7

Privacy and Knowledge Production Across Contexts

Brett M. Frischmann,[1] *Katherine Haenschen*,[2] *and Ari Ezra Waldman*[3]

In his seminal article, *The Sociology of Secrecy and of Secret Societies*, Georg Simmel (1906) argued that secrecy is a "universal sociological form" defined by hiding something in certain contexts (p. 463). Although secrecy can constitute a barrier between people, separating those who know the secret from those who don't, secrecy within a social space binds people together; secrecy in this context "determines the reciprocal relations of those who possess the secret in common" (p. 470). Those relations are often governed by rules that protect the secret, whether that is a Masonic rite, a pledge at an Alcoholics Anonymous meeting, a provision in a contract, or a norm developed over time. In other words, far from stifling conversation, social interaction, and sharing, formal and informal rules about secrecy, privacy, and information dissemination actually allow social groups to share information among their members, contributing to social solidarity, cohesion, and even knowledge production.

This chapter begins where Simmel and many other social and legal scholars left off. In contrast to many traditional theories of privacy (Westin 1967; Inness 1992; Rosen 2000), we argue, as one of us has argued before, that privacy rules and norms are essential to social interaction and generativity (Waldman 2018). Through primary source research, we suggest that the rules and norms governing information privacy in three knowledge creation contexts – Chatham House, Gordon Research Conferences ("GRC"), and the Broadband Internet Technical Advisory Group ("BITAG") – are

[1] Charles Widger Endowed University Professor in Law, Business and Economics, Villanova University, Charles Widger School of Law; Affiliated Faculty, The Vincent and Elinor Ostrom Workshop in Political Theory and Policy Analysis, Indiana University Bloomington; Affiliate Scholar, Center for Internet and Society, Stanford Law School; Affiliate of the Princeton Dialogues on AI and Ethics, Princeton University; Trustee, Nexa Center for Internet & Society, Politecnico di Torino. J.D. Georgetown University Law Center; M.S., Columbia University; B.A., Columbia University.

[2] Assistant Professor, Department of Communication Studies and Political Science, Northeastern University. Ph.D., University of Texas at Austin; M.A., University of Chicago; B.A., Columbia University.

[3] Professor of Law and Founding Director, Innovation Center for Law and Technology, New York Law School; Microsoft Visiting Professor of Information Technology Policy, Princeton University, Center for Information Technology Policy; Affiliate Fellow, Yale Law School Information Society Project. Ph.D., sociology, Columbia University; J.D., Harvard Law School; A.B., Harvard College.

https://doi.org/10.1017/9781108749978.008 Published online by Cambridge University Press

necessary to develop the kind of trust that is essential for sharing ideas, secrets, and other information. More specifically, when it is part of institutional structures governing knowledge commons, privacy fosters knowledge through a systematic social process. Privacy rules have *expressive effects* that embed confidentiality norms in the background of institutional participation, which in turn create a sense of *community* among participants that can both bring in new members and threaten *sanctions* for misbehavior. Knowledge production, therefore, depends on privacy.

7.1 COMMONS, KNOWLEDGE PRODUCTION, AND PRIVACY

This chapter builds on some of our previous work. Madison, Frischmann, and Strandburg (2010a, 2010b) and Frischmann, Madison, and Strandburg (2014), for example, describe the knowledge commons framework. *Commons*, they note, refers to an institutional arrangement governing resources, whatever they may be, among a group of people. In addition to being both a form of governance and a social construct, the "basic characteristic that distinguishes commons from noncommons is institutionalized sharing of resources among members of a community" (Madison, Frischmann, and Strandburg 2010b, 841). That is, the goal of commons governance is to devise a way to share resources despite endogenous (e.g., diminishing resources) and exogenous (e.g., political pressure) obstacles.

Knowledge, one of the resources governed within the commons, is a broad term, encompassing the "various cultural, intellectual, scientific, and social resources (and resource systems) that we inherit, use, experience, interact with, change, and pass on to future generations" (Frischmann, Madison, and Strandburg 2014, 2–3). Whether these are norms of interaction, cultural artifacts, or art, knowledge refers to the full range of socially constructed pieces of information constituting human social experience. Knowledge *production*, then, is the social process in which information is shared and added to our collective consciousness. Knowledge production can be the development of new ideas for research, new cultural or artistic contributions, new processes or systems, and so on. Together, *knowledge commons* captures the "institutionalized community governance of the sharing and, in some cases, creation, of information," broadly defined (p. 3).

