Law and Philosophy (2010) 29:505–534
DOI 10.1007/s10982-010-9067-9

BOUDEWIJN DE BRUIN

THE LIBERAL VALUE OF PRIVACY

(Accepted 17 March 2010)

ABSTRACT. This paper presents an argument for the value of privacy that is based on a purely negative concept of freedom only. I show that privacy invasions may decrease a person's negative freedom as well as a person's knowledge about the negative freedom she possesses. I argue that not only invasions that lead to actual interference, but also invasions that lead to potential interference (many cases of identity theft) constitute actual harm to the invadee's liberty interests, and I critically examine the courts' reliance on a principle of 'no harm, no foul' in recent data breach cases. Using a number of insights from the psychology of human belief, I also show that the liberal claim for protection of privacy is strengthened by the observation that often the privacy invader cannot be held responsible for the influence on the invadee's negative freedom.

I. INTRODUCTION

Liberal thinkers wrestle with privacy, especially if they operate with a negative concept of freedom.[1] Some even hold that

[1] An invasion of the privacy of a person, B, involves an agent, A, disclosing a fact about B to a third person, C. A and B may be identical. It is a triadic relation between a sender, a subject, and a recipient. This sets the notion apart from the way the term is used in Griswold v. Connecticut, 381 US 479 (1965) and Roe v. Wade, 410 US 113 (1973), where privacy is rather defined in terms of abilities to decide and act. If we use such a 'decisional' concept of privacy instead of the 'informational' concept that underlies the present paper, a connection between privacy and freedom can be demonstrated *directly*. See, for instance, Judith DeCew, 'The Priority of Privacy', *Social Philosophy and Policy* 17 (2000): 213–234; R. G. Frey, 'Privacy, Control, and Talk of Rights', *Social Philosophy and Policy* 17 (2000): 45–67; Robert Hallsborg, Jr., 'Principles of Liberty and the Right to Privacy', *Law and Philosophy* 5 (1986): 175–218; Adam Moore, 'Privacy: Its Meaning and Value', *American Philosophical Quarterly* 40 (2003): 215–227. The connection between informational privacy and negative freedom uncovered in this paper is rather more indirect.

privacy has little liberal value and ought not to receive much special legal protection. These thinkers see the pursuit of privacy as self-interested economic behavior, aimed at concealing 'discreditable' facts about oneself, which is opposed to liberal interests such as freedom of speech, freedom of market transactions, or security.[2] Generally, therefore, such thinkers do not object to the presence of surveillance cameras in public spaces, to bookstores forwarding information about purchases to companies and government agencies, or to airlines requiring numerous items of data from travelers boarding planes. Naturally, these skeptics about the value of privacy acknowledge that the disclosure of private information can have unpleasant, even harmful effects, but they assert that such effects are outweighed by liberty (free speech, security, economic growth, etc.), and that most problems arising from invasions of privacy should be left to individuals rather than the state to redress.[3]

[2] Richard Posner, *The Economics of Law* (Cambridge: Harvard University Press, 1981), p. 233ff.

[3] Skeptical positions about privacy have been articulated by many authors – not all of them liberals. For example, Anita Allen, *Why Privacy Isn't Everything: Feminist Reflections on Personal Accountability* (Lanham: Rowman and Littlefield, 2003); Richard Epstein, 'Deconstructing Privacy: And Putting It Back Together Again', *Social Philosophy and Policy* 17 (2000): 1–24; Amitai Etzioni, *The Limits of Privacy* (New York: Basic Books, 1999); Catharine MacKinnon, *Towards a Feminist Theory of the State* (Cambridge: Harvard University Press, 1989); Posner, *The Economics of Law*; Jesper Ryberg, 'Privacy Rights, Crime Prevention, CCTV, and the Life of Mrs Aremac', *Res Publica* 13 (2007): 127–143; Michael Sandel, *Democracy's Discontent: America in Search of a Public Philosophy* (Cambridge: Harvard University Press, 1996). I am concerned most with such authors as Allen, Epstein, and Posner, who combine skepticism about privacy with a form of liberalism and individualism. Their position differs from feminist and communitarian critiques of privacy, as well as from the *nothing-to-hide argument* popularly defended by many laypeople. The nothing-to-hide argument against privacy is to the effect that as long as I do not perform any illegal and immoral acts, I have nothing to be afraid of, and consequently, I do not have to hide anything. In contrast to proponents of the nothing-to-hide argument, liberal privacy skeptics acknowledge that even though I do not perform illegal or immoral actions, others may use information about me in ways that harm me. See Daniel Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy', *San Diego Law Review* 44 (2007): 745–772.

Traditional arguments for privacy fail to convince the liberal skeptic. Take the *argument from perspective change*. This is to the effect that, if I were to discover someone observing me while I am engaged in certain activities, I would change from being a genuine 'participant' in the action to being an 'observer' of it, which – the argument states – is bad.[4] However, many privacy skeptics will probably not be troubled overmuch by subjective feelings of perspective changes. They will hold that, after all, it is possible to carry out the tasks irrespective of whether or not someone is watching you.

Take now the *argument from relationships*. According to this argument, privacy is a necessary condition for many human relationships, because relationships involve the mutual giving of gifts in the form of information exchange; and such gift giving only prospers when individuals have secure possession of what they want to give, namely, private information.[5] Yet does another person's listening into a conversation between friends *really* make it impossible to share intimate thoughts and feelings? The privacy skeptic will doubt that. The friends may *feel* inhibited, but that does not mean that they *are* inhibited.

Or take the *argument from human dignity*, according to which invasions of a person's privacy go against her dignity. This is exemplified by a famous case that came before the Michigan Supreme Court in 1881 in which a woman laid a complaint against a man who had been present when she was giving birth, and who was presumed to be connected to the medical profession whereas in fact he was not.[6] Thereby, it was

[4] See Stanley Benn, *A Theory of Freedom* (Cambridge: Cambridge University Press, 1988), pp. 271–278; Robert Gerstein, 'Intimacy and Privacy', *Ethics* 89 (1978): 76–81.

