Ethics and Information Technology (2020) 22:211–222
https://doi.org/10.1007/s10676-020-09530-6

ORIGINAL PAPER

Privacy, transparency, and the prisoner's dilemma

Adam D. Moore[1] · **Sean Martin**[1]

Published online: 30 April 2020

Abstract
Aside from making a few weak, and hopefully widely shared claims about the value of privacy, transparency, and accountability, we will offer an argument for the protection of privacy based on individual self-interest and prudence. In large part, this argument will parallel considerations that arise in a prisoner's dilemma game. After briefly sketching an account of the value of privacy, transparency, and accountability, along with the salient features of a prisoner's dilemma games, a game-theory analysis will be offered. In a game where both players want privacy and to avoid transparency and the associated accountability, the dominant action will be to foist accountability and transparency on the other player while attempting to retain one's own privacy. Simply put, if both players have the ability or power to make the other more accountable and transparent, they will do so for the same reasons that player's defect in a prisoner's dilemma game. Ultimately this will lead to a sub-optimal outcome of too much accountability and transparency. While there are several plausible solutions to prisoner dilemma games, we will offer both technical, as well as, law and policy solutions. We need to change the payoffs of the game so that is it in everyone's interest to balance privacy and accountability rather than foisting transparency on others.

Keywords Privacy · Transparency · Prisoner's dilemma · Privacy rights · Unraveling problem

> 'It's too late. What kind of a world we'll have from now on, I don't know, I can't tell, but the world we know has been destroyed completely. Until now, every custom, every habit, every tiniest way of life has always taken a certain amount of privacy for granted, but that's all gone now.' He saluted each of the three with elaborate formality. 'You have created a new world among the three of you. I congratulate you. Happy goldfish bowl to you, to me, to everyone, and may each of you fry in hell forever.'[1]

Introduction

In Isaac Asimov's classic short story, "The Dead Past," a technological device called a "chronoscope" is invented which allows anyone to view the past, anyone's past, at any time, for any reason. In an odd twist, Asimov has the government suppressing the advancement and use of this technology to save humanity from itself. The goal of this suppression is to prevent a world in which "The housewife [will] take to watching her neighbor... the businessman will watch his competitor; the employer his employee... Every man his own peeping Tom and there'll be no getting away from the watcher." The problem is that in Asimov's story information about this technology is published—anyone who wishes can build and use a chronoscope.

Imagine that you were in possession of a chronoscope and could focus it on anyone. Suppose further that the device delivered complete, accurate, searchable, and detailed descriptions, in words, audio, and video, of the target's life. In a world where you controlled the only existing chronoscope, would you use it? What if only the powerful or politically connected possessed this technology? What if anyone could use this technology? Like Glaucon's wearer of the ring of Gyges, would you use the device to secure a life of privilege and comfort?[2] Leaving no travesty, slight, or temptation unexamined, would we fix our gaze on the past

✉ Adam D. Moore
moore2@u.washington.edu

[1] Information School, University of Washington, Mary Gates Hall, Ste 370, Box 352840, Seattle, WA 98195-2840, USA

[1] Isaac Asimov, "The Dead Past," *The Complete Stories*, Vol. 1 (Doubleday: Nightfall Inc. 1990), p. 40. See also, Arthur C. Clarke and Stephen Baxter's *The Light of Other Days* (New York: Tor Books, 2000).

[2] Plato, *Republic*, Bk. 2.

and succumb to the 'backward-looking' destruction of all privacy? Asimov, not typically known for advocating governmental paternalism, found an exception in this case.

While it is true that chronoscope technology is pure science fiction, we are inexorably moving toward something similar. The meta-data in our pictures shared across social networks is mined, geo-locational information collected from our smart phones track our movements, license-plate readers monitor the movements of cars, and our email messages are searched by governments and corporations. Video surveillance, facial-recognition technology, data-mining, financial surveillance, data-re-identification, not to mention predictive analytics, neuro-surveillance, and virtual frisking, each represent small steps toward a transparent society.[3] The tension between privacy and transparency has always been with us. The power to foist or demand transparency is, in part, the power to access locations and information about others. Moreover, transparency is obviously connected to accountability. Gathering information is a necessary condition for holding someone to account. To resist being transparent or accountable on grounds of privacy is to challenge the strength or existence of justified access demands.

Starting with Warren and Brandeis' 1890 article, "The Right to Privacy," there has been much analysis regarding the meaning, value, and scope, of privacy rights.[4] Moreover, in recent times the tensions between privacy, transparency, and accountability have been intensified by technology and the ascendency of the surveillance state. In this article, we hope to avoid most of the substantive disagreements about privacy, transparency, and accountability while providing a different sort of argument. No controversial assumptions about consequentialism, deontology, or virtues need to be advanced or defended. We will offer an argument for the protection of privacy, and thereby limit the scope of accountability, based on individual self-interest and prudence.

In a game where both players want privacy and to avoid transparency and the associated accountability, the dominant action will be to foist accountability and transparency on the other player while attempting to retain one's own privacy. Simply put, if both players have the ability or power to make the other more accountable and transparent, they will do so for the same reasons that players defect in a prisoner's dilemma game. Ultimately this will lead to a sub-optimal outcome of too much accountability and transparency—we have substantial incentives to undermine privacy. If only one player is given the power to foist accountability and transparency on the other, then rationality and prudence would dictate he or she do so. This is our current situation with respect to state, NSA, or corporate surveillance. A different real-world problem is when individuals relinquish their own privacy in order to obtain some benefit. Known as the "unraveling problem," in specific circumstances such incentives may lead individuals to give up all privacy. Finally, while there are several plausible solutions to prisoner dilemma games and the unraveling problem, we will offer both technical as well as law and policy solutions. We need to change the payoffs of the game so that is it in everyone's interest to balance privacy and accountability rather than foisting transparency on others.

Privacy, transparency, accountability: meaning and value

Privacy has been defined in many ways over the last century.[5] On our view, privacy is a *right* to control access to, and uses of, places, bodies, and personal information.[6] If

[3] Adam D. Moore, "Privacy, Neuroscience, and Neuro-Surveillance," *Res Publica*, 23, no. 2, 159–177. David Brin. *The Transparent Society*. New York: Perseus Books, 1998. David Lyon. *Surveillance Society: Monitoring Everyday Life*. Buckingham, UK: Open University Press, 2001. See also Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization," *UCLA Law Review*, 57, no. 6 (2009): 1701. Chris Jay Hoofnagle, "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement," *North Carolina Journal of International Law and Commercial Regulation*, 29 (2004): 595–637.