Privacy is part of that community governance and we argue that it plays a critical role in knowledge production (Sanfilippo, Frischmann, and Strandburg 2018). Understanding what we mean by *privacy*, then, is critical. There is a long tradition of social scientists, lawyers, philosophers, economists, and other scholars trying to develop a singular definition of privacy (Warren and Brandeis 1890; White 1951; Blaustein 1964; Westin 1967; Gerety 1977; Gavison 1980; Bok 1983; Reiman 1984; Innes 1992; Rosen 2000). There is also a growing group of researchers eschewing that approach (Solove 2002; Nissenbaum 2009) and recognizing how privacy can be generative (Richards 2015; Waldman 2018). But many scholars have defined privacy in terms of separating, hiding, or staking out autonomy from society (Waldman 2018,

13–33). We resist that conceptualization. In previous work, Waldman defined privacy as a social structure governing information sharing (p. 67). Similarly, Sanfilippo, Frischmann, and Strandburg (2018) conceptualize "privacy as information flow rules-in-use constructed within a commons governance arrangement." It may sound strange to talk about privacy from a social perspective. But privacy presumes that we exist in both formal and information relationships with others; privacy only matters when we share within those relationships. When making sharing decisions, we rely on and develop expectations about what should happen with our information based on the contexts in which we share, thus integrating privacy into our lives relative to other people. As Post (1989) has noted, privacy norms "rest[] not upon a perceived opposition between persons and social life, but rather upon their interdependence" (p. 959). Privacy, then, is socially situated; it is about the social relationships governing disclosure between and among individuals.

Those relationships are based on trust, or lack thereof. Trust is a "resource of social capital between or among two or more persons concerning the expectations that others will behave according to expected norms" (Waldman 2018, 51). Social capital is the advantages and benefits that accrue to individuals in a community by virtue of their connected status (Putnam 1997). For example, teams of coworkers can be more productive by learning from each other and relying on each team member's particular expertise. Scholars, physicians, lawyers, compliance professionals, technologists, and other elite professionals can learn from each other at workshops and conferences. Unionized workers can exercise greater leverage over their working conditions and contract terms than isolated laborers. Different countries can realize economic, political, military, and cultural benefits from cooperation. In all of these examples, social capital refers to the good things that develop out of our interactions with others.

Trust is one of those good things, and an essential part of the social structure created by privacy governance. Trust is the "favorable expectation regarding other people's actions and intentions," or the belief that others will behave in predictable manners according to accepted contextual norms (Möllering 2001, 404). In the information context, those norms are usually confidentiality and discretion. For example, if we ask a friend to hold our spare set of keys, we trust she will not break in and steal from us. When an individual speaks with relative strangers in a support group like Alcoholics Anonymous, she trusts that they will not divulge her secrets. Trust, therefore, includes a willingness to accept some risk and vulnerability toward others and steps in to grease the wheels of social activity in the absence of perfect knowledge. We cannot know for certain that our neighbor will not abuse her key privileges or that our fellow support group members will keep our confidences.

Trust, like other norms of social life, can develop hierarchically from above or organically from below. For example, legal rules can influence norms of behavior through the law's expressive power (Citron 2009; Hellman 2000). Fiduciary laws, medical malpractice law, and legally enforced canons of ethics are just three of the

myriad rules and private ordering schemes that support trust norms. Private ordering can achieve the same end, like when organizations establish rules of conduct, prohibit harassment, and create privacy protocols. From below, experience or explicit or implicit social cues develop trust. Experience gives us more data from which to judge the trustworthiness of others: keeping a friend's confidences for ten years gives them a stronger basis for trust than doing so for a single day. Explicit ("This is between us") and implicit cues (physically turning away from a crowd, huddling down, whispering) can also generate expectations of trust (Goffman 1966). As can reciprocity, that is, mutual sharing, which establishes mutual vulnerability (Buchan, Croson, and Dawes 2002) and helps generate mutual feelings of cooperation and altruism (Fukuyama 2001). Cues also allow us to trust strangers. For example, two people who share a stigmatizing social identity often create an instant bond of trust based on a shared set of narratives and experiences (Williams 2001). And we are more willing to interact with others the more embedded they are in a familiar social network, even if we don't know them (Granovetter 1985). As Niklas Luhmann (1979) has stated, trust begins where knowledge ends. As such, trust allows us to interact with and rely on others.

7.2 CASE STUDIES

In this way, privacy governance contributes to knowledge production in institutional contexts by greasing the wheels of disclosure and social interaction. Privacy rules define the terms and expectations of information sharing and express the norms of trust for a given community. That community then internalizes those privacy rules and expectations of trust to ensure ongoing compliance by bringing in new members to an environment where privacy is a social fact (Durkheim 1895/1982) and leveraging the threat of formal and informal sanctions for breaches. That social process helps develop new ideas, new knowledge, and new culture.