[5] Developed mainly by Charles Fried, 'Privacy', *Yale Law Journal* 77 (1968): 475–493, and James Rachels, 'Why is Privacy Important?' *Philosophy & Public Affairs* 4 (1975): 323–333, the argument is revisited by Jean Cohen, *Regulating Intimacy: A New Legal Paradigm* (Princeton: Princeton University Press, 2002), and Julie Inness, *Privacy, Intimacy, and Isolation* (New York: Oxford University Press, 1992).

[6] DeMay v. Roberts, 46 Mich. 160 (1881).

claimed, he affronted the woman's dignity.[7] Now, in this case privacy skeptics will not be so callous as to ignore the fact that the woman suffered feelings of 'shame and mortification', but what they will condemn is the man's pretending to a false identity, rather than an invasion of privacy.[8]

Finally, take the *argument from autonomy*. Starting from the assumption that the possession of correct beliefs about what *others* know about me fosters my autonomy, this argument claims that it is in my interest to be in control of what others know about me.[9] It matters, for instance, in terms of my decision to practice the salsa in my office whether or not I know someone is watching me. But again, liberal privacy skeptics would not be moved. Someone peeping through my office window in no way obstructs me from dancing.

To convince the skeptic of the liberal value of privacy, we would have to show that invasions of a person's privacy

[7] Classic statements of this argument are those of Samuel Warren and Louis Brandeis, 'The Right to Privacy', *Harvard Law Review* 4 (1890): 193–220, and Edward Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser', *New York University Law Review* 39 (1964): 962–1007. More recent articulations are given by Hallsborg Jr., 'Principles of Liberty and the Right to Privacy', and Iris Marion Young, 'A Room of One's Own: Old Age, Extended Care, and Privacy', in *Privacies: Philosophical Evaluations*, ed. Beate Rössler (Stanford: Stanford University Press, 2004), pp. 168–186.

[8] The defender of the argument from dignity could retort that we can imagine that the woman refuses consent on the grounds that the presence of the young man affronts her dignity, and that this shows that the affront to dignity is independent of the consent. But then one has to answer the question of what a person A, committed to protecting human dignity, ought to do if she sees that B consents to C affronting B's dignity. If A stops C, she will affront B's dignity by not respecting B's autonomous choice. If A does not stop C, she will be resigned to B's dignity being affronted.

[9] Autonomy is the broad notion that goes far beyond bare negative freedom. See, for instance, Mark Alfino and G. Randolph Maynes, 'Reconstructing the Right to Privacy', *Social Theory and Practice* 29 (2003): 1–18; Joseph Kupfer, 'Privacy, Autonomy, and Self-Concept', *American Philosophical Quarterly* 24 (1987): 81–89; Beate Rössler, *The Value of Privacy*, trans. R. D. V. Glasgow (Cambridge: Polity Press, 2005); Alan Rubel, 'Privacy and the USA Patriot Act: Rights, the Value of Rights, and Autonomy', *Law and Philosophy* 26 (2007): 119–159; Ferdinand Schoeman, *Privacy and Social Freedom* (New York: Cambridge University Press, 1992).

decrease the extent of her freedom. Is this possible? A first attempt to meet the challenge would be the following: Strictly speaking, activities such as having sexual intercourse, exchanging secret information, or giving birth can, as the skeptic correctly notes, also be performed if someone were to keep you under observation. But the 'logic' of these activities requires that they be performed 'unwatched'. If someone listens in, it is just not possible, for example, to exchange *secrets*, or to correct a friend's mispronunciation of a particular foreign term *in a discreet and friendly manner*. Similarly, it is impossible to have sex or to give birth *in the typical way* if someone is watching you.[10]

This attempt can only be successful, however, if we assume a rather broad manner of describing actions, which is not universally accepted. Moreover, circularity is lurking, since absence of a privacy invasion now becomes part of the description of the action. That is why I propose a different way to meet the skeptical challenge.

First, we have to do some *analysis*. I show that disclosures of private information about a person, A, may lead to a change in the extent of A's negative freedom as well as to a change in A's *knowledge* concerning the extent of her negative freedom. An example of a change in negative freedom is the following. A parent spies on the headmaster of her child's school, discovers he is gay, and reveals this publicly to other parents. A little later, the headmaster is barred from entering the school and is eventually forced to resign because of pressure exerted by worried parents – a decrease in his negative freedom. An example of a change in one's knowledge about freedom is the following: My bank's computer server has been stolen. I do not know whether the burglar wanted to get the computer hardware or the financial records stored on it, and hence my knowledge about future interference is reduced. I am less sure than I was prior to the burglary about, say, the chance that criminals will try to obtain credit in my name, constituting a decrease of knowledge about negative freedom that may find

[10] This line of argument was suggested by Rachels, 'Why is Privacy Important?' My discussion has benefited from as discussion with Luc Bovens.

reflection in the fact that I decide to buy insurance against identity theft.

These are two cases in which a disclosure of private information ultimately leads to reduced negative freedom, or reduced knowledge about negative freedom. Liberal privacy skeptics may accept this analysis of privacy and negative freedom, but they may still hesitate to draw any further normative conclusions, though, on the grounds that, as long as we have antidiscrimination laws and laws against identity theft, no further regulation is necessary. Empirical and conceptual reasons show, however, that such hesitation is entirely misplaced. Assigning moral and legal responsibility to the 'recipients' of private information – in the above two cases, the parents, the burglar – becomes problematic if, for instance, individuals act on their prejudices. (Suppose some of the parents held the outrageous, yet still extant prejudice that homosexuals are more than likely pedophiles.)[11] Moreover, the liberal interest individuals have in knowledge concerning the extent of their negative freedom is not affected by laws. Laws against identity theft may be adequate and well-enforced, but that does not make me any less ignorant about what the burglar will do with my private data once he has obtained the computer.

Section II, "Privacy, Freedom, and Knowledge" contains the analysis, which also shows where the innovation of my approach to privacy lies in comparison with alternatives. Sections III and IV, "Privacy and Negative Freedom" and "Privacy and Knowledge About Negative Freedom", respectively, discuss normative consequences. More specifically, the former section looks into the normative relevance of empirical and conceptual research bearing on responsibility, and the latter section discusses the liberal value of knowledge about negative freedom.