[4] Samuel D. Warren and Brandeis Louis, "The Right to Privacy," *The Harvard Law Review*, 4 (1890): 193–220.

[5] Parts of this section draw from Adam D. Moore, "Privacy: Its Meaning and Value," *American Philosophical Quarterly*, 40, no. 3 (2003): 215–227. For a rigorous analysis of the major accounts of privacy that have been offered, see Judith Wagner DeCew's *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology* (Ithaca, NY: Cornell University Press, 1997), chaps. 1–4; Adam D. Moore, "Defining Privacy," *Journal of Social Philosophy*, 39, no. 3 (Fall 2008): 411–228, and *Privacy Rights: Moral and Legal Foundations* (University Park: Pennsylvania State University Press, 2010), chaps. 2–3.

[6] Viewing privacy as a "condition that obtains or not" is not a defensible account on our view. Consider how simple advancements in technology change this condition. What we care about is not if some condition obtains, but rather if we have a right that such a condition obtains. You may be able to use your x-ray device to look into private areas. The question is not a matter of "can," it is a matter of "should." Moreover, it is important to clarify the importance of privacy and accountability because it is this analysis that leads to the prisoner's dilemma problem. For example, if privacy were simply nothing more than a mere subjective preference, if we are wrong about why privacy in morally valuable in the following section, then having no privacy could not be modeled as a suboptimal outcome within a prisoner's dilemma. For a defense of this account of privacy see Adam D. Moore, "Privacy: Its Meaning and Value," *American Philosophical Quarterly* 40, no. 3 (2003): 215–227, "Defining Privacy," *Journal of Social Philosophy* 39, no. 3 (Fall 2008): 411–428, and *Privacy Rights: Moral and Legal Foundations* (University Park: Pennsylvania State University Press, 2010), chaps. 2–3.

access is granted accidentally or otherwise, it does not follow that any subsequent use, manipulation, or sale of the good in question is justified. Similarly, allowing you access to my poem is not also a waiving of all downstream moral and legal claims over the poem. In this way, privacy is both a shield that affords control over access or inaccessibility and a kind of use and control right that yields justified authority over specific items—such as a room or personal information.

Finally, many privacy theorists argue that privacy is morally valuable because it is associated, in some central way, to autonomy and respect for persons.[7] Our view is that privacy is essential for human well-being or flourishing and linked to autonomy in obvious ways.[8]

In the typical case, transparency and privacy appear to be opposites. If transparency holds, then there is no privacy. Alternatively, if privacy holds, then transparency does not. Thus, we can understand transparency as a condition of open, unrestricted, perceptual access to information, data, or knowledge. A normative definition might run as follows. A right to transparency is a right that justifies perceptual access to information, data, or knowledge. Accountability and transparency are closely connected. For example, the reason democratic societies champion governmental *transparency* is precisely because citizens want to hold those in power to account.[9] If we had the power or ability to access information about governments, corporations, or other individuals, this would, in the typical case, allow us to make better decisions related to self-government. Moreover, if we had the right to access information about governments, corporations, or other individuals, this right would be beneficial for establishing and promoting the appropriate capacities or abilities for self-government.[10]

Assuming these definitions are correct and that individuals value privacy, accountability, and transparency, we are now in a position to analyze a privacy-based prisoner's dilemma game.

The privacy game

Imagine a game with two players, Fred and Ginger where neither has any outstanding obligations with respect to the other.[11] Both have the choice to make the other player transparent by using Asimov's chronoscope. The information disclosed by the chronoscope, if used, is only available to Fred and Ginger. Moreover, for each player this is a one-time choice. Additionally, nothing hinges on the existence of chronoscope technology. Suppose Fred and Ginger are two ex-lovers locked in a custody case fighting over the kids. Both are competent at deploying various commonly used surveillance technologies so that each can "get the goods" on the other. Neither are "saints." This would be a single play, 2-person, PD. Bonnie and Clyde, two rivals, are going after the same promotion at work. One or the other will get the promotion and both have bosses (or friends in HR) who will disclose why they did or did not get the job. Both could deploy surveillance technologies to get "dirt" on the other. Both could anonymously publish this information so that company bosses will find it... etc. (a single play, 2-person PD). Now imagine 10 rival workers... (a multi-player PD). Now imagine 10 players and more than one promotion opening (a multi-player, iterated PD). With modifications, our view is that a similar analysis would apply to these cases. Consider the following table.

[7] S.I. Benn, "Privacy, Freedom, and Respect for Persons," in Pennock, R. and Chapman, J. (eds.), *Privacy Nomos XIII* (New York: Atherton, 1971), pp. 1–26; Rachels, J. "Why Privacy is Important," *Philosophy and Public Affairs*, 4 (1975) 323–333; Reiman, J. "Privacy, Intimacy, and Personhood," *Philosophy and Public Affairs*, 6 (1976), 26–44; J. Kupfer, "Privacy, Autonomy, and Self-Concept," *American Philosophical Quarterly*, 24 (1987), 81–89; J. Inness, *Privacy, Intimacy, and Isolation* (New York: Oxford University Press, 1992); B. Rössler, *The Value of Privacy*. Trans. Rupert D. V. Glasgow (Cambridge: Polity Press, 2005).

[8] See the sources cited in note 5. See also, Bryce Newell, Cheryl Metoyer, and Adam D. Moore, "Privacy in the Family," in *The Social Dimensions of Privacy*, edited by Beate Roessler and Dorota Mokrosinska (2015).

[9] For example, see Andreas Schedler, Larry Jay, and Marc F. Plattner, *The Self-Restraining State: Power and Accountability in New Democracies* (Boulder, CO: Lynne Rienner Publishers, 1999); Kay Mathiesen, "Transparency for Democracy: The Case of Open Government Data," in Adam D. Moore, *Privacy, Security, and Accountability: Ethics, Law, and Policy*, edited by A. Moore (Rowman & Littlefield International), December 2015), chap. 7; Nadine Strossen, "Post-9/11 Government Surveillance, Suppression, and Secrecy," in Adam D. Moore, *Privacy, Security, and Accountability: Ethics, Law, and Policy*, edited by A. Moore (Rowman & Littlefield International, December 2015), chap. 12.

[10] For a general analysis of trust and accountability see Onora O'Neill, "Reith Lectures 2002: A Question of Trust," https://immagic.com/eLibrary/ARCHIVES/GENERAL/BBC_UK/B020000O.pdf (last visited 04/29/2020).

[11] For example, they are not spouses, or Fred is not a police officer and Ginger is not a suspect. Also, as with the traditional prisoner's dilemma game, moral norms, promises, and the like, play no central role in the analysis. For example, players may make agreements and the like, but this will not alter what is rational and prudent within the game.