To illustrate this process and its role in knowledge creation, we rely on primary source research, including interviews with leaders and participants, to describe three different information sharing contexts that have associational rules and norms that govern disclosure.[4] First, Chatham House has an eponymous non-attribution rule widely used in meetings to facilitate open dialogue. The rule restricts the dissemination of identity and affiliation information, but does not govern what participants can do with the content of communications. Second, GRCs follow a well-known set of nondisclosure and nonuse rules designed to enable researchers to come together and present their cutting-edge data without fear of being scooped. Third, the BITAG has adopted privacy and intellectual property rules that allow their expert participants to come together, hash out their ideas and points of contention, and develop

[4] In line with past GKC case studies, we conducted semi-structured interviews using the GKC framework to organize questions. In this chapter, we report on the privacy rules directly focused on appropriate information flows within and beyond the community and context.

technical advisory reports for industry and government. In all three of these case studies, privacy governance builds the trust necessary for knowledge production.

7.2.1 *Chatham House*

British and American delegates to the Paris Peace Conference after World War I originally conceived of what would become Chatham House as a community of cross-Atlantic experts "to study international problems with a view to preventing future wars." Then called the British Institute of Foreign Affairs, the think tank moved to Chatham House in 1923 and received its official Royal Charter in 1926. To this day, it remains a locus of expert discussions and global problem solving in foreign affairs, economic progress, and sustainability (Chatham House, History). Despite its participation in many of the most important worldwide debates in the last century, the community is primarily known for one thing: the Chatham House Rule.

The Chatham House Rule ("Rule") is a simple rule of non-attribution used far beyond the confines of the Chatham House itself. The Rule reads as follows:

> When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed (Chatham House, About, Chatham House Rule).

The Rule allows "people to speak as individuals, and to express views that may not be those of their organizations." Therefore, the Rule "encourages free discussion" (Chatham House Rule FAQ) and knowledge production by establishing dissemination rules and norms of a given context, creating a sense of community around those rules, and threatening sanctions for violators. And the Rule can be modified in any given circumstance to fit the needs of a particular environment, thus providing the flexibility needed for knowledge production in different settings (Burnett Interview).

Keith Burnett, the Director of Communications and Publications at Chatham House, explains that the Rule sets the terms for information flow. Any event, meeting, or discussion governed by the Rule would either begin with an acknowledgment that the Rule applies – "This meeting is governed by Chatham House Rule" – or participants "would know in the invitation" to the event. Laying out the ground rule at the beginning has several important effects, according to Burnett. First, it lets meeting participants set their expectations for the shelf life, if any, of their statements during the event. Burnett noted, for example, that "whoever is running the meeting could take away some information and use it" to write a report or address some ongoing problem. Participants come into the meeting knowing this and can calibrate their participation accordingly. Second, the Rule encourages free flow of ideas by protecting participants from any negative effects of open sharing. The Rule is "there to help people share

https://doi.org/10.1017/9781108749978.008 Published online by Cambridge University Press

information that they learn in the meeting" without having to "worry about attribution" and any retribution that can result. Third, it prioritizes ideas and solutions over people and egos. Chatham House was established to solve important and vexing problems of international affairs, so sharing ideas is essential: "the idea is to free people up [to speak], free people up to feel that the ideas are more important than the individuals sharing them." Finally, putting everyone on the same page with respect to information use immediately creates a sense of mutual trust among participants; there is, at least, an initial expectation that participants will behave according to the norms set out by the Rule (Waldman 2018; 52–54). Chatham House itself makes this connection between the Rule and trust, noting that "the rigorous implementation of the Rule is crucial to its effectiveness and for Chatham House's reputation as a trusted venue for open and free dialogue" (Chatham House Rule FAQ).

The Chatham House Rule, then, reflects the contextual nature of information flow. Like the American sociologist Erving Goffman (1959), who explained that differences in social behavior and information disclosure often depend on the rules and expectations associated with different contexts, the Chatham House Rule creates contexts conducive to free discussion. Goffman suggested that social life can be divided into "front" and "back" stages, like a play, with different forms of social interaction happening in each. In front, like in the dining room of a fancy restaurant, servers interact with patrons formally, conversation is restricted to business, and behaviors are constrained by strict rules. In back, like in a kitchen out of view of paying customers, servers can let their hair down, curse, talk about their lives, and behave more informally among their colleagues. There are many front and back stages: work/home, professional/social interactions, when the kids are awake/after bedtime, and so forth. Each context maintains different rules and expectations, which permit or constrain social behavior accordingly. As Julie Cohen (2000) has noted, this account of social behavior is not really about hiding from others; rather, it is about establishing the parameters of social space in ways that make continued interaction possible. That is precisely what the Chatham House Rule does, as well. It establishes the parameters of information flow in a meeting governed by the Rule, allowing participants to act more informally, engage more freely, and, hopefully, work more effectively to achieve the meeting's goal. As Burnett notes, the Rule clarifies what is and is not permissible: "the whole purpose of the Rule," Burnett notes, "is to share ideas without identifying the speaker, the source of the information, so if you do anything to identify that person, directly or indirectly, you should avoid it."