[11] Albert Klassen, Colin Williams, and Eugene Levitt, *Sex and Morality in the U.S.: An Empirical Enquiry Under the Auspices of the Kinsey Institute* (Middletown: Wesleyan University Press, 1989).

II. PRIVACY, FREEDOM, AND KNOWLEDGE

A. Privacy and negative freedom

I defend the claim here that disclosures of private information lead to changes in one's negative freedom, as well as to changes in the knowledge one has concerning the extent of one's negative freedom. Negative freedom appears in many guises, though, so I will first define the notion I am applying. It is the 'pure negative' concept of freedom according to which I am unfree to perform some action, A, if someone interferes with my performance of A or if someone has the disposition to interfere with my performance of A if I were to attempt to perform A.[12] It does not matter here whether the interference is intentional or not. My negative freedom to travel home is obstructed by the police blocking the road (they interfere), by a highway robber forcing me to stop at gunpoint (he has the disposition to interfere as soon as I attempt to drive on), or by a bridge superintendent forgetting to close the open bridge (unintentionally). But my negative freedom is not restricted by my ignorance of topography, or my lack of driving skills, or my absentmindedness (no external obstacles).

I begin, then, with a number of examples of how disclosures of private information lead to less negative freedom. A top-ranked midshipman at the Naval Academy, Joseph Steffan, told his chaplain about his own homosexuality. The chaplain passed on this information to his superiors, who forced Steffan to resign (on the basis of old Pentagon regulations barring gay people from the military, still operative in the late 1980s).[13]

A banker was illegally given access to a Maryland government database of medical records. Obtaining knowledge about the medical situations of a number of his bank's customers, he forced customers diagnosed with cancer to pay off their loans.[14]

Subsequent to the rape and murder of a seven-year-old girl, Megan Kanka, numerous states implemented laws requiring

[12] Matthew Kramer, *The Quality of Freedom* (Oxford: Oxford University Press, 2001). See also Ian Carter, *A Measure of Freedom* (Oxford: Oxford University Press, 1999).

[13] Steffan v. Perry, 41 F. 3d. 677 (1994).

[14] Etzioni, *The Limits of Privacy*, p. 140.

sex offenders to register with a public database allowing every interested individual access to information about the sex offenders' home addresses, offenses, photographs, and many other personal data. This has led, in some cases, to harassment of sex offenders (and bystanders mistaken for them), to actual vigilantism, and even to the death of registered sex offenders.[15]

Employers increasingly consult social networking websites such as Facebook and MySpace in order to check the profiles of candidates they consider hiring, and some even admit to having decided against candidates because of the risqué pictures such profiles contain or the 'wild' student life boasted of. One college student interviewed by a *New York Times* journalist reported that as soon as he had removed some material from the Internet he began to receive invitations to job interviews.[16]

As these cases exemplify, the connection between privacy and negative freedom has a three-step structure. The first step is the very *disclosure* of information. A sender, A, discloses information about a subject, B, to a recipient, C. (Note that A and B may be identical.) Disclosure is used in a general sense here, as it may involve not only speaking and writing but also drawing C's attention to a certain scene involving B that is happening right now, sending C a photograph capturing B in a certain situation, showing video footage of B, passing on B's criminal or medical records, or A allowing C to hack A's website containing B's home address and social security number. The second step covers *belief revision*. On the basis of the information obtained from A, agent C revises her earlier beliefs about B. This may amount to adding more information, more detail, and leaving earlier beliefs intact; often, though, it will

[15] Michael Laforgia, 'Sex Offender Killed Outside Game Arcade', *Miami Herald* 18 December 2008; Jordi Nordheimer, '"Vigilante" Attack in New Jersey is Linked to Sex-Offenders Law', *The New York Times* 11 January 1995.

[16] Alan Finder, 'For Some, Online Persona Undermines Resumé', *The New York Times* 11 June 2006.

involve a real change of belief.[17] Finally, the third step involves *action*. The new beliefs may motivate C to perform a certain action she would not have performed if A had not given her the information concerning B; and if performing this action constitutes interference with B, then B's negative freedom has been reduced as a result of an invasion of privacy.[18]

The new beliefs can be reasons for C to perform some action, but also merely to adopt a *disposition* to perform some action. Consider the following two cases. Having learned that a convicted sex offender moved into her neighborhood, a woman in Timberlane, Washington, decided that she would gun him down if he came too close to her house. The sex offender never did come close to her house, but if the woman's decision was genuine enough (there seems no reason to assume it was not), the man would not have survived if he had tried.[19] Many sex offenders are equally unfree to enter areas around kindergartens and other schools. Most of them do not try, but if they did, watchful and informed parents would stand in their way.

Likewise, several airline companies use information about travel itineraries to decide on whom they choose to put on their 'no-fly lists'. Many of the individuals appearing on such lists

[17] If an agent 'updates' her beliefs, she adopts the doxastic attitude of belief towards a proposition, P, towards which she did not previously have a doxastic attitude. If she 'changes' her beliefs, she adopts the doxastic attitude of belief towards a proposition, P, towards which she previously held the attitude of disbelief; that is, she changes from believing that P is true to believing that P is false, or *vice versa*. In certain cases, agent C will decide to retain her original beliefs, rejecting the new information. This is rational, for instance, when A informs her about a proposition which has both low *prior* probability and low *conditional* probability, given C's current beliefs about B, such as when A tells C that B was hijacked by extraterrestrials.

[18] Just as much as new information may lead to the performance of a certain action, it may also lead to the omission of a certain action. Performing an action and omitting one can both be forms of interference. I can interfere by actively blocking the road, or just by refraining from letting the bridge down. For stylistic reasons I do not always refer to omissions explicitly in what follows below. Nevertheless, what I say about actions is also true of omissions.