		Ginger's choices: use chronoscope	Ginger's choices: don't use chronoscope
Fred's choices: use chronoscope		bad / bad	worst / best
Fred's choices: don't use chronoscope		best / worst	okay / okay

best > okay > bad > worst

Given that Fred and Ginger are, more or less, equal and both are narrowly self-interested and rationally prudent, the best outcome for Fred is one where he makes Ginger's past transparent while retaining his own privacy (i.e. Ginger does not use her chronoscope). Remember the chronoscope delivers complete, accurate, searchable, and detailed descriptions, in words, audio, and video, of the target's life. This option is the worst case for Ginger. Fred loses no privacy, so he is no worse-off than if he had not played the game. Fred will also obtain a positional advantage over Ginger going forward given that he would be able to use the information provided by the chronoscope to his advantage. Moreover, Ginger incurs numerous risks. Fred could use Ginger's chronoscope information to disadvantage her directly, but he may also sell this information to others or simply leave it unsecured.

Assuming that privacy is valuable, from the moment Fred uses the chronoscope back to the moment she was born, Ginger would have no privacy or be at serious risk of having no privacy. Moreover, modern predictive analytics, neuro-surveillance, de-anonymization, along with a host of other technologies could be used to manipulate, control, or nudge Ginger.[12] While it is true that the near perfect information the chronoscope provides others may afford Ginger benefits in some cases, the threats are also relevant and independent of her control. Given that Ginger does not know if Fred is a saint, villain, or anything in-between, she would most likely, on grounds of rational self-interest and prudence, assume the worst and act accordingly. To protect herself from the mischief Fred might do, Ginger is virtually forced to deploy the chronoscope against Fred. If Fred uses the chronoscope and Ginger does not, it is as if there is a loaded gun pointed at Ginger and controlled by Fred. Using the chronoscope herself allows Ginger to point a gun back at Fred. Wondering about the other, both Fred and Ginger comb through the information about the other to take measure and see what sorts of risks are relevant. They also search for sensitive information to threaten the other player as to not be put at a positional disadvantage. Thus, we arrive at the sub-optimal outcome where both Fred and Ginger have no privacy and incur risks of manipulation, control, or physical harm. Finally, both realize that the best option in a collective sense, the option that yields the be outcome for both players, is where neither use the chronoscope given that neither is accountable to the other.

The privacy game just described takes the form of a prisoner's dilemma. The classic version of a prisoner's dilemma game begins with two individuals and two choices.[13] Adam and Eve are picked up by the police and charged with robbing a bank. Each are given the choice of ratting on the other or staying silent. If Adam rats on Eve and she remains silent, he is set free and she gets life in prison. If Eve rats on Adam while he remains silent, then she is set free while he gets life in prison. If both rat on each other, then both get 20 years in jail. Finally, if both stay silent, then each will receive 1 year in jail.

		Eve's choices: Rat	Eve's choices: Stay Silent
Adam's choices: Rat		10 years / 10 years	Life / Freedom
Adam's choices: Stay Silent		Freedom / Life	1 year / 1 year

Both Adam and Eve prefer freedom to 1 year, 1 year to 10 years, and 10 years to life in prison. Given the structure, payoffs, and preferences, the option of "ratting" dominates over the option of "staying silent." That is, no matter what the other player does it is always better to rat. Eve would reason the following way: "Suppose Adam rats, then I will do

[12] Alas, there is a reason many online services are "free." When some online service is offered for "free" the chances are it is your data that is being used as payment.

[13] See, Robert Axelrod, "The Emergence of Cooperation Among Egoists," *The American Political Science Review* 75 (1981): 306–318; Robert Axelrod, *The Evolution of Cooperation* (New York: Basic Books, 1984); and Brian Skyrms, *The Dynamics of Rational Deliberation* (Cambridge, MA: Harvard University Press, 1990).

better to rat as well and avoid the sentence of life in prison. Suppose Adam stays silent, then I will do better if I rat and attain freedom. In either case, ratting is better." Of course, Adam is engaging in the same sort of reasoning and thus both are driven to a sub-optimal outcome—10 years for each of them. Both will rat. The lesson of such a game is that prudentially rational self-interested players will end up with sub-optimal outcomes.[14] Collectively, however, both would do better if each remained silent. If Adam and Eve could just cooperate, then they could each avoid the harsh result of spending 20 years in prison—this option yields what economists call Pareto optimality.[15] What is individually rational may well be collectively irrational.

Prisoner's dilemma games can also be played between two players numerous times. Imagine that Adam and Eve were going to play an iterated prisoner's dilemma game with no known end point. They might play 10 rounds or 100 rounds of the game. In this sort of game, when both can reasonably guess that the game will continue for some time, strategies like tit-for-tat dominate.[16] A tit-for-tat strategy starts off with cooperation (non-ratting) and then imitates the opponent's previous move in subsequent rounds. The problem is that if either player guesses the game end is near, defection or ratting becomes the dominant strategy once again. Defection, or threat of defection, late in the game pressures players to not cooperate earlier in the game.[17]

Unlike a prisoner's dilemma, an iterated *privacy game* does not appear to promote tit-for-tat as a dominant strategy. Unless there is lots of useful information captured between rounds, the advantages of using a chronoscope as punishment for past transgressions is limited. If Fred uses the chronoscope in the first round against Ginger, he won't gain much more information if he chooses to use the chronoscope in the second round. Thus, in an iterated privacy game of unknown length players would likely use the chronoscope (rat) early in the game and insure themselves against future uses of the chronoscope (defections) by the other player. There may also be good reasons to use the device in later rounds to determine if the other player is using the information provided by the chronoscope to obtain an advantage.

Rather than a two-person game, consider a multi-player game with an unknown number of counterparts. In this version of the game, if only one person rats, then that person is set free while all the others get life in prison. If more than one player rats, then those that rat get 20 years while those that remain silent get life in prison. Finally, if everyone remains silent, then 1 year in prison is the sentence for each player. As with the single-player version of the prisoner's dilemma game, the option of ratting dominates over staying silent. Again, what is individually rational yields a collectively sub-optimal outcome.