Although one has to apply, anyone can join Chatham House in London (Chatham House Individual Membership). For Chatham House events and meetings held under the Chatham House Rule, it is the expressive power of the Rule that creates a sense of community among participants. A meeting governed by the Chatham House Rule immediately binds all participants together in a secret-keeping endeavor (Simmel 1906). This creates a sense of trust among the members

of the group that they are all present for the same purpose, on the same terms (Waldman 2018, 52–54). Although Chatham House is a "global community" and that "academics come from all over" to participate, Burnett suggests that the Rule, and the information flow it facilitates, is what matters. That is, it doesn't matter who says what, "the whole point is to come and share knowledge – we share ours, you share yours," and the Rule creates the space for that to happen (Burnett Interview). This is also part of the ethos of meetings run under the Rule, which allows participants new to Chatham House or the Rule to integrate into the community norms rather quickly.

The threat of sanctions also plays that role. Chatham House explains that although its Rule is "not legally binding, Chatham House will take disciplinary action against a member or guest who breaks the Rule," which can mean "exclusion from all institute activities" (Chatham House Rule FAQ). Participants in Chatham House events governed by the Rule also mutually reinforce the Rule. The FAQs and Burnett both note that individuals ask other members if a given example of sharing – on social media or to other people – is permissible, with the overarching response focused on sharing without any kind of attribution. In this way, formal and informal sanction from the governing structure, as well as reinforcing work from other participants, work to ensure the Rule, and the meetings it governs, will achieve their goals.

This discussion suggests that the Chatham House Rule may be an effective form of privacy governance that fosters knowledge production within specific groups. By setting the parameters of information flow, it creates a sense of trust among participants, allowing them to rely on the confidentiality and discretion of a community built around the Rule.

7.2.2 *Gordon Research Conferences*

Like the Chatham House Rule, the Gordon Research Conference is a replicable institutional structure where privacy governance can foster knowledge production. The GRC was started in 1931, when the chemist Neil Gordon brought together scientists to network and share research results at Johns Hopkins University. Since then, the GRCs have grown worldwide, having attracted more than 30,000 participants annually to 300 conferences across the world (Gordon Research Conferences, History of GRC). They are well-regarded, invite-only, and attract what one participant called "the best people" (Sanfilippo Interview). Like Chatham House, GRC integrates a simple privacy rule into institutional governance; unlike Chatham House, its rule is strict confidentiality, not nonattribution. Like most knowledge commons, GRCs depend on other governance strategies beyond the privacy rule. For example, to maintain a close-knit community, each GRC is kept small and focused on a narrow topic at the frontier of the field. Secluded locations are preferred because seclusion is seen as something that helps structure the

https://doi.org/10.1017/9781108749978.008 Published online by Cambridge University Press

community, create a forum where people can get together and build relationships and trust, and avoid distractions.

The GRC No Publication Policy ("Policy"), sometimes referred to as the "off-the-record policy," states, in relevant part: "To encourage open communication, each member of a conference agrees that any information presented at a Gordon Research Conference . . . is a private communication . . . and is presented with the restriction that such information is not for public use." The Policy prohibits audio or video recording and photography. It also prohibits participants from preparing any form of publication based on the conference proceedings. The Policy covers any form of information sharing, including through social media, and covers formal presentations, poster sessions, and even informal discussions and conversations among participants. Yet the Policy is not an absolute prohibition; it vests authority in the individual making a presentation to consent to quotation, publication, recording, or other deviations from the rule: "[Y]ou [must] have the explicit written permission of the person you're planning to quote. So, it's allowable, but it's kind of locked down" (Grannas Interview).

The primary purpose of the Policy is to give participants the confidence that they can share their latest, in-progress research without fear of others taking their ideas and publishing them first (Grannas Interview). Amanda Grannas, Associate Vice Provost for Research and Professor in the Department of Chemistry at Villanova University, explained how at the GRCs, she and other participants presented early stage research, data, and hypotheses without fear of being "scooped" by other participants. Her post-doc advisor had encouraged her to attend her first GRC to present work in progress to receive feedback and network with others. For Grannas, this experience stood in stark contrast to the American Chemical Society national meeting routinely attended by 12,000–15,000 people, where she would not present early work because the risk of being scooped was real. Grannas had been warned and knew of people whose ideas had been taken at the conference. During our interview, she praised GRCs for being a trusted community and forum and emphasized how important it was to be able to present pre-publication research in an environment where the rules facilitated free and constructive feedback on in-progress works.

Therefore, the GRC's No Publication Policy contributes to knowledge production through a social process similar to that of the Chatham House Rule: a clearly defined rule sets participant expectations, building trust through community and the threat of sanctions. And those expectations are communicated to participants clearly and repeatedly up front. According to Grannas, acceptance letters to GRCs state "congratulations, . . . here are all kinds of expectations . . . . It's expected that you're not sharing this information, you're not quoting any of this, you can't refer to anything." The Policy is also on the GRC webpage and conference chairs state the rules at the beginning of the event. "When the group comes together for the first time, there is a welcome from the chair and . . . they sa[y] explicitly that you can have a great time at Gordon" and even have a Gordon hashtag on Twitter, "but do not talk

about hearing a great talk, . . . do not take a picture of a slide and tweet it or put it on Facebook." There is, then, a real sense in which "what happens at Gordon, stays at Gordon" (Grannas Interview).

