

A Social Network Users' Bill of Rights: "You" Must Decide

Christina M. Gagnier, Esq.
Gagnier Margossian LLP
gagnier@gamallp.com

A Social Network Users' Bill of Rights provides a framework for town hall style engagement in the complex online privacy policymaking process while arriving at a body of generally accepted principles that can guide government regulatory efforts. The importance of such dialogue is in addressing the normative aspects to privacy law and user rights, whether reinforcing the tort protections currently available for individual privacy here in the United States or working towards a set of "principles" that recognizes the international impacts of web platforms. A norm-driven endeavor can support entrepreneurs to employ architectural solutions to privacy, creating a complimentary regulatory framework and marketplace that rewards "privacy by design" while promoting innovation.

I. Introduction

The convergence of "reality media," social networks and instant publication have led to the misconception that privacy is dead; rather, we remain in our own societal beta test of the global power of the social net. For digital natives and the rest of us, valuing privacy has always required some sort of a contextual element, a lesson, a moment or an incident that causes one to value privacy. Privacy is subject to a trigger effect.

The trigger for many came with the Facebook and Google privacy controversies of 2010. The technological changes by these companies that undermined user privacy led various stakeholder groups to come together at the 2010 Computers, Freedom and Privacy Conference and create a draft "Social Network Users' Bill of Rights." The "Bill of Rights" (#snubor), in its current draft form, includes the following rights:

"We the users expect social network sites to provide us the following rights in their Terms of Service, Privacy Policies and implementations of their system:

- 1. Honesty: Honor your privacy policy and terms of service.*
- 2. Clarity: Make sure that policies, terms of service, and settings are easy to find and understand.*
- 3. Freedom of speech: Do not delete or modify my data without a clear policy and justification.*
- 4. Empowerment: Support assistive technologies and universal accessibility.*
- 5. Self-protection: Support privacy-enhancing technologies.*
- 6. Data minimization: Minimize the information I am required to provide and share with others.*
- 7. Control: Let me control my data, and don't facilitate sharing it unless I agree first.*

8. *Predictability: Obtain my prior consent before significantly changing who can see my data.*

9. *Data portability: Make it easy for me to obtain a copy of my data.*

10. *Protection: Treat my data as securely as your own confidential data unless I choose to share it, and notify me if it is compromised.*

11. *Right to know: Show me how you are using my data and allow me to see who and what has access to it.*

12. *Right to self-define: Let me create more than one identity and use pseudonyms. Do not link them without my permission.*

13. *Right to appeal: Allow me to appeal punitive action.*

14. *Right to withdraw: Allow me to delete my account, and remove my data.”*

At the Southwest by Southwest Interactive festival in March 2011, accompanying two of the “Bill of Rights” authors, Lisa Borodkin and Jack Lerner, the “Bill of Rights” was presented in an open discussion. The points outlined within this paper address the commentary provided, and the questions asked both on and offline about the contents of the draft itself. This content is fundamental to the debate surrounding user privacy. Despite treatment by the Federal Trade Commission and the Department of Commerce in their policy papers and emerging legislative solutions, most recently, the McCain-Kerry draft online privacy bill, an effort to actively solicit public input as to desired privacy and associated user rights is lacking in this continuing evolution of consumer rights online.

II. The lack of an individual private right of action within circulated legislative draft bills further disables individuals to rely on the tort protections available for the protection of individual privacy in the absence of a mechanism to evaluate user norms.

Our tort privacy framework in the United States is largely shaped by cultural norms and practices. The lack of a private right of action within the circulated draft provisions of the McCain-Kerry online privacy legislation, and the absence of discussion of these protections in the policymaking process, merits user-driven efforts. Legislative attempts aim to address the obvious violations of user trust and data mismanagement of platform providers, but fail to recognize the underlying priorities users may have. The prioritization by a broad and diverse user base of the rights they deem necessary, and in some cases, fundamental to their use of social networks, will serve to educate the legislative process and create a normative framework necessary to perhaps revive the tort protection currently available for individual privacy. A legislative fix is not necessarily a normative one, and does not serve the enhanced need for users to access these tort protections in the digital age.

