Platform Data is Social: How Publicity and Privacy are Vital to Data Governance

Prem Sylvester and Wendy Hui Kyong Chun

Canada, like many other nations, is proposing a new suite of legislation that acknowledges privacy as a fundamental and individual human right, most notably the Digital Charter Implementation Act, 2022 or Bill C-27. Although important, these proposals do not adequately consider how platforms' social nature challenges the neat distinction between private and public spheres. These challenges occur at the levels of user actions, algorithmic data processing, and technical communications. For example, users frequently post pictures and birthdates of their children on social media; recommender systems and digital advertising regularly target users based on data that serve as proxies for political affiliation or sexual orientation; wireless network cards constantly read-in all available data—including their neighbours' passwords—in order to determine what information to forward to a computer's Central Processing Unit.

To address these challenges, researchers and advisors have called for group-based privacy rights and the introduction of the category of inferred data, both of which underscore the limitations of an individual-based rights framework. Recommendations from the Office of the Privacy Commissioner of Canada (OPC) for Bill C-11 also underscore an individual's "right to reputation," including the right to be forgotten that may take the form of data deletion.

To complement and further these interventions, this brief describes the unique challenges posed by social data and how to revise policy around data collection, use, and governance to account for public rights.

Being in Public on Platforms: How We are Recognized by Data

To be on platforms is to be social. As Hannah Arendt had argued long before the advent of social media, the social is neither public nor private—it deliberately blurs the distinction between the two, enabling seemingly private concerns to have a wider audience and bringing a (sometimes unwanted) audience into seemingly private matters.

On platforms, this blurring takes three interrelated forms. First, the technical architecture of networking technologies operates through blurring boundaries between private and public. We connect to platforms through wireless devices that constantly 'leak' data such as IP addresses and (geo)location.

Second, algorithms designed to 'personalize' platforms use *correlated* data to predict and shape our social habits. Such social data makes our private desires appear in/as public. With Amazon's acquisition of One Medical, for example, the cost of medical insurance policies may be correlated not just to our own purchase history and financial data, but to the (private) data of other people.

Third, platforms encourage people to publicly interact with each other as if we were in a private space with trusted, or seemingly trustworthy, others. At the same time, through platforms, people choose to (or have to) be in public — and garner publicity — to participate in social life. The rise of influencers and other forms of microcelebrity, collective action organized on social media platforms, and platforms tracking gig workers driving on public roads, all point to how platforms make possible and change publicity. Such publicity may expose prominent members of vulnerable groups, such as female influencers and Black activists, to harassment. Even while having everyday conversations or discussions tangential to their political activity, social data connects such individuals to those who might mock or threaten them.

The interactions and relations that emerge from such publicity both rely on, and generate, data that are collected and used by privately owned and operated platforms. Platforms make possible the collection of *social* data for their *private* benefit. The privacy of platform companies, as currently codified, protects their rights to the generation of social data for commercial use. The privacy of individuals, however, is subject to violation through the very information that can be inferred from such data.

We therefore need to develop two forms of rights. First, we need privacy rights that protect boundaries between ourselves and platforms to protect us from corporate data extraction. Second, we need to develop public rights that allow us to engage in collective and public actions without being exposed to collective harms.

Privacy and publicity rights that do not recognize how we might want to, or are compelled to be, in public are inadequate. To govern platforms and their data operation, we need to recognize the particular (and peculiar) way platforms use our data to engender publicity and, consequently, shape people's reputations. We need a framework for *public* rights that acknowledges the social grounds of publicity's relationship to privacy.

From Publicity Rights to Public Rights

The publicity rights established through decades of case law offer precedent for our framework. Such rights are intended to protect against the "wrongful appropriation of personality," or what may be termed one's identity as defined by their image, name, or likeness, especially for commercial exploitation or profit. More recent case law asserts that a person does not need to be a 'public figure' (such as an influencer or a celebrity) to expect that their privacy will not be infringed upon while being in public. The link between reputation and privacy, meanwhile, has some legal precedent in the Civil Code of Québec: Article 35 stipulates that "Every person has a right to the respect of his reputation and privacy." In general, however, an individual's reputation is protected against *defamation* through provincial regulation such as Libel and Slander Acts (e.g., in Ontario and BC) and sections of the federal Criminal Code pursuant to Offences Against the Person and Reputation. In such cases, the *publisher* of the defamatory statements or claims pays monetary damages to the affected person(s).

There are, however, two significant ways in which existing regulation is limited. First, publicity rights primarily protect individual rights to the extent that one's identity is 'proprietary.' Second, individual rights are insufficient to protect one from the reputational harms that might *emerge* from socially derived data. Private information *becomes public* because of the social dimensions of platforms—one's identity and reputation, built in part via correlations, is not solely individual. That is, one's actions on social media may affect one's own, or another person's, public identity. That data, in turn, holds commercial value for platforms due to their correlations to people's identities.

Protecting privacy would therefore require *public rights* premised on our *privacy in public*: it would require the ability to refuse publicity in the first place. These rights in the context of data governance would delineate what data about groups and individuals should never be collected, stored, or used. They would also establish how data about our platform use should be collected, stored, or used so that collective or individual harms do not accrue to vulnerable people. Public rights would allow us to be social without our privacy being violated or our publicity being exploited.

Operationalizing Public Rights in (Social) Data Governance

A public rights framework would thus regulate data that could be used to make harmful inferences about people: inferences that could impact people's reputations, their ability to be safe online, and their ability to keep some information private. It would prevent *private* platforms from making problematic inferences about individuals as well as groups of people through what people are — technically, algorithmically, and for commercial benefit — encouraged to share *publicly*. Such a framework would set the terms for anonymity — not simply anonymization or de-identification — so that platforms do not impinge on our *fundamental* right to privacy (beyond our *data* privacy). Public rights would take fully into account the reality that the data which platforms collect, store, use, and sell are inherently, and unavoidably, *social data.*