The tragedy of the commons can be modeled as a multi-player prisoner's dilemma game.[18] Garret Hardin writes,

> If a pasture becomes a commons open to all, the right of each to use it may not be matched by a corresponding responsibility to protect it. Asking everyone to use it with discretion will hardly do, for the considerate herdsman who refrains from overloading the commons suffers more than a selfish one who says his needs are greater. If everyone would restrain himself, all would be well; but it takes only one less than everyone to ruin a system of voluntary restraint. In a crowded world of less than perfect human beings, mutual ruin is inevitable if there are no controls. This is the tragedy of the commons.[19]

In this sort of example, a value will be destroyed if it is overused. Adding in one or two extra sheep will benefit me at only a slight cost to others who use the commons. The result of each herder thinking this way is overgrazing and the destruction of the commons. Admittedly, some overgrazing

[14] Thus, ratting is said to dominate staying silent and is a *Nash equilibrium*. "A Nash equilibrium is any profile of strategies—one for each player—in which each player's strategy is a best reply to the strategies of the other players." Ken Binmore, "Why all the Fuss? The Many Aspects of the Prisoner's Dilemma," in M. Peterson (ed.) *The Prisoner's Dilemma: Classical and Philosophical Arguments*, vol. 20 (Cambridge: Cambridge University Press, 2015), pp. 16–34.

[15] Pareto conditions are named after Vilfredo Pareto (1848–1923) an Italian economist and sociologist.

[16] See, Axelrod, "The Emergence of Cooperation Among Egoists;" and Axelrod, *The Evolution of Cooperation* (Basic Books, 1984). For indefinitely repeated prisoner's dilemma games tit-for-tat is a Nash equilibrium.

[17] Pettit and Sugden offer a critique of this argument. See, Phillip Pettit and Robert Sugden, "The Backward Induction Paradox," *Journal of Philosophy*, 86 (1989): 169–182. While the backward induction argument has been challenged in two-person iterated prisoner's dilemmas with no known end point, it is not clear that such considerations hold in multi-player iterated prisoner's dilemmas.

[18] Garret Hardin, "The Tragedy of the Commons," *Science* 162 (December 13, 1968): 1243–1248. See also, R. M. Dawes, "Formal Models of Dilemmas in Social Decision Making," in M. F. Kaplan and S. Schwartz (eds.), *Human Judgement and Decision Processes: Formal and Mathematical Approaches* (New York: Academic Press, 1975), pp. 87–108; Xin Yao and Paul J. Darwen, "An Experimental Study of N-Person Iterated Prisoner's Dilemma Games," 18 *Informatica,* 435–450 (1994); and Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action,* (1994). Others have modeled public goods problems, like the tragedy of the commons, as assurance, chicken, or voting games. See Luc Bovens, "The Tragedy of the Commons as a Voting Game," pp. 156–176 and Geoffrey Brennan and Michael Brooks, "The Role of Numbers in Prisoner's Dilemmas and Public Good Situations," in M. Peterson (ed.) *The Prisoner's Dilemma: Classical and Philosophical Arguments* (Cambridge: Cambridge University Press, 2015), pp. 177–198.

[19] Garret Hardin, "Lifeboat Ethics: The Case Against Helping the Poor," *Psychology Today* (September. 1974).

is within the carrying capacity of the typical commons. Nevertheless, there will be some amount of overuse that cannot be sustained. Once this point is reached, overgrazing will ensure the destruction of this common resource. As with the two-person version of a prisoner's dilemma game, there appears to be a dominant action. Each player would do better by overusing the commons no matter what the other players do.[20] Individuals acting prudentially lead to a collective tragedy.

A multi-player privacy game also leads to a collectively sub-optimal outcome although it takes a bit of tinkering with the example. As before, use of the chronoscope delivers complete, accurate, and searchable detailed descriptions, in words, audio, and video, of each player's life. After the game and if the chronoscope is used and assuming no little cost in time or money, a player would know exactly how many others players were involved in the game. As with the two-person game and for the same reasons, the dominant strategy would be use the chronoscope.

Like the iterated version of the two-person game, a multi-player iterated version of the privacy game yields the surprising conclusion that strategies like tit-for-tat fail. As before, assuming there is minimal new information generated between rounds for the players, use of the chronoscope early in the various games would seem to be required just in case the game ends. Moreover, if the game continues, repeated uses of the chronoscope would be rational so that players could determine who had deployed the device and if they had used relevant information provided by the chronoscope against various players.[21] Note we are assuming that chronoscope users will be able to identify if another player has used the device—covert use is impossible. Importantly, outside of this example, current uses of surveillance technology do not have this feature. We are also assuming that the chronoscope device is impossible to defeat. There can be no anti-chronoscope privacy shield developed.

Note how these considerations make a real-life iterated version of the privacy game more risky. If a player does not know how many other players there are or who is watching, then prudence would dictate watching everyone. At least obtaining the chronoscope reports on everyone, but perhaps not actually analyzing them, would allow for risk mitigation and potential benefits downstream. Moreover, if anti-chronoscope technology is developed or possible, then securing these reports would ensure that players have a level playing field.

Given that in our original two-person privacy game Fred and Ginger could be individuals, corporations, states, or other groups, and that in multi-player iterated versions of the game all of these entities could be playing against each other, the complexity of the problem space should be obvious. In each instance, rational self-interested players would do best by making the other players transparent. Used as an insurance policy against future violations, a means to discover what sort of risks one is subject to, or as a tool that facilitates predatory activity, players will find it rational to use the chronoscope and this will ensure a sub-optimal outcome.

Privacy in the wild and the unraveling problem

Moving from thought experiments about how and why players might use a chronoscope device in two-player, iterated, and multi-player privacy games, to actual cases in the real world, it becomes even more obvious how privacy is under threat. As already noted, unlike the cases so far, the privacy game we are playing in the real world includes covert monitoring. We simply do not know the players, risks, and types of surveillance being used to foist transparency and accountability on unsuspecting players. Moreover, individuals, corporations, and to some extent states, trade their own privacy away for other values. Individuals, corporations, and states are happy to gather and then sell the private information about others. We discount future risks of privacy intrusions and manipulation for the immediacy of some value or good wanted currently. Finally, we are happy to give away private information to secure advantages in many competitive situations.

Unlike the classic prisoner's dilemma where there is essentially only one value in play, our game includes other values like security, transparency or accountability, as well as more mundane values like food, shelter, health benefits, or even faster online content consumption.[22] For example, we each engage in utility calculations and trade private information for store loyalty "club prices" at the market. This sort of pattern repeats itself across all of our different values.

[20] For a rich discussion of these issues, see Michael Taylor, *The Possibility of Cooperation* (Cambridge: Cambridge University Press, 1987); and Phillip Pettit, "Free Riding and Foul Dealing," *Journal of Philosophy*, 83 (1986): 361–379.

[21] For an interesting analysis of multi-player iterated prisoner's dilemmas see Xin Yao and Paul J. Darwen, "An Experimental Study of N-Person Iterated Prisoner's Dilemma Games," *Informatica*, 18 (1994): 435–450.