The confidentiality policy reinforces a sense of community by relying on participants to enforce it and, as noted earlier, by creating a network of secret-keepers (Simmel 1906), thus creating the trust necessary for open discussion. The GRC Policy "facilitates community" by permitting open "coordination, collaboration, and direction of research" (Sanfilippo Interview). The Policy, in other words, solves a problem particularly salient to academic researchers: "how to facilitate discussion without worrying about people stealing your ideas" (Id.).

When veterans see new participants, "the chain keeps going and norms and rules are passed on" (Grannas Interview). Sometimes this happens explicitly. One participant recalled hearing presenters say, for example, "In the spirit of the GRC, I'm showing you unpublished research," which implies a duty to maintain the speaker's confidentiality (Sanfilippo Interview). Otherwise, participants "learn [the norms] just by observing the practice" (Id.). Participants recognize that GRCs include a relatively "small number of people" where "everybody knows everybody, except for new people coming in and we want to do right by them" (Grannas Interview). GRCs include social events for networking purposes, including group meals, mentorship opportunities, and other "non-sciencey" meet-ups (Id.). These not only promote additional knowledge production but also serve to pass on appropriate expectations of social behavior to the next generation of scholars. Invited attendees are encouraged to bring guests who can participate in daily social activities, but to preserve confidentiality, "guests are not permitted to attend the conference lectures, or poster sessions." (Gordon Research Conferences, Policies; Grannas Interview). As Grannas noted, the GRC has become "more family friendly. They very much lock it down that guests cannot attend the science. Only the scientists are there. And I think that is kind of leading towards the privacy issue. It's easy for someone that isn't as familiar with the expectations to start tweeting about, oh this cool thing that I'm sitting at with my wife or my husband at this thing."

Also like Chatham House, GRCs mostly rely on participants to enforce privacy governance. Participants who notice someone flouting the Policy may "contact the chair and say, 'look, this happened, I don't know what you want to do, but maybe this person shouldn't come back to one of these" (Id.). More commonly, though, the pressure to adhere to GRC confidentiality norms is social and informal. According to Grannas, there is a "level of accountability that, I think, the small nature of the group [provides]. . . . [T]he fact that you're going into it with very explicit goals, it would be very antithetical to then take an idea and go off and scoop or do whatever nefarious thing you're going to do." Violators are "blackballed" in the scientific community if they record, tweet, or scoop. "We would take care of it," Grannas noted, if it actually happened.

Notably, the GRC Policy is different from the Chatham House Rule. The former is a confidentiality requirement, whereas the latter permits disclosure of the substance of discussions just without names and attribution. Although both are privacy governance structures, they serve both overlapping and distinct purposes. The goal of the Chatham House Rule was, from the beginning, to foster open conversation to solve a pressing problem in world affairs. The discussion would inform the meeting's chair, who would likely take what she had learned and incorporate it into public facing reports, recommendations to policymakers, or proposals for peace. The GRC No Publication Policy also fosters conversation and sharing ideas by creating the space necessary for researchers to trust they won't be scooped. Indeed, its expansion over the last few decades is a testament to its success at creating that kind of environment. But the goal of the GRCs is to help participants, not the outside world, learn and receive feedback on their own research projects. As such, different rules regarding dissemination make sense. Both rules, however, leverage the same social process by which privacy governance fosters knowledge production.

7.2.3 *Broadband Internet Technical Advisory Group*

The Broadband Internet Technical Advisory Group (BITAG) was created to bring together technical experts on a voluntary basis to discuss and develop consensus advisory reports on technical operation of the Internet. Here, there is no risk of being scooped, as there is at GRCs. Like the original Chatham House meetings, BITAG members come together to produce a public-facing document. But the need for privacy governance to create open and frank conversation remains; stakeholders and participants come from different sectors, business, and backgrounds, and they are trying to solve potentially contentious technical problems. To do that, members must be free to share inchoate or developing ideas (Richards 2015) and offer suggestions that their employers might oppose. To achieve this goal, BITAG sets out a strict confidentiality rule that leverages the same social process of fostering knowledge production through trust, community, and the threat of sanctions.