[19] Linda Keene, 'Warning Signs: A New State Law Alerts Parents to Predators in the Neighborhood and the Struggle to Cope Begins', *Seattle Times* 15 September 1991.

never buy tickets from these airline companies, but if they did they would be barred from flying to certain destinations.[20]

The woman in Timberlane, Washington, did not use the new information concerning the sex offender to perform an actual interfering action, but she did use it to change her disposition to act. The no-fly policy similarly embodies a changed disposition towards certain potential customers. Following the pure negative concept of freedom, these changed dispositions are a decrease of freedom, just as much as actual interference would constitute a decrease of freedom. This means that the third step in the connection between privacy and negative freedom may not only involve the *performance* of an action (or omission), but also the *adoption* of a *disposition* to perform (or omit) some action.

It might be objected that referring to 'dispositions' leads to the inclusion of *counterfactual* or *hypothetical* obstacles, and that that makes the definition of freedom too broad. Since this ingredient is obviously essential to my analysis, let me say something in defense of it.[21] The counterfactuality resides not in the interferer's actions or dispositions (the woman's decision to kill the sex offender and the no-fly policy are very real) but in the interferee's performance of the action (the sex offender never actually entered her neighborhood, the person on the no-fly list never actually bought a one-way ticket from Tehran to London). Suppose, for instance, that I am working in my office. In one scenario, the door has been locked and I do not have a key. I am unfree to leave. In another scenario, someone is waiting outside my office. He has the key in his hands and if he heard me walking to the door, he would lock it. I do not have the key myself, so in this scenario, too, I cannot leave my office: if I attempted to leave the room I would find the door locked. The pure negative view of freedom describes me as unfree in both situations.

[20] See, for instance, Sally Donnelly, 'You Say Yusuf, I Say Youssouf…', *Time.com*. http://www.time.com/time/nation/article/0,8599,702062,00.html. Accessed 25 September 2004.

[21] See for more details Matthew Kramer, 'On the Counterfactual Dimension of Negative Freedom', *Politics, Philosophy & Economics* 2 (2003): 63–92.

And, indeed, many unfreedoms are exactly of this form. That I am unfree to protest against the government or to travel abroad may involve actual barriers. More often, though, my unfreedom will reside in the fact that if I attempted to protest or travel, I would be interfered with. Excluding dispositions to interfere would give rise to an implausible evaluation of the freedom of, say, citizens of totalitarian regimes. Therefore, it is preferable to have a concept of freedom that takes dispositions to interfere as reductions of the extent of a person's negative freedom.

Disclosure of privacy leads to belief revision, which in turn leads to the performance of actions, or dispositions to perform actions. This framework is entirely general. To be sure, privacy cases dealt with by legal scholars and philosophers witness *decreases* of negative freedom most of the time, but there is no reason why disclosure of information would lead to decreases of one's negative freedom in *all* cases. If agent A discloses information about B to C, the information may not be new to C, in which case C has no reason to change the plan of action she settled on before A gave her the information about B. Even if the information is new to C, the beliefs revised in accordance with that information need not be a reason for C to act differently. A banker obtaining information about a customer's cancer diagnosis, or an employer learning about a prospective candidate's behavior at frat parties, may simply find no grounds therein to change their (dispositions to) actions.

In fact, disclosing private information is often essential to *increase* one's negative freedom. A large number of services are impossible to obtain if you do not identify yourself (entrance to a night club, medical services, and so on), and many market transactions also require one to disclose a great deal of private information (buying a house, starting a business).[22] In such cases, agent C does update or revise her beliefs about B. But the

[22] James Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty', *The Yale Law Review* 113 (2004): 1151–1221 makes the case that the strictness of the European privacy legislation in comparison to that in the US is one of the factors that determine differences in individuals' wealth. As it is easier in the US, especially in terms of time and costs, for banks to obtain information about someone's credit record, it is also easier for customers to obtain credit.

actions (or dispositions) motivated by her new beliefs do not restrict B's negative freedom; they increase B's freedom. It is true that the examples of privacy invasions given by alarmist authors typically involve decreases of freedom, but this should not obscure the fact that disclosures of private information may lead to decreases as well as to increases of negative freedom, or to no change at all.

How does this approach to privacy and negative freedom differ from the traditional arguments from perspective change, relationships, and so forth? If someone is peeping through my office window all the time I am working on a paper, the argument from perspective change suggests I may resent this because it forces me to adopt the observer's point of view, thereby making it harder (or even impossible) for me genuinely to 'participate' in my writing activities. And if someone overhears me talking to a friend, the argument from relationships implies this makes it harder (or even impossible) to engage in the mutual gift-giving essential to friendship. Now this, it might seem, reveals that the arguments from perspective change and relationships *also* indicate ways in which disclosures of private information make individuals less free. I am less free to work on the paper, and less free to maintain relationships. Or so it would seem.

If the traditional arguments relate privacy and freedom at all, their concept of freedom is certainly not a *negative* one. The privacy invasions do not influence my negative freedom to write a paper or to perform gift-giving actions, because the peeper and the eavesdropper do not establish *external* impediments to my typing at the keyboard or uttering certain words to my friend. Moreover, unlike the traditional arguments, my analysis is not concerned with the (perspective on) actions the agent is *presently* performing, but rather with the influence an invasion of privacy has on the agent's extent of negative freedom at some *future* point in time. The point is not that the eavesdropper makes it less easy to talk to my friend, but that the eavesdropper may use what my friend and I tell each other in ways that frustrate my future negative freedom. (Imagine, for instance, that the eavesdropper is a government informant in

the rather totalitarian country in which I live, and my friend and I have talked disparagingly about the president.) Altogether, by focusing on *external* impediments to *future* actions, my approach is very different from the traditional ones.

B. Privacy and knowledge about negative freedom

People often resent invasions of their privacy. The traditional arguments explain the feeling of resentment in terms of a perceived frustration to be a genuine 'participant' in a certain action, by feeling affronted, or by feeling obstructed in realizing a certain friendship. The problem with this view, however, is that it is hard to distinguish between a situation in which a person is peeping through your window observing you typing a paper, and a situation in which you share your office with a colleague who observes you typing a paper. Both would be cases of perspective change, yet most people only feel resentment in the former case.

While the traditional arguments find it difficult to account for such forms of resentment, the approach I put forward can be used to proffer an explanation. To that end, it is not sufficient to consider the ways in which negative freedom is compromised, because peeper and colleague may change my negative freedom to the same degree. Rather, we have to consider the influence of privacy invasions on a person's *knowledge* about negative freedom.