[22] See Michael Froomkin, "The Death of Privacy," Adam Moore, ""Privacy, Security, and Government Surveillance: WikiLeaks and the New Accountability," *Public Affairs Quarterly*, 25 (April 2011): 141–156; and Mike Katell and Adam Moore, "The Value of Privacy, Security, and Accountability," in *Privacy, Security, and Accountability*, edited by A. Moore (Rowman & Littlefield International, December 2015), pp. 1–17.

Unraveling privacy

Consider the case where two individuals are competing for a job. Bonnie and Clyde are two job seekers who are, all things considered, equally talented. In this game both want a job most of all and the best possible payoff for any player would be to get the job and to retain privacy. Given the structure of the game this is not possible. When players are in a competitive situation and notice that revealing more private information or allowing invasive monitoring would likely yield an advantage, the best payoff for any player would be to get the job but lose privacy (1 Job, 0 Privacy). The second-best outcome is one where both players refuse to reveal private information or allow themselves to be invasively monitored. In this case, neither player would have a competitive advantage and both would have a 50% chance at getting the job (0.5 Job, 1 Privacy). The next best outcome is where both players give up privacy yielding neither an advantage. Both have lost privacy but still retain a 50% chance at getting the job (0.5 Job/ 0 Privacy). Finally, the worst outcome mirrors the payoff for the best outcome. While the job-seeker retains privacy she/he does not get the job (0 Job, 1 Privacy).

Bonnie's choices

Clyde's choices	Reveal	~Reveal
Reveal	.5 Job, 0 Privacy .5 Job, 0 Privacy	0 Job, 0 Privacy 1 Job, -Privacy
~Reveal	1 Job, 0 Privacy 0 Job, 1 Privacy	.5 Job, 1 Privacy .5 Job, 1 Privacy

Job/-Pri > .5 Job/Pri > .5 Job/-Pri > -Job/Pri

When individuals don't think privacy is worth much and jobs are scarce and needed, individuals playing this game, like Clyde, would likely reason the following way. "Allowing my employer to know more about me during the hiring process will likely allow them to minimize risk and make a good hiring decision. If I also agree that my employer may monitor my activities during work hours and off-work hours, I will likely have a competitive advantage compared to Bonnie in the case that she does not reveal. If we both give up privacy, then neither will have the advantage. If I retain privacy while Bonnie does not, then I will be at a competitive disadvantage. So, no matter what Bonnie does, it is always best for me to give up privacy." The problem should be obvious. Bonnie will reason the same way and privacy will be unraveled. Also note, that with more players there would be a lower probability of getting the job. For example, with 10 roughly equal players the chance of getting the job when everyone reveals or fails to reveal would be 10%. This would make the sub-optimal outcome even worse.

The tendency toward allowing intrusions into one's privacy is further strengthened by how others perceive someone who refuses to allow the intrusion. Because some give up their privacy, others assume that those who do not reveal certain information about themselves have negative information to hide. This affects everyone, starting from those with higher quality information and eventually covering those with lower quality information. By higher and lower quality information, we mean information that would be looked upon favorably by the one evaluating it.

There are many modern environments in which agents are incentivized to give up their privacy.[23] As pointed out by Scott R. Peppet's "Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future," some individuals disclosing personal information can penalize those who wish for his or her information to remain private.[24] As modeled above, such encounters can also be understood as a prisoner's dilemma. In such cases, all individuals may be forced to reveal personal information, regardless of whether the revelation is beneficial to them or whether they desire to reveal it. Generally, the problem

[23] It is also the true that sometimes the costs of unraveling outweigh any benefits in some cases. For example, the costs of disclosing past bad actions or assault related to the #MeToo movement would likely outweigh whatever benefits would be available. Thanks to Ofer Engel for this suggestion.

[24] Scott Peppet, "Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future," *Northwestern University Law Review* 105 (2011): 1153-1204. See also, Anita Allen, *Unpopular Privacy: What Must We Hide?* (Oxford: Oxford University Press, 2011).

of unraveling can be laid out the following way. Candidates with the best information to reveal will disclose first, since they know that they will have advantages over their competition. After the first candidates disclose, the candidates in the best position to disclose will be those with the next best information, who will want to distinguish themselves from the rest. Next, the candidates with the third best information will reveal, and so on. This pressure forces those who did not want to disclose to do so anyway.[25] This process results in a state where an agent must give up privacy in order to avoid a penalty and is an illustration of Robert Frank's Full Disclosure Principle: "if some individuals stand to benefit by revealing a favorable value of some trait, others will be forced to disclose their less favorable values."[26]

It's important to note that individual choice will still be the final gatekeeper. Privacy unraveling will not necessarily lead to individuals divulging personal information. What the process does do, however, is put increasing pressure on those who do not reveal as the game progresses. Let's say a job candidate is supremely qualified and, if she revealed everything about herself, would be found to be the ideal candidate. To distinguish herself from those with less perfect credentials she has everything to gain and little to lose by revealing. Suppose, however, she chooses not to reveal. If her competitor with slightly less perfect information reveals, then the employer has to make a choice between a known employee who has revealed and one who has not. As other candidates decide to reveal, and assuming that some of them are "above the hiring bar," our ideal candidate looks worse and worse to the prospective employer. Not wanting to risk hiring a bad candidate the employer would almost certainly hire the best of those who revealed. This is bad for the ideal candidate who would have gotten the job and the employer who would have hired the very best candidate. What happens, on the other hand, is that the desire to get the job or promotion pressures individuals to unravel and this yields a sub-optimal result for those caught in this dilemma.

Re-statement of the problem

Given the preceding, it looks like privacy and accountability are in trouble. Modeled as a prisoner's dilemma we each have prudential and self-interested reasons to watch, record, and analyze the activities of other individuals, corporations, groups, or states. We don't value privacy enough and don't appreciate the ways we may be controlled, manipulated, or nudged by those who gather and use this information. In the balance between privacy and accountability we each want to hold others transparent while avoiding accountability ourselves. At odds with these considerations, are cases where individuals are willing to trade almost any amount of privacy for use of a search engine, smartphone, or a promotion at work. In these latter cases, the lure of what might be called "shiny objects" or the desire for immediate gratification, tempts us to forget about privacy and accountability.

Solutions: the way out of the privacy prisoner's dilemma and unraveling

Working backwards from the unraveling problem to the privacy prisoner's dilemma, we will defend several different solutions to these worries.[27] As it ends up, the unraveling problem is rather weak and there are several compelling solutions to the privacy prisoner's dilemma.