The BITAG restricts the dissemination of "all information disclosed by any Participant during any meeting or activity" of the BITAG Technical Working Group or committees ("BITAG information").[5] All such information is considered confidential, and participants agree that they "shall not use any portion of the ... information for any purpose except to perform his, her, or its obligation to BITAG" (BITAG Intellectual Property Rights Policy ("IPR Policy") Section 4.1). BITAG also

[5] With the exception of "public information" and "highly confidential information," "all information disclosed by any Participant during any meeting or activity" is classified as BITAG information. See BITAG IPR Policy Sections 4.1, 4.2, and 4.3. Notably, in contrast with the Chatham House rule, public information includes "BITAG and TWG [technical working group] membership rosters" as well as "identities of BITAG's Board, including the identity of Designated Participating Members and their Director Designees, and BITAG's officers and employees." BITAG IPR Policy Section 4.2.

binds itself to not use or disclose confidential information shared during BITAG meetings and working group sessions (Id.). There is some leeway to share information with other BITAG members. Membership in BITAG extends beyond the individuals who participate in meetings to the companies and organizations of which individuals are a part. Thus, for example, if one company's employee attends a BITAG meeting, that employee may disclose BITAG information (but not "highly confidential information"[6]) to other "employees, contractors and agents of" her company, but only if they "agree to maintain the confidentiality of the BITAG Information" (BITAG IPR Policy Section 4).

The BITAG confidentiality rule "helps, especially when there is disagreement" to ensure open and frank discussion. Jason Livingood, Vice President of Technology Policy and Standards at Comcast and a BITAG participant, notes that the point of the rule is to "learn and move forward" together and "talk about things openly." To do that, participants need to know that "there's not going to be any attribution; we're not going to go back to our bosses and say, 'this other guy at this other company said'" something at a BITAG meeting. What's more, BITAG wants to encourage expert participants to speak openly, even if what they say conflicts with their employers' official position. Therefore, the expectation is that conversations "are very private and in particular may surface something about my company's perspective, but I personally disagree with. . . . If someone were to share that, I would be in a lot of hot water professionally" (Id.). In this way, the rule fosters sharing and knowledge production by protecting participants from professional retribution.

To ensure that all participants can operate under the same set of confidentiality expectations, BITAG deploys the same strategy as Chatham House and GRC: event chairs state the rule at the beginning and participants reinforce it over time. At the start of working group sessions, for example, leaders will "go back for the standards . . . [and say,] 'here, just as a reminder, this is how we work, we are not going to tweeting about what we're talking about here to sharing anything we talk about.' Everything is confidential" (Livingood Interview). Throughout the process of working together to achieve some kind of consensus report, "there are reminders, [like,] 'hey, don't share any of this externally. There will be a point in time when we're ready to do that, but it's not right now'" (Id.). This set clear expectations and fosters trust among BITAG working group participants by setting the terms of social

[6] An even stricter confidentiality rule applies to "Highly Confidential Information," which "(a) relates to any non-public financial information disclosed by the Member to BITAG and its staff and advisors as part of the membership application process; (b) identifies how any individual TWG Representative voted with respect to a majority opinion in a Report; or (c) is marked by the Member as 'Highly Confidential Information' when disclosing such information to BITAG." BITAG IPR Policy Section 4.3. The first two categories are not surprising or controversial; the last category is open-ended in that it allows Members to attach the label upon disclosure. "BITAG will not use or disclose such Highly Confidential Information to any person except that BITAG may disclose such information to its legal counsel and advisors or to the Board if BITAG legal counsel deems such disclosure necessary to enable BITAG, BITAG staff and the Board to comply with its obligations under the Bylaws, the TWG Governance Manual, these Policies or the Certificate of Incorporation." Id.

interaction and expressing what the organization feel is proper behavior. If participants found out that someone was disclosing the substance of their discussions, members "would be very upset." It would, Livingood noted, "be a real violation of trust."

According to Kaleb Sieh, the Deputy Director and General Counsel of BITAG, Inc., the confidentiality and nondisclosure rules create a community of members: "confidentiality binds the entire organization" because everyone knows that "we only share with people as necessary." BITAG further develops this community sentiment by design, creating working groups and committees that have professional membership requirements. This allows participants to trust that they're getting the best input and advice on their projects (Livingood Interview). Membership rules aim to (i) maintain openness to "both individuals and organizations representing stakeholders from a broad cross-section of the Internet ecosystem" (Seih and Hatfield 2012, 8) while (ii) ensuring technical expertise among the working group participants and (iii) guarding against "forum packing" or other strategic behavior by particular stakeholders. In other words, membership and some associated voting rules aim to maintain the integrity of the community and trust within and from outside the community.

This community takes it upon itself to police and enforce the confidentiality rules, even though there has been little need for enforcement (Livingood Interview). Although individuals and companies can be terminated from BITAG for violating the rules, the most important sanctions are more organic and social: "if they violate the rules, their professional reputation would be shot" (Id.). Individual participants, the scientific experts and engineers, often know (or know of) each other from the broader scientific and technological community or even from other similar working groups or standard setting organizations, such as the Internet Engineering Task Force. While governance rules vary across organizations and contexts, the professional norms and reputations span them (Id.). More importantly, violations of BITAG confidentiality represent breaches in trust (Waldman 2018). As Livingood noted, those who disseminate information are "definitely no longer part of the group. . . . But even other members would make it clear that you can't trust" those who violate the rules. "Not trusting on an individual level is important," and when BITAG members can't trust someone, they are ostracized from the community, even if they're not formally expelled.