Knowing my colleague quite well, I know that she will not plagiarize my work, use the credit card that is lying on my table to buy books on the Internet, or gossip to my students about my habit of talking to my computer. My knowledge of the peeper, by contrast, is very limited. I do not know why she is watching me at all. For all I know she may be trying to find some pattern in my working hours to plan a burglary of my house; she may be attempting to get hold of business secrets; she may be checking whether the office contains any things worth stealing; or she may be an anthropologist doing fieldwork. This only serves to increase my ignorance about the likelihood of interference with future actions of mine. I am just less sure about what I can do.

Let us consider two examples. Customers of Old National Bancorp filled in online forms requesting personal information from applicants for certain banking services. A hacker obtained

access to the bank's computer server, thereby gaining access to confidential information on more than 10,000 individuals. Numerous of these individuals decided to buy credit monitoring services to insure themselves against the risks of future identity theft, thereby reflecting their increased uncertainty about future interference.[23]

Three undercover police officers investigated a drug conspiracy in a violent gang in Columbus, Ohio. When some gang members were tried, their lawyers requested access to the personnel files of the officers. And that is what the lawyers got. Such files contain information about names, home addresses, phone numbers, driver license numbers, and information about the officers' family members. None of the officers seems to have suffered from any harm to date; no lawyer seems to have passed on the information to her clients. Clearly, though, the officers' uncertainty about the risk of harmful interference has increased.[24]

The connection between an invasion of privacy and reduced knowledge about negative freedom is a kind of 'internalization' of the earlier connection between privacy and negative freedom. Agent A discloses private information about B to C. Agent B knows about the disclosure and, internalizing the three-step process linking privacy to negative freedom, she knows that C may use the information to motivate the performance (or omission) of certain actions or the adoption of certain dispositions to perform (or omit) certain actions.[25] If B knows C

[23] Pisciotta v. Old Nat. Bancorp 499 F. 3d. 629 (2007).

[24] Kallstrom v. City of Columbus, 136 F. 3d. 1055 (1998).

[25] If B is unaware of the fact that A discloses private information about B to C, then the internalization will not take place. This means that if novel information about B makes C interfere with B, then B will not know that. Agent B's knowledge about negative freedom is then reduced, but not because B has changed her beliefs (as when she internalizes), but because B has *not* changed her beliefs, even though her negative freedom has changed. (An example is when unbeknown to me someone makes use of my Social Security Number to obtain credit.) This scenario reveals a second way in which known freedom decreases after an invasion of privacy, but I do not treat it as a separate category in the paper since it also directly involves a decrease of negative freedom. The interesting cases involve a decrease of knowledge about negative freedom that is not accompanied by a decrease of negative freedom. See section III, "Privacy and Knowledge About Negative Freedom".

well, B has some information about C's current beliefs, about the ways C revises her beliefs, and about C's desires. As a consequence, B can predict the influence that the disclosure of private information will have on C's actions, and C's knowledge about negative freedom will be as accurate as it was previously.[26] If B does not know C, she will not be able to infer anything about what C will do with the information. She will not be able to predict C's action, and consequently, her knowledge about negative freedom will be reduced.[27]

III. PRIVACY AND NEGATIVE FREEDOM

The advantage of the approach to privacy I am advocating here is that it allows us to cast arguments about the special protection of a person's privacy in a uniform, normative vocabulary. Whether or not to protect a person's privacy in a certain situation is almost always a question of balancing. The traditional arguments, however, put a rather heterogeneous collection on the scales: perspective changes or human dignity on the one side, for instance, and freedom of speech or freedom of market transactions on the other. As soon as we cast the

[26] Of course, B's negative freedom may be less. But if that is so, then B knows it.

[27] Several champions of the argument from autonomy also consider the effects of privacy invasions on the expectations of the subject. However, their position differs crucially from the approach I proffer here, since it is not beliefs about the extent of one's negative freedom with which these authors are concerned, but rather beliefs about the 'level' of privacy protection one enjoys. If, unbeknown to me, someone is watching me practicing the salsa in my office, it is my current beliefs – my belief that I am dancing unobserved – on which the argument from autonomy focuses. That is, a belief about the presence of observers. The beliefs figuring in my approach, by contrast, are beliefs about my future negative freedom. See Rössler, *The Value of Privacy*; Robert McArthur, 'Reasonable Expectations of Privacy', *Ethics and Information Technology* 3 (2001): 123–128. To some extent, the argument from autonomy may not even be able to find fault with a peeper whom I know to be watching me practicing the salsa. In that case, no incorrect beliefs arise about my level of privacy. Following my approach, by contrast, observed and unobserved invasions of privacy can be seen to harm my liberty interests.

value of privacy in terms of negative freedom, only one unit of measurement is needed – liberty.[28]

This strategy bears certain risks, though. Liberal privacy skeptics may concede that I have connected invasions of privacy to changes in the extent of a person's negative freedom, but they can still refuse to draw any normative conclusions from that analysis on the grounds that whether or not the recipient C of the private information uses the information to interfere with subject B is up to C's moral and legal *responsibility*. If, upon receiving new information about B, agent C decides to use B's credit card number or to fire her because of sexual prejudices, then C does something that is already prohibited by law, so there is no ground for protecting privacy here. And if, upon receiving the information about B, agent C decides to put an end to her friendship with B, then that is something B simply has to cope with, however immoral it may be.[29]

This move to moral and legal responsibility is standard in many cases where liberal values are balanced. Consider, for instance, the connection between media violence and subsequent aggressive behavior. Proponents of legal measures suggest that the statistical correlation is strong, and that the interests of the potential victims of aggression outweigh the interests of the viewers of certain movies and television shows.[30] Opponents of regulation, by contrast, point out that as long as the individual viewer can be held morally and legally *responsible* for the aggressive acts there is no need for the regulation of media violence. It suffices to have laws prohibiting homicide, assault, and so on.

Such an argument against regulation of media violence succeeds only if it is possible to assign responsibility to the

[28] Section IV, "Privacy and Knowledge About Negative Freedom" discusses the value of knowledge about negative freedom.