First, the strength of the unraveling problem may be challenged. Information Saints, as well as individuals from other levels, may simply refuse to share and forgo the benefits because of privacy norms.[28] As noted in Peppet's article, Richard Posner "gives the example of the market for physical attractiveness. Beautiful people have an obvious incentive to reveal their attractiveness by wearing little or no clothing whenever possible. In an unraveling of sorts, those who remain covered should be assumed to be less desirable. In equilibrium, everyone should become a nudist."[29]

[25] Scott Peppet, "Unraveling Privacy," p. 1181.

[26] Robert H. Frank, *Passions within Reason*, (1988), p. 104. For an interesting analysis of signaling, information transfer, competitive games see Justin P. Bruner, "Disclosure and Information Transfer in Signaling Games, *Philosophy of Science*, 82 (2015): 649–666.

[27] Elinor Ostrom notes "… the classic models have been used to view those who are involved in a Prisoner's dilemma game or other social dilemmas as always trapped in the situation without capabilities to change the structure themselves. This analytical step was a retrogressive step in the theories used to analyze the human condition. Whether or not the individuals who are in a situation have capacities to transform the external variables affecting their own situation varies dramatically from one situation to the next." Elinor Ostrom, "Beyond Markets and States: Polycentric Governance of Complex Economic Systems," Nobel Prize lecture (December 8, 2009): 416.

[28] Peppet notes "Not all information markets unravel. Instead, unraveling is limited by transaction costs, ignorance of desired information, inability to accurately make negative inferences, and social norms." Scott Peppet, "Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future," (2011): 1191. See also, Annamaria Nese, Niall O'Higgins, Patrizia Sbriglia, and Maurizio Scudiero, "Cooperation, Punishment and Organized Crime: A Lab-in-the-Field Experiment in Southern Italy," *IZA Discussion Papers* 9901 (2016) https://www.econstor.eu/bitstream/10419/142340/1/dp9901.pdf. Nese et all note the norms adopted by various groups affect the willingness of players to cooperate or defect. "Camorra prisoners show a high degree of cooperativeness and a strong tendency to punish, as well as a clear rejection of the imposition of external rules even at significant cost to themselves . . . a strong sense of self-determination and reciprocity both imply a higher propensity to cooperate and to punish . . ." p. 2.

[29] Scott Peppet, "Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future," (2011): 1196.

Obviously, this is not the case. Other norms may also work to stop unraveling.[30]

Moreover, individuals who have the means to resist—where getting the promotion or service is not all that important—may do so despite the incentives to reveal.[31] If there are enough defections from unraveling at different levels, then the assumption that those who don't disclose are in the worst group is undermined.[32] Additionally, there is some evidence that those who reveal information about their past bad behavior become biased against individuals with similar information. An odd experimental result "finds a correlation between propensity to disclose sensitive information on social media sites and negative attitudes towards other disclosers: participants who shared information online about past questionable behaviors judged more harshly others who had made similar disclosures, compared to participants who did not share such information."[33] Avoiding this bias would give all parties a reason to refrain from disclosing such information.

Transaction costs may also prevent unraveling.[34] Gathering verified information into a digital prospectus may be costly and time consuming. If the costs of this activity are more than the benefits of unraveling, then individuals would not create or maintain such digital profiles. Additionally, the receiver of such information must have the time and inclination to process and analyze the digital profile. If the costs of processing and analyzing information disclosed by individuals who unravel is more than the benefits secured, then there would be no incentive to engaged in such activity. Moreover, if storing and maintaining these profiles were risky or if the individuals sending these signals insisted on limited use, no transfer, and the like, then those receiving these profiles may have incentives for not retaining the information. As discussed below, if there are legal limits placed on the acquisition, use, and transfer of personal information, then privacy unraveling may be stopped.

Finally, we can question the moral strength of individual consent in unraveling situations.[35] If consent is offered under certain conditions—assume that there are lots of jobs and few workers or that a specific type of surveillance is necessary for doing business—then privacy claims may be justifiably waived. If you know that no one else has disclosed private information, but you do, then the waiver seems permitted. When conditions do not favor the employee—suppose there are lots of workers and no jobs—and the monitoring is unnecessary, counterproductive, and violates a basic right, then we should proceed with caution.[36] It is not so clear that in this latter case consent is sufficient for waving privacy rights. In a case of unraveling, when someone is forced to relinquish privacy because others have done so and getting the job is gravely important, it is unclear that individual consent to disclose would retain moral force.

Turning to the privacy prisoner's dilemma and our Asimov case, one solution would be to only play with individuals that you can trust. Imagine that Fred and Ginger are known privacy rights champions and would never look beyond what is minimally required. By being a known privacy champion, we can choose to play accordingly and thus collectively avoid the sub-optimal outcome of always watching and recording.[37] While counterintuitive, we each obtain more privacy by disclosing our past practices of respecting the privacy rights of others. Individuals, companies, and even states could be certified as 'privacy respecting' entities.[38] In communities where privacy is understood as a

[30] In working environments unionization may provide a way out of the unraveling problem. This idea was suggested by Ofer Engel at the Information Ethics Roundtable, Copenhagen 2018. See Simon Head, "Big Brother Goes Digital, The New York Review of Books, May 24, 2018, https://www.nybooks.com/articles/2018/05/24/big-brother-goes-digital/#fn-11 (last visited 10/02/2018). Note that this solution will not work in other areas where unraveling occurs.

[31] For example, Benndorf and Normann note that some individuals simply refuse to sell personal information for various reasons. Volker Benndorf and Hans-Theo Normann, "The Willingness to Sell Personal Data," *Scandinavian Journal of Economics* (April 2017). See also, Volker Benndorf and Hans-Theo Normann, "Privacy Concerns, Voluntary Disclosure of Information, and Unraveling: An Experiment," *European Economic Review* 75 (2015): 43–59. In this latter paper the authors note that unraveling occurred less than what was predicted.

[32] See Ginger Jin, Michael Luca, and Daniel Martin, "Is No News (Perceived) Bad News? An Experimental Investigation of Information Disclosure," Working Paper. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2591450 (last visited 04/29/2020). Jin et al argue that information senders reveal less than what is expected and information receivers don't assume the worst of those who don't reveal.

[33] See Laura Brandimarte, Alessandro Acquisti, and Francesca Gino, "A Disclosure Paradox: Can Revealing Sensitive Information Make us Harsher Judges of Others' Sensitive Disclosures?" Working Paper, https://mis.eller.arizona.edu/sites/mis/files/documents/events/2015/mis_speakers_series_laura_brandimarte.pdf (last visited 01/17/18).

[34] See Justin P. Bruner, "Disclosure and Information Transfer in Signaling Games, *Philosophy of Science* 82 (2015): 649–666.

