the Obama campaign, the Tea Party, and the daily activities of innumerable charities and social causes show that modern associations occur extremely frequently through social networks and related online services.

My goal in this discussion draft is to explain the ways the rights of both privacy and freedom of association should fit together. In this analysis, I have not sought to pick sides—to be an advocate 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."

Or similarly, 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 and other advocates write briefs in future cases that involve both of the rights.

Perhaps the most fundamental point in this paper 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 sharing). The huge privacy literature in recent decades has given many of us strong intuitions about how privacy rights may be at stake.

I have spent many 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 individual rights are indeed enhanced by many develop-

ments in social networking and other current online tools. The Supreme Court has said: "we 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."

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

Endnotes

1 Cecillia Kang and Ian Shapira, "Facebook treads carefully on Egypt, international takedowns," *The Washington Post*, February 3, 2011, available at http://voices.washingtonpost.com/posttech/2011/02/in_egypt_the_tried-and-true_to.html.

2 A very similar version of this document is being submitted as a comment to: Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers" (2010), available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

3 Because of the number of issues addressed in this paper where I have not found prior discussion, it seemed wise to release this paper as a discussion draft and then provide more detailed legal and factual discussion in subsequent papers.

4 I have done 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 below, 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. The power of social media in this way is a theme of the U.S. State Department project on Internet Freedom. When this paper was already in the works, Clay Shirky published an insightful article in Foreign Affairs called "The Political Power of Social Media" (Dec. 2010). I welcome readers to point me to any existing writing that explains how these two major themes about social networking—privacy and freedom of association—fit together.

5 The focus of the discussion here is on social networks, which have emerged very recently and 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 "social network" or not; instead, the facts of the way that associations are formed online will be crucial to the relevance of freedom of association.

6 Pew Internet & American Life Project, "The Social Side of the Internet," Press release, January 18, 2011, available at http://www.pewinternet.org/Press-Releases/2011/Social-Side-of-the-Internet.aspx.

7 For a set of my materials about Web 2.0 and the federal government, see: Peter Swire, "Six New Media Challenges" (Washington: Center for American Progress, 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," The New York Times Bits Blog, June 2, 2009, available at http://bits.blogs.nytimes.com/2009/06/02/the-obama-adminstrations-silence-on-privacy/. I spoke in greater detail about data empowerment at the OECD Conference on data privacy guidelines in Jerusalem in October 2010. See: "Swire's Speeches and Public Appearances: 2010," available at http://www.peterswire.net/psspeeches2010.htm.

8 My experience is that many (but by no means all) conservatives are more inclined to favor a free-market approach to legal regulation of privacy for the private sector.

9 Peter Swire, "Consumers as Producers: The Personal Mainframe and the Law of Computing," *Law/Technology* 42 (1) (2009): 5–37, available at http://www.peterswire.net/world%20jurist%20consumers.pdf.

10 The interaction of trust-enhancing and innovation-reducing rules is discussed in: Peter P. Swire and Robert E. Litan, *None of Your Business* (Washington: Brookings Institution, 1998).

11 Swire, "Consumers as Producers."

12 "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." Pew Internet & American Life Project, "The Social Side of the Internet."

13 There are minor exceptions, such as in a "company town" where the local coal mine owns all the property and limits speech in the town. For an in-depth treatment, see: Dawn C. Nunziato, *Virtual Freedom: Net Neutrality and Free Speech in the Internet Age* (Stanford, CA: Stanford University Press, 2009).

14 *Roberts v. U.S. Jaycees*, 468 U.S. 609 (1984).

15 Ibid.

16 The "time, place, and manner" cases to date have concerned free-speech rights. My research has not uncovered any example of applying this sort of "time, place, and manner" standard to the freedom of association. To defend a state action, it is interesting to consider whether the settings for a social networking service might be considered "time, place, and manner" restrictions on association, and thus subject to less than strict scrutiny. This possibility shows the relative lack of precise precedents about how the right to association applies to social networks, and is a reason why I welcome comments on this "discussion draft."