[29] Herman Tavani and Frances Grodzinsky, 'Cyberstalking, Personal Privacy, and Moral Responsibility', *Ethics and Information Technology* 4 (2002): 123–132 examine the responsibility of Internet providers and users in the context of cyberstalking.

[30] Susan Hurley, 'Imitation, Media Violence, and Freedom of Speech', *Philosophical Studies* 117 (2004): 165–218.

perpetrators of aggressive acts subsequent to exposure to media violence, and that assumption may not be true. If, for instance, viewers copy aggressive behavior they have seen on television in ways that bypass autonomous and responsible decision making, then it is doubtful whether they can be held responsible. In such a case legal regulation of media violence may come into sight.

In the case of media violence this is probably hard to defend, because copycat crime and other forms of aggression following exposure to media violence often involve a huge amount of advance planning, which is incompatible with decreased or bypassed autonomy. Moreover, only a small number of viewers ever engage in subsequent aggressive acts.[31] Matters are different in the case of privacy, though.

Recipients of private information tend to be *credulous*, they tend to *overgeneralize* on the basis of limited information, and they often suffer from *prejudices* – all without their being aware of it. Besides that, the *collective* effect of the actions performed by recipients of private information is often considerable, even though the individual agents' contributions are small. And recipients of information frequently remain *anonymous*. These empirical facts about belief revision and human agency suggest that in many cases it is hard, or even impossible, to assign moral or legal responsibility to the recipients of private information for the freedom-decreasing effects of their actions.[32] Let me explain.

A. Collectivity

A good illustration of the structure of *collective* interference is given by e-mail spam, junk mail, and unsolicited phone calls. One phone call from one company may be annoying, but if you receive a phone call a day (typically around dinner time)

[31] See Boudewijn de Bruin, 'Media Violence and Freedom of Speech: How to Use Empirical Data', *Ethical Theory and Moral Practice*, 11/5 (2008): 493–505.

[32] Charles Stangor, ed. *Stereotypes and Prejudices* (Philadelphia: Taylor and Francis, 2000) collects a number of key papers in the psychological literature.

because your phone company has sold information about your household to numerous other companies, you are simply suffering a decrease in your negative freedom. The same is true when your surface mailbox is stuffed with catalogs and other mailings from companies you will never buy from (you have to trash them), and when removing spam takes you valuable (business) time every day; not to speak about e-mail messages that accidentally get lost in the deletion process. Estimates of the costs of spam, for instance, amount to $130 billion worldwide, and $42 billion in the US – for just a single year, that is.[33]

Moreover, collective interference may have much more devastating effects than these relatively harmless examples suggest, especially now that the Internet has rapidly become a place where large groups of people voice their opinions on political and social topics, as well as on individual citizens. A sadly famous case involved a South-Korean college student who was photographed by a bystander when she refused to clean up her dog's accidental excrement on the Seoul subway. Posted on an Internet forum, the story led people to condemn her behavior, often in extremely violent language. One or two comments she might have found bearable, but hundreds or even thousands of Internet tirades made her case so famous that she was recognized as the 'dog poop girl' wherever she went on the Seoul campus, and *treated* as such – she quit college.[34]

What is important here is that these collective effects are not always readily sensed by the individual agents. If I send you one catalog once a year, or make an unsolicited phone call, in my view this is only a tiny disturbance of your life. Likewise, the Internet commentators do not see themselves as part of a large protest crowd, and they would probably not participate in marches gathering against a girl who does not clean up in the subway. Put abstractly, the recipients of the information know what they are doing, but they do not always know that many others are doing the same thing; and if they know that others

[33] Estimation by Ferris Research, a firm specializing in communication research, for 2009. See http://www.ferris.com/research-library/industry-statistics.

[34] Daniel Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* (New Haven: Yale University Press, 2007), pp. 1–2.

are doing the same thing, they are not aware of the fact that all these individual, anonymous actions may add up to massive, collective interference.[35]

B. Anonymity

Collectivity of interference makes it conceptually problematic to assign responsibility to interfering recipients of private information; that recipients often remain *anonymous* is a practical reason why responsibility is hard to designate. Databases such as those developed after Megan's Law afford anonymous individuals access to information about numerous sex offenders; individuals ranting on Internet forums often contribute anonymously; hackers and identity thieves remain largely unidentified; and newspapers and TV news shows cater to a largely anonymous audience. If they interfere, it is hard to backtrack these individuals and hold them responsible.[36]

C. Credulity

It was once said on the Web that Tommy Hilfiger, the fashion designer, had remarked to Oprah Winfrey that 'If I had known African-Americans, Hispanics, Jews and Asians would buy my clothes, I would not have made them so nice. I wish these people would not buy my clothes, as they are made for upper-class white people'. It cost his company a lot of money. Readers

[35] The sender of the information possesses more extensive knowledge than the recipient. Most of the time, she knows to whom she has passed on the information, and she will generally have rather accurate beliefs about the use recipients are likely to make of the information. This is one of the reasons why relevant legal cases involve individuals suing the sender rather than the (interfering) recipients of the information. In Smith v. Chase Manhattan Bank, 293 A.D. 2d. 598 (2002), for instance, customers sued a bank for selling personal data to third parties who would use the data for advertising purposes. Realizing that a claim against an individual party sending out one unsolicited catalog would be entirely hopeless, they sued the bank – unsuccessfully. (Courts that recognize the difference between individually harmless actions and collectively harmful results might decide differently.)

[36] Solove, *The Future of Reputation*, pp. 139–149.

took the report seriously. In reality, though, Hilfiger had never been on Oprah's show at that time. The rumor was entirely false.[37]

Richard Posner and other privacy skeptics believe that the Internet offers a fast and powerful means to set errors right, because 'private demand for screening for accuracy will eventually result in equipping the Internet with quality controls as effective as those of the traditional media'.[38] I do not think we can be very optimistic here, though. First of all, while I may have a clear interest in the accuracy of information provided by my bank and my insurance company, I may just not care too much about Hilfiger clothes to require the same level of accuracy here. What is more, even if websites started printing corrections, as newspapers often do, this would not be too successful a corrective mechanism because many people will never return to the website where they read the false rumor. Finally, while the reliability of most websites is notoriously hard to judge, many individuals have a tendency to believe such rumors as the one about Hilfiger on the grounds that, even if it is not entirely true, it will be 'basically' true – where there's smoke there's fire.