[35] For an analysis of consent related to employee privacy see Adam D. Moore, "Drug Testing and Privacy in the Workplace," *The John Marshall Journal of Computer & Information Law*, 29 (2012): 463–492 and "Employee Monitoring & Computer Technology: Evaluative Surveillance v. Privacy," *Business Ethics Quarterly*, 10 (2000): 697–709.

[36] GDPR, Article 7/Recital 43 states explicitly that consent "should not provide a valid legal ground" when there is a clear imbalance between the parties. While this example is about a "data controller" who is also a public authority, the general idea is welcome. Thanks to Ofer Engel for this citation.

[37] See David Gauthier, *Morals by Agreement* (Oxford: Clarendon Press, 1986).

[38] For example see TrustArc's Privacy Assessments and Certifications program. https://www.trustarc.com/products/certifications/ (last visited 04/29/2020).

fundamental right those who watch too much or those who try to secure a competitive advantage by violating privacy norms, may find themselves isolated or ostracized.

In a prisoner's dilemma situation players who have the option to exit the encounter and play with someone else, will do so if the current game yields poor payoffs. When Ginger learns that Fred used the chronoscope she will seek new partners or simply will not play. Players given the right to exit are more likely to cooperate.[39] Additionally, games that are being monitored by other potential players lead to more corporation within these games. This is where accountability, in part, gets its value. Ginger does not need to know everything about Fred. All she needs to know is if he has respected her privacy or not. If not, she will seek new partners who do respect privacy norms. Finally, if it becomes known that Fred is a non-cooperator, he is the sort of person who will use the chronoscope, then those who value privacy will refuse to play with him.

Consider the 'real life' example of employee monitoring. Businesses that use various covert and overt surveillance techniques tend to have higher employee turnover.[40] For example, drug testing deters highly qualified workers from applying, has a negative impact on workplace morale, diverts funds from drug treatment programs, and has been indicated in reduced productivity.[41] "Companies that relate to employees positively with a high degree of trust are able to obtain more effort and loyalty in return. Drug testing, particularly without probable cause, seems to imply lack of trust."[42] Additionally, it has been found that employees view electronic monitoring as harmful intrusions of privacy and this perception increases aggression and destructive behavior.[43] Invasive computer surveillance leads to increased computer abuse. Finally, when electronic monitoring is imposed, perhaps along with higher pay, employees view these intrusions negatively and rate their employers as ethically poor.[44] In turn, such perceptions lead employees to seek better job prospects.

Another possibility would be to change the payoffs of the game. For example, imagine that a government, or Hobbes' Leviathan, would penalize individuals who acted out of prudence or narrow self-interest. Suppose that in the two-person version of this scenario, a payoff of freedom would come with weekly severe beatings. In this case, prudence and self-interest would lead toward silence and a collectively optimal solution. In multi-player games, like Hardin's tragedy of the commons, the Leviathan could simply penalize those who overuse shared resources. Hardin's own solution to the tragedy of the commons was to assign property rights along with corresponding legal obligations and privileges. By setting up institutions of private property, the negative consequences of overuse could be internalized to those who own the land. Imagine we treated informational privacy as a kind of property right like copyright. Allowing others access to personal information would not also entail abandonment of downstream control over this information. Similarly, allowing you access to my copyrighted poem does not invalidate my copyrights. Using the chronoscope without consent from other player(s) in a single play game or an iterated multi-player game would violate a property right and, perhaps, incur various penalties.

To solve the privacy prisoner's dilemma we could enact laws or adopt legislation that prohibit or limit the gathering or use of private information. For example, the European Union's rules on notice and consent are a welcome step in the right direction.[45]

> [P]ersonal data may be processed only if: (a) the data subject has unambiguously given his consent. (Article 7 of Directive No. 46/1996).

[39] Charles Holt, Cathleen Johnson, and David Schmidtz, *Prisoner's Dilemma Experiments*, in M. Peterson (ed) The Prisoner's Dilemma: Classical and Philosophical Arguments (Cambridge University Press, 2015), pp. 243–264.

[40] ". . . the use of monitoring for control purposes will have dysfunctional consequences for both employees (lower job satisfaction) and the organization (higher turnover)." John Chalykoff and Thomas Kochan, Computer-Aided Monitoring: Its Influence on Employee Job Satisfaction and Turnover," *Personnel Psychology: A Journal of Applied Research*, 42 (1989): 826, 807–834. See also, Roland Kidwell Jr. and Nathan Bennett, "Employee Reactions to Electronic Control Systems," *Group & Organization Management*, 19 (1994): 203–218.

[41] Lewis Maltby, "Drug Testing: A Bad Investment," ACLU Report (1999), pp. 16–21.

[42] Edward Shepard and Thomas Clifton, "Drug Testing: Does It Really Improve Labor Productivity?" *Working USA*, November–December 1998, p. 76.

[43] Clay Posey, Rebecca Bennett, Tom Roberts, and Paul Lowry, "When Computer Monitoring Backfires: Invasion of Privacy and Organizational Injustice as Precursors to Computer Abuse," *Journal of Information System Security* 7 (2011): 24–47. See also R. Irving, C. Higgins, and F. Safayeni, "Computerzed Performance Monitoring Systems: Use and Abuse," *Communications of the ACM*, 29 (1986): 794–801 and J. Lund, "Electronic Performance Monitoring: A Review of Research Issues," *Applied Ergonomics*, 23 (1992): 54–58. Whereas Irving et al found that electronic monitoring caused employees to report higher stress levels Lund found that such policies caused anxiety, anger, depression and a perceived loss of dignity. See also National Workrights Institute, "Electronic Monitoring: A Poor Solution to Management Problems" (2017), https://www.workrights.org/nwi_privacy_comp_monitoring_poor_solution.html (last visited 04/29/2020).

[44] Matthew Holt, Bradley Lang, and Steve G. Sutton, "Potential Employees' Ethical Perceptions of Active Monitoring: The Dark Side of Data Analytics," *Journal of Information Systems: Summer*, 31 (2017): 107–124.

[45] See also, the California Consumer Privacy Act (CCPA), https://oag.ca.gov/privacy/ccpa.