7.3 COMPARATIVE ANALYSIS

These organizations and their rules are not identical. Chatham House and BITAG have always been structured to produce outward-facing reports on contentious issues; GRCs provide scholarly feedback to participants only. GRCs and BITAG use strict confidentiality rules; Chatham House created a rule that encourages sharing without attribution. The Chatham House Rule is leveraged by working

groups, discussions, and meetings across the world that have nothing to do with the original Chatham House, whereas the GRC No Publication Policy applies to its series of scholarly scientific conferences and BITAG's confidentiality rule applies to its meetings alone. GRCs and BITAG depend on strictly managed membership in groups where relationships are expected to last beyond the duration of a specific meeting; Chatham House membership is open, and the Chatham House Rule can but need not be used in conjunction with membership rules. The differences in institutions reflect different social dilemmas faced in pursuit of shared community objectives (Sanfilippo, Frischmann, and Strandburg 2018).

And yet despite these differences, all three institutions leverage privacy governance to foster knowledge production, and they use the same social process to do it. Their rules give meeting participants the confidence to share sensitive information and engage openly and honestly without fear of retribution or premature public dissemination. This reflects the connection between trust and sharing within a community (Waldman 2018; Sanfilippo, Frischmann, and Strandburg 2018). That is, regardless of any variation in their strength and breadth, the rules generate trust among participants that their colleagues will behave according to the privacy norms established by the rules. This allows members to share sensitive information, whether to improve colleagues' scholarship or solve a vexing problem. As secret keepers pursuing a shared set of objectives or common purpose, participants are bound together in a community and, because the secret defines the boundaries of their community, members have an interest in reinforcing the strength of their privacy rules (Simmel 1906). As such, they mutually reinforce the privacy norms that allow the institutions to persist.

None of the organizations rely on legal enforcement of privacy governance rules. Instead, members leverage the value of the community itself and threat of being removed from it to drive conformity with the norm. Chatham House explicitly states in its FAQ that members or guests who break the rule will likely be excluded from all future events. For GRC, violators can be banned from future events, and other members might go so far as to speak to the offending faculty member's university administrators about the action, causing even greater professional harm. For BITAG members, breaching the confidentiality and intellectual property rules could lead to legal action, but our research suggests that has yet to happen. Breaking the rules would greatly upset the other members, potentially leading to expulsion from the community and reputational consequences that extend into other professional communities. In all instances, it is the threat of shame, the perception that others would look down on an individual for violating the privacy norm, that compels this behavior.

In this way, privacy rules foster knowledge production by socially constructing an environment in which trust gives individuals the confidence and safety to share information. Without the Chatham House Rule, the GRC No Publication Policy, and BITAG's confidentiality rule participants would restrict what they say to guard

against personal and professional harm. These rules, then, foster open communication, learning, and new ideas.

7.4 CONCLUSIONS

In this Chapter, we have relied on ethnographic interviews of participants and leaders in three organizations – Chatham House, the Gordon Research Conferences, and the Broadband Internet Technical Advisory Group – to suggest that privacy rules contribute to knowledge production. But although the interviews reinforced evidence from the social science literature on the connection between trust and a propensity to disclose information, ethnographic evidence is necessarily limited. Empirical research can add rigor to the theoretical structure developed here. Scholars can survey participants in meetings governed by the Chatham House Rule, the GRC Policy, and the BITAG confidentiality requirement for self-reported perceptions on the role of privacy governance in knowledge production across contexts. Researchers can also move beyond the narrow confines of the three case studies discussed here to analyze privacy governance in more informal social institutions, including among friends and families, among support group members, and even among strangers. Other questions remain, including the role of formal law in fostering knowledge production and the ways in which privacy may interact with conflicting values like openness and transparency.

REFERENCES

Blaustein, Edward J. "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser." *New York University Law Review* 39, 962–1007 (1964).

Bok, Sissela. *Secrets: On the Ethics of Concealment and Revelation*. New York: Vintage, 1983.

Broadband Internet Technical Advisory Group, Inc., Intellectual Property Rights Policy, Version 2.0, Adopted: June 28, 2012.

Buchan, Nancy R., Rachel T.A. Croson, and Robyn M. Dawes. "Swift Neighbors and Persistent Strangers: A Cross-Cultural Investigation of Trust and Reciprocity in Social Exchange." *American Journal of Sociology* 108, 168–206 (2002).

Burnett, Keith. Interview. By Brett Frischmann. October 9, 2018.

Chatham House Rule FAQ. *Chatham House: The Royal Institute of International Affairs*. www.chathamhouse.org/chatham-house-rule-faq.

Chatham House Individual Membership. *Chatham House: The Royal Institute of International Affairs*. www.chathamhouse.org/membership/individual-membership.