What is a “reasonable expectation of privacy” in our digital age? User demands at times seem incompatible: users openly share photos of intimate situations while demanding privacy of certain personally identifiable information. In the battle to coalesce the tension between the virtual and visceral world, the concepts who is a “public figure,” what is of “legitimate concern to the public,” and generally determining the difference between private and public space are in flux. These are not merely abstract ideas: they are the elements of existing tort actions relied upon by individuals to protect their privacy rights. It is imperative to learn from users and develop norms around these concepts, as their legal impact comes from a judicial interpretation of shifting societal mores.

Aside from merely protecting these individual rights in terms of our existing privacy tort regime, the “rights” conversation is not limited to user rights vis-à-vis platforms: there is a need to address the interactions between users as well. An intimate understanding of the desired rights in these situations can only come from users themselves; a top-down legislative fix will not serve to resolve these points of contention when the technology shifts so rapidly and some challenges may be platform-specific. Each platform has its own unwritten “code,” a set of norms and language standards that only apply in that context. Understanding the necessary data limitations and privacy expectations that should be placed on these platforms must be generated from the users themselves based on collective experience.

III. A user-generated effort allows for the integration of norms beyond those developed in the United States, supporting a movement towards universal human rights principles online.

Organizing around a “Social Network Users’ Bill of Rights” accomplishes normative goals that are essential to our existing privacy regime in the United States. Yet, this conversation has international implications: it is platforms provided by companies based in the United States that are defining rights for a growing base of international users.

A gaping void in international human rights law, the lack of treaty law and customary international law concerning human rights in the online world, leaves those who are denied basic freedoms very little to turn to. While principles protecting free expression are codified in both the *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political Rights*, the borderless nature of the Internet, and the daily global interaction between Internet users, transforms the domestic online privacy conversation in the United States into an international one.

The powerful utility of social networks in facilitating mass communication during political revolution could not have been envisioned less than two years ago, beginning with Iran, a situation where content spread a message virally across the globe in a handful of hours. Hashtags like #jan25 support the idea of a continued “rights” conversation, as our society finds itself in the early stages of understanding what rights and values are important in an international context, with the consideration that many of these platforms are provided by companies in the United States.

Platform agnosticism is one such issue that has emerged, a proposed “right” that would prevent companies from taking sides in international conflicts by filtering or removing content, inspired by companies like Twitter who have taken the lead by demonstrating such a commitment. In the larger international law conversation, the treatment of these networks as non-state actors, with a public function or nexus in times of social and political turmoil, has yet to be explored.

IV. While a subset of bad actors has necessitated the need for government intervention in online privacy, a “Bill of Rights” provides an opportunity for entrepreneur-supported efforts, allowing for the creation of voluntary mechanisms leading to a competitive privacy marketplace with a complimentary regulatory framework.

Media has embraced the narrative of a necessarily adversarial relationship between user and platform. This context has caused many emerging startups to perceive the attempts at regulation as anti-entrepreneur: additional rules and regulations will hinder growth, whether or not one finds merit in the “technology bubble” rumors around the startup industry. Regulation may be necessary for the “800-pound gorilla” bad actor, but a policymaking effort absent startups, specifically in the burgeoning data industry, may stymie essential economic growth.

No doubt governments, at the state and federal level, find themselves in a conundrum with user rights: a “wait and see” approach, hoping that the bad actor will change its policies, brings with it few guarantees. Additionally, positive incremental changes to the privacy practices of platform operators are not indicia of a corporate commitment to respecting user rights. When Facebook announced in October 2010 that it was now allowing users to download their data from their Facebook account, putting users in control of where their data is and in the driver's seat for where they take their data next, these actions seemed to comport with rights that were included in the draft Social Network Users’ Bill of Rights, specifically, Article 7, "Data Control," and Article 14, "Right to Withdraw.” Despite these changes, the six-month time period since these the launch of these features has been riddled with announcements by Facebook of practices exposing its users to an increased amount of data misuse.

Competition with privacy is a tricky concept; it cannot replace the need for regulation, but regulation and competition can surprisingly be complimentary. Some privacy adherents believe true preservation of privacy rights can only be achieved through “code,” through site architecture that is designed with privacy in mind. The market may be the appropriate place to provide these incentives to startup companies while a complimentary regulatory framework, cognizant of the challenges faced by entrepreneurs, can police the companies whose actions will have the largest net impact on the user community.

V. Conclusion

The corporate-created legal regimes that users are currently beholden to have their failures, but the mechanisms to address these failures are still in the early stages of development. The Social Network Users’ Bill of Rights states in its preamble, “We the users...” In order to create a true solution in terms of protecting user rights, user stakeholders must be involved.