> [T]he subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. (Article 5/3 of Directive No. 58/2002).
>
> Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing by the data controller. (Directive No. 2009/136/EC)

The new 2018 General Data Protection Regulation (GDPR) goes even farther by requiring consent, breach notification, information access, data erasure, portability, and privacy by design. The scope has also expanded to "all companies processing the personal data of data subjects residing in the Union, regardless of the company's location." Data subjects must explicitly consent to the use and purpose of how their information will be processed. Data subjects must be notified when a breach, or unauthorized access, has occurred. This notification must occur within 72 h of the breach. Data subjects have the right to know if personal information about them is being held, used, or processed by data controllers. Individuals, with various exceptions, have the right to be forgotten. Data subjects can have "... the data controller erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data."[46] Data portability gives data subjects the right to obtain a copy of his/her data. The privacy by design rule requires data protection be a core value in system design rather than an after-the-fact add on. The GDPR also allows fines up to four percent of a company's worldwide yearly revenues or 20 million euros, whichever is higher. Finally, these rules apply to government agencies as well as private entities.

Consider a recent US case *FTC v Wyndham Inc*.[47] Due to defective security practices Wyndham was hacked on three separate occasions with the result of over 10 million in losses due to identity theft. Section 5 of the FTC act indicates that an unfair and actionable behavior is one that "causes or is likely to cause substantial injury to consumers; cannot be reasonably avoided by consumers; and is not outweighed by countervailing benefits to consumers or to competition."[48] Keeping information about their patrons on an insecure system and not correcting the security flaws after the first hack was deemed to be actionable behavior. This line of thought could be used in a more robust way. Imagine that companies or states who hold sensitive personal information about individuals, information not central to the enterprise or business concern, could be held liable if this information is stolen. To put the point another way, to hold sensitive personal information about someone beyond the original purpose for the initial disclosure and use, opens these data subjects to foisted risks. For example, when a patron checks in at a Wyndham hotel and discloses credit card, home address, and license plate information, the purpose of these disclosures is to secure payment for the room and a parking spot for the car. When Wyndham unilaterally decides to store this information, the patron is subject to unconsented to risks. Foisting such risks could be considered an actionable harm.

Imagine that we adopted the following rule: when information is hacked, liability lies by default with, not only the hackers, but also with individuals, institutions, corporations, or states that have warehoused the information.[49] While there could be numerous exceptions, like the hacked information was vital for state operations and was held secure by the latest and best systems, such a rule would incentivize various actors to delete everything but the most important information. Like the GDPR, such a rule would change the

[46] https://www.eugdpr.org/the-regulation.html. While many have warned that the right to be forgotten will undermine freedom of speech there is reason to believe that these worries are overblown. See Paul J. Watanabe, "Note: An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure," *Southern California Law Review* 90 (2017): 1111; Giancarlo Frosio, "The Right to be Forgotten: Much Ado About Nothing," *Colorado Technology Law Journal* 15 (2017): 307–336. See also, "Privacy, Speech, and Values: What we have No Business Knowing," *Journal of Ethics and Information Technology* 18 (2016): 41.

[47] *FTC v Wyndham Inc*. 799 F.3d 236 (3d Cir. 2015).

[48] Federal Trade Commission Act, Section 5: Unfair or Deceptive Acts or Practices (15 USC §45). https://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.

[49] Along with the suggested *Wyndham* rule we could also re-invigorate US privacy torts. William Prosser separated privacy cases into four distinct but related torts. "*Intrusion*: Intruding (physically or otherwise) upon the solitude of another in a highly offensive manner. *Private facts*: Publicizing highly offensive private information about someone which is not of legitimate concern to the public. *False light*: Publicizing a highly offensive and false impression of another. *Appropriation*: Using another's name or likeness for some advantage without the other's consent." Dean William Prosser, "Privacy," *California Law Review* 48 (1960): 383–389, quoted in E. Alderman and C. Kennedy, *The Right to Privacy* (New York: Alfred A. Knopf, 1995), pp. 155–156. While US privacy torts have been undermined by a series of cases, there have been suggestions to strengthen them. See for example Danielle Keats Citron, "Prosser's Privacy at 50: A Symposium on Privacy in the 21st Century: Article: Mainstreaming Privacy Torts," *California Law Review* (2010): 1805 and Adam D. Moore, *Privacy Rights: Moral and Legal Foundations* (2010), chap. 7.

payoffs of the privacy prisoner's dilemma game. Looming over the use of Asimov's chronoscope would be the risk of substantial fines and sanctions. GDPR rules would go further by allowing data subjects caught in the privacy prisoner's dilemma to demand that their personal information be deleted. Such legislation would change the payoffs of the privacy game, thus giving us all a compelling reason not to look, record, or store the personal information of others.

Conclusion

There are reasons to be concerned about privacy and the current unstoppable march toward a transparent society. Even more alarming is that when individuals have the power to foist transparency on others they will likely do so, and thus we become a society of the watchers and the watched. In the short run it seems that we need to level the playing field—if some are to be incessantly watched, then everyone should suffer this fate. Only when we are each caught in unraveling games or numerous iterated privacy prisoner's dilemmas, will we conclude that foisting or requiring such transparency is a Faustian bargain.

We have maintained that privacy is essential for human flourishing and well-being which supports the European view of privacy as a fundamental right. One way to stop from spiraling down into a surveillance society is to adopt and internalize rationally endorsed privacy principles. It is simply wrong to watch, record, and analyze the behavior of others beyond what is minimally required given the interaction. If Clyde were to follow Bonnie around all day, record her every move, analyze the data, and share this information to any who might look, we would likely consider this a threat or a form of harassment. Clyde shouldn't engage in this activity and we shouldn't countenance it. Like finding someone's diary in a public place, it would be wrong to read it cover to cover after discovering its owners name and cell number on the first page. Nevertheless, in large communities, where foisting anonymous privacy degradation and complete transparency is possible, relying solely on norms will fail.

Technology may also aid in protecting privacy. Technology-based obfuscation, misinformation, anonymization, encryption, and the like, may be utilized to shield individuals from those who can't help but watch. Like some sort of cloaking device, we could each wrap ourselves in anti-disclosure technology. End-to-end encryption of phone services and email is now possible and privacy promoting technologies will continue to advance. As with privacy norms, relying on technology will be imperfect, as evidenced by the fact that the arms race between surveillance technology and privacy-enhancing technology is currently being won by the former.

Laws and legislation could also alter the game. If the General Data Protection Regulation (GDPR) in Europe works, and other nations follow suit, we could see the end of the privacy prisoner's dilemma. Rather than adopting different data policies for different markets, the largest players may decide to adhere to the most restrictive data privacy laws. The efficiencies of such an approach would be obvious and the resulting privacy enhancements would be most welcome. In setting a new baseline for data governance, the GDPR, and legislation like it, will incentivize innovation in privacy enhancing technologies and also highlight the value of privacy. When news of the first 20 million euro lawsuit becomes widely known, everyone will view the value of data privacy in a new light. If so, selfish reasons and prudence will lead us toward a collectively optimal solution to the privacy prisoner's dilemma.