Citron, Danielle Keats. "Law's Expressive Value in Combatting Cyber Gender Harassment." *Michigan Law Review* 108, 373–415 (2009).

Cohen, Julie E. "Examined Lives: Informational Privacy and the Subject as Object." *Stanford Law Review* 52, 1373–1438 (2000).

Durkheim, Émile. *Les règles de la méthode sociologique*. Translated by Halls, W. D. as *The Rules of Sociological Method*. New York: Free Press, [1895]1982.

Frischmann, Brett M., Michael J. Madison, and Katherine J. Strandburg, eds. *Governing Knowledge Commons*. Oxford, UK: Oxford University Press, 2014.

Fukuyama, Francis. "Differing Disciplinary Perspectives on the Origins of Trust." *Boston University Law Review* 81, 479–494 (2001).
Gavison, Ruth. "Privacy and the Limits of Law." *Yale Law Journal* 898, 421–471 (1980).
Gerety, Tom. "Redefining Privacy." *Harvard Civil Rights-Civil Liberties Law Review* 12, 233–296 (1977).
Goffman, Erving. *Behavior in Public Places: Notes on the Social Organization of Gatherings*. New York: Free Press, 1966.
The Presentation of Self in Everyday Life. New York: Doubleday, 1959.
Grannas, Amanda. Interview. By Brett Frischmann. April 6, 2018.
Granovetter, Mark. "Economic Action and Social Structure: The Problem of Embeddedness." *American Journal of Sociology* 91, 481–510 (1985).
Hellman, Deborah. "The Expressive Dimension of Equal Protection." *Minnesota Law Review* 85, 1–70 (2000).
History. *Chatham House: The Royal Institute of International Affairs*. www.chathamhouse.org/about/history.
History of GRC. *Gordon Research Conference*. www.grc.org/about/history-of-grc/.
Inness, Julie. *Privacy, Intimacy, and Isolation*. Oxford, UK: Oxford University Press, 1992.
Livingood, Jason. Interview. By Brett Frischmann. May 14, 2018.
Luhmann, Niklas. *Trust and Power*. New York: John Wiley and Sons, 1979.
Madison, Michael J., Brett M. Frischmann, and Katherine J. Strandburg. "Constructing Commons in the Cultural Environment." *Cornell Law Review* 95, 657–709 (2010a).
"Reply: The Complexity of Commons." *Cornell Law Review* 95, 839–850 (2010b).
Möllering, Guido. "The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation and Suspension." *Sociology* 35, 403–420 (2001).
Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Palo Alto, CA: Stanford University Press, 2009.
Policies. *Gordon Research Conference*. www.grc.org/about/grc-policies-and-legal-disclaimers/.
Post, Robert. "The Social Foundations of Privacy: Community and Self in the Common Law Tort." *California Law Review* 77, 957–1010 (1989).
Putnam, Robert. "Democracy in America at Century's End." *Democracy's Victory and Crisis*. Ed. Axel Hadenius. Cambridge, UK: Cambridge University Press, 1997.
Reiman, Jeffrey H. "Privacy, Intimacy and Personhood." *Philosophical Dimensions of Privacy*. Ed. Ferdinand David Schoeman. Cambridge, UK: Cambridge University Press, 1984.
Richards, Neil. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. Oxford, UK: Oxford University Press, 2015.
Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Vintage, 2000.
Sanfilippo, Joseph. Interview. By Brett Frischmann. August 2, 2018.
Sanfilippo, Madelyn Rose, Brett M. Frischman, and Katherine J. Strandburg. "Privacy as Commons: Case Evaluation through the Governing Knowledge Commons Framework." *Journal of Information Policy* 8, 116–166 (2018).
Sieh, Kaleb A. Interview. By Brett Frischmann. January 11, 2019.
Sieh, Kaleb August and Hatfield, Dale N., "The Broadband Internet Technical Advisory Group (BITAG) and Its Role in Internet Governance" (March 31, 2012). *2012 TPRC*. Available at SSRN: https://ssrn.com/abstract=2032233.
Simmel, Georg. "The Sociology of Secrecy and of Secret Societies." *American Journal of Sociology* 11, 441–498 (1906).
Solove, Daniel J. "Conceptualizing Privacy." *California Law Review* 90, 1087–1155 (2002).

Waldman, Ari Ezra. *Privacy As Trust: Information Privacy for an Information Age*. Cambridge, UK: Cambridge University Press, 2018.
Warren, Samuel and Louis D. Brandeis. "The Right to Privacy." *Harvard Law Review* 4, 193–220 (1890).
Westin, Alan. *Privacy and Freedom*. New York: Ig Publishing, 1967.
White, Howard B. "The Right to Privacy." *Social Research* 18, 171–202 (1951).
Williams, Michele. "In Whom We Trust: Group Membership as an Affective Context for Trust Development." *Academy of Management Review* 26, 377–396 (2001).