17 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 often involved "adult" commercial activity. More nuanced legal discussion would be needed but "association" in the form of dating has been a prominent feature of social networking sites, and laws limiting dating sites might be struck down as violating the freedom of intimate association.

18 The FTC preliminary staff report (referenced in endnote 2) supports greater use of privacy by design, including at page v in the executive summary.

19 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." The staff 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.

20 The discussion of "do not track" raises two additional legal issues that will require more detailed examination in follow-up work. First, an issue raised by the application of "do not track" to political campaigns and nonprofits is whether and how the "commercial speech" doctrine should apply to the freedom of association. For advertising and other commercial speech, the Supreme Court has permitted state action with less than strict scrutiny under *Central Hudson Gas & Elec. Corp. vs. Public Service Comm'n*, 447 U.S. 557 (1980). The ability of organizations to reach out to new members might lead to a similar analysis of "commercial association" doctrine, where less than strict scrutiny might apply to limits on the ability of corporations to reach out to new members of a group that supports them on a social network. This appears to be a novel area of doctrine—I am not aware of any previous discussion of a "commercial association" approach. Next, if any such "commercial association" doctrine exists, the question arises of whether stricter scrutiny would apply to political campaigns, nonprofit organizations, and other noncommercial actors seeking to use an online service for political association reasons. A second issue concerns the FTC report's attention to rules for material changes in a privacy policy, and the effect on freedom of association of strict rules that require affirmative consent before a social network or other online service is allowed to make changes to its data uses and privacy policies. In light of the rapid and recent rise of social networking, we are still in the experimental or "learning by doing" phase of knowing what features individuals prefer and what their expectations are or will be once people get more experienced in social networking. In this phase, there are strong reasons to allow a fair amount of experimentation to see what works for users in general and what is effective at fostering freedom of association, freedom of speech, and other individual rights. Strict rules that chill experimentation thus would be another topic subject to the compelling state interest and tailoring legal doctrines discussed here. One particular concern is to combine strict limits on changes of privacy policy with strict standards for privacy by design up front. In combination, a strict limit on changes can reduce the incentive of an online provider to be strict at the design phase: If the initial setting is set with loose privacy protections, the online provider can shift to stricter privacy protections over time; however, if the initial setting is set with strict privacy protections, then it becomes much more risky for the provider to shift the settings to a less restrictive setting over time. Put more simply, strict rules on changing policies can undermine the effectiveness of privacy by design.

21 Katherine Strandburg, "Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance," 49 B.C. L. Rev. 741 (2009).

22 *NAACP v. Alabama*, 357 U.S. 449 (1958).

23 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. The factual persuasiveness of the two different aspects of freedom of association may vary for "normal" politics, such as related to ordinary elections in the United States, and for "revolutionary" politics, such as occurs when human rights and other activists are seeking to topple a current regime. The Strandburg aspect of freedom of association is likely to be more salient in the latter situation, where protecting the identities of activists is likely to be especially important.

About the author

Peter P. Swire is the 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. He is also a Policy Fellow at the Center for Democracy and Technology and a member of the Advisory Board for the Freedom of Privacy Foundation. He was special assistant to the president for economic policy from 2009 until August 2010, serving in the National Economic Council under Lawrence Summers. From 1999 until early 2001, he served as chief counselor for privacy in the U.S. Office of Management and Budget.

Acknowledgements

My thanks for comments on an earlier draft by Neil Richards, Katherine Strandburg, and Eugene Volokh. The views expressed here are my own and should not be attributed to them.

The Center for American Progress is a nonpartisan research and educational institute dedicated to promoting a strong, just and free America that ensures opportunity for all. We believe that Americans are bound together by a common commitment to these values and we aspire to ensure that our national policies reflect these values. We work to find progressive and pragmatic solutions to significant domestic and international problems and develop policy proposals that foster a government that is "of the people, by the people, and for the people."

Center for American Progress

1333 H STREET, NW, 10TH FLOOR, WASHINGTON, DC 20005 • TEL: 202 682 1611 • FAX: 202 682 1867 • WWW.AMERICANPROGRESS.ORG