D. Overgeneralization

Many recipients are eager to *generalize* beyond justification on the basis of information they obtain. Suppose you show me a video clip of a man yelling at a young child for no obvious reason. Instead of stating that I cannot form any reasonable beliefs about the man on the basis of only ten seconds of video footage, I will probably form a negative opinion about him, and I may use this opinion to decide against hiring him as a baby sitter, say, or day care employee. While this may sound outrageous, it is precisely what employers do when, as we saw earlier, they examine prospective candidates' social networking profiles. What appears on Facebook profiles reflects only part

[37] Nicholas DiFonzo, *The Watercooler Effect* (London: Penguin Books, 2008), pp. 204–205.

[38] Richard Posner, *Frontiers of Legal Theory* (Cambridge: Harvard University Press, 2004), p. 93.

of a person's life, and it is plausible that candidates whose profile is more conventional (or simply nonexistent) engage in roughly the same kind of social activities during their student years as those who display them more openly on the Internet. But many an employer will fail to pay heed to such statistical reasoning when deciding on a candidate.

E. Prejudice

Recipients of private information often process information in light of a body of background beliefs – or prejudices – of which many are false. To give an example, numerous men and women suffer from false preconceptions about rape victims, such as that women encourage men to rape, that rapists are lower-class, or that women's rape reports are often false.[39] Such prejudices nurture incorrect beliefs that influence the ways in which, in the present example, individuals treat people they know to be rape victims. In fact, while the US does not yet seem to have witnessed such extremes, some European rape victims are reported to have been renounced by their families, disinherited, and divorced on the basis of exactly this prejudice.

If people could be held responsible for the false beliefs to which credulity, overgeneralization and prejudice lead, the skeptic would perhaps not yet be moved to afford special protection to privacy. But the psychological literature on credulity, overgeneralization and prejudice not only reveals how widespread the phenomena actually are; it also shows that we frequently fail to notice it when we ourselves are subject to these influences. We are often unaware of our preconceptions and of the fact that we are far too ready to draw conclusions and adopt beliefs. To give one example, the way television news programs frame news items has a considerable effect on the viewers' beliefs, and this is an effect of which most viewers remain unaware. When the Iraq war started in 2003, about 30% of Fox News viewers believed that American intelligence

[39] Marietta Sze-chie Fa, 'Rape Myths in American and Chinese Laws and Legal Systems: Do Tradition and Culture Make the Difference?', *Maryland Series in Contemporary Asian Studies* 4 (2007): 1–109.

had actually found weapons of mass destruction. How is that possible, in the face of massive counterevidence? To be sure, Fox News did not state any falsehood. Rather, false beliefs were induced in the viewers by means of long-term framing techniques. News programs consistently devoted more attention to White House statements about alleged proofs of the presence of weapons of mass destruction in Iraq than to the withdrawals that would always follow. Statements of proofs, for instance, would figure in the opening of a news show, accompanied by vivid visual imagery or interviews with 'experts'. Withdrawals, by contrast, would be deferred to the end of the show, being only read out by the anchor, with no images or interviews.[40] Without knowing about these techniques, numerous viewers were led to false beliefs for which they can hardly be held responsible.[41]

To summarize, privacy invasions may lead to decreases in the subject's extent of negative freedom. As far as the interferers can be held responsible for the interference, the liberal

[40] Steven Kull et al., 'Misperceptions, the Media and the Iraq War', *PIPA/Knowledge Networks* 2 October 2003; Stephan Lewandowsky et al., 'Memory for Fact, Fiction, and Misinformation: The Iraq War 2003', *Psychological Science* 16 (2005): 190–195. The figures compare with around 20% for most other national networks, and 10% for PBS. With respect to the question whether there was, in 2003, clear proof of a connection between Al Qaeda and Saddam Hussein the figures are even more worrying; they range from about 70% for Fox to 16% for PBS. The PIPA report makes clear that only part of the difference may be explained by different characteristics of the viewer populations of the networks.

[41] I do not suggest that one can never be responsible for one's ignorance. A family doctor cannot excuse herself by saying that she did not know of a likely side effect of a common medication she prescribed. But it seems unreasonable to demand from most Fox News viewers that they are aware of the intricate framing techniques and their effects on belief formation in viewers. Alvin Goldman, 'Epistemic Paternalism: Communication Control in Law and Society', *Journal of Philosophy* 88 (1991): 113–131 discusses the influence of biases and overgeneralization on jury members, pleading for a kind of epistemic paternalism. For a growing body of philosophical research into epistemic normativity, see the special issue of *Synthese* on 'Epistemic Deontologism' (vol. 161, no. 3, April 2008).

privacy skeptic may not be moved to regulate.[42] But I have shown several circumstances where it is hard, or even impossible, to assign responsibility. It is in exactly these cases that the subject's liberty interest in the protection of privacy has to be balanced against the liberty interests the recipients have in freedom of information, speech, and so on. To be sure, the actual weighing of interests is going to be a difficult task, and the subjects of the private information will certainly not always win. Yet, if my analysis of privacy invasions in terms of negative freedom is correct, and if the beliefs that underlie the recipient's interference with the subject of the information do at least in certain circumstances form in ways that bypass autonomy, then there is a clear reason why the liberal privacy skeptic has to abandon his or her skepticism. Privacy is a liberal value, and it does outweigh other liberal values in certain cases.

IV. PRIVACY AND KNOWLEDGE ABOUT NEGATIVE FREEDOM

Numerous liberal theorists have developed arguments for the value of negative freedom, such as the argument from *experiments in living*, the argument from *progress*, the argument from *responsibility*, and the argument from *desire satisfaction*.[43] While these arguments are often quite involved, their structure is quite plain: If a person's negative freedom increases, she can try out different ways of living; she can engage in more activities that lead to technological, scientific or cultural progress; she can more often assume responsibility for her actions (instead of leaving responsibility to other individuals or the state); and she will be better placed to satisfy her desires.

[42] Another factor is the subject's responsibility. Compare medical and criminal records. If we suppose that in both cases recipients of private information are prone to similar epistemic errors (and to the same extent), we may still want to distinguish between them if individuals can be held responsible for their crimes, but not for their diseases.

[43] See, for instance, John Stuart Mill, *On Liberty* (London: John W. Parker and Son, 1859); Friedrich von Hayek, *The Constitution of Liberty* (Chicago: University of Chicago Press, 1960); Thomas Hurka, 'Why Value Autonomy?' *Social Theory and Practice* 13 (1987): 361–382; Ian Carter, 'The Independent Value of Freedom', *Ethics* 105 (1995): 819–845.

A closer examination of the precise structure of these arguments reveals that they are not merely arguments for negative freedom, but also for *knowledge* about negative freedom. It is nice to have the negative freedom to perform some action, A, but I will not perform A as long as I am unaware of the fact that I am free to perform A. Only those freedoms of which I have knowledge will figure in experiments in living and responsible decision making, or lead to progress and desire satisfaction. Freedom is valuable, but knowledge about freedom is valuable, too. I call this 'known freedom', and it includes not only knowledge about one's freedom, but also about one's unfreedom, because to know that you are unfree to perform a certain action spares you the frustration of 'attempting the impossible', as Isaiah Berlin observed.[44]

In section II, "Privacy, Freedom, and Knowledge" we saw that invasions of privacy may lead to a reduction of knowledge about negative freedom. If subject B of the private information knows that A has disclosed private information about her to recipient C, but B does not know what C will do with the information (how she will revise her beliefs, and what actions or dispositions she will settle on), then B will have to suspend a number of beliefs about future negative freedom.[45] A lot hinges on whether B can predict C's belief revision and C's actions or dispositions. Suppose I believe that I can fly to London from Tehran. In one scenario I subsequently learn that my travel itineraries have been publicized, and I also learn that because of that my name has been put on no-fly lists of all airline carriers connecting Tehran and London. As a result, I know I am no longer free to fly to London directly. This constitutes a reduction of negative freedom, but not a reduction of knowledge

[44] Isaiah Berlin, *Two Concepts of Liberty* (Oxford: Clarendon Press, 1958), p. 29. This is not the place to discuss the argument for known freedom in more detail. See, apart from Berlin's inaugural lecture, Boudewijn de Bruin, 'Liberal and Republican Freedom', *Journal of Political Philosophy*, 17/4 (2009): 418–439; Carter, *A Measure of Freedom*; Hurka, 'Why Value Autonomy?'

[45] An agent 'suspends' belief about a proposition, P, whenever she does not adopt any doxastic attitude towards P. She does not believe that P is true, but nor does she believe that P is false.

about my freedom and unfreedom, as I do have accurate beliefs about my unfreedom to fly to London.

In another scenario, the only thing I learn is that my travel itineraries have been sold to some airline carriers. Not knowing much about the criteria that underlie no-fly lists, but knowing that my travel itineraries *may* be thought of as 'suspicious', I do not know for sure that I will be barred from flying. But neither am I sure that I will not, so I have to suspend my initial belief that I can fly to London. This constitutes a genuine reduction of known freedom.

In the examples discussed in section II, "Privacy, Freedom, and Knowledge", a hacker gained access to the financial records of a bank's customers, and lawyers of a criminal gang obtained information contained in the personnel files of undercover police officers who had investigated the gang's alleged drug conspiracy activities. As we saw, this led to a decrease in the victims' known freedom. Upon learning about the privacy invasion, the victims suspended their beliefs about their freedom and unfreedom.

Not all decreases in known freedom should be taken seriously when we weigh liberal interests, though. Agent A informs C, a notorious car thief, about the fact that B is the owner of a Porsche Turbo. Agent B learns about the disclosure, and claims no longer to know that her car will not be stolen. But B still parks the car in front of her house, often even leaving it with the key in the ignition. She still acts on the belief that her car is safe. So there is no demonstrable change of belief. Or suppose that A informs C, a reliable and law-abiding friend of B, about the fact that B is the owner of a Porsche Turbo. Agent B learns about the disclosure and decides to hire a person to guard the car 24 h a day. In this case, B's known freedom did in fact decrease – she did revise her beliefs about the likelihood of car theft – but she adopted an irrational, paranoid belief revision policy.

These two cases show that the belief change that underlies the decrease in knowledge about freedom has to be *demonstrable* and *reasonable*. To grasp something of what this concretely means, let us look at a recent legal case concerning

privacy, *Stollenwerk v. Tri-West Healthcare Alliance*.[46] This case is about burglary leading to the theft of laptops and computer hardware on which personal information was stored about Tri-West customers (names, home addresses, and social security numbers). The personal data of one of the plaintiffs (Brandt) were used on several occasions in attempts to illegally obtain a credit account; those of the other plaintiffs (Stollenwerk and his wife) were not. Stollenwerk judged the risk of identity theft high enough to buy credit monitoring services and additional insurance, and claimed damages accordingly. The court, however, rejected his claim.

Stollenwerk's *known* freedom decreased in demonstrable and reasonable ways. Stollenwerk's action of buying credit monitoring services and extra insurance clearly demonstrates that he changed his beliefs about the likelihood of future interference. He would not have bought such services had he thought that he had incurred no additional risks because of the burglary. Moreover, his beliefs were *reasonable* to adopt. Computer servers may be stolen for their hardware, but they are also stolen for the data stored on them. Furthermore, the fact that another person's data were in fact misused (which the court accepted) shows that Stollenwerk's suspicions were far from irrational. He did not, for instance, change his beliefs in paranoid ways, claiming an increased likelihood of, say, kidnapping or burglary of his house; and the court documents suggest that he was careful enough to request advise from insurance specialists.[47]

The *Stollenwerk* court, in common with many others, was unwilling to adopt this kind of reasoning, though. In one kind

[46] Stollenwerk v. Tri-West Healthcare Alliance, 254 Fed. Appx. 664 (2007).

[47] The burglary was even covered by national newspapers, in which many experts pointed out the risks run by the victims. *The New York Times* published an article two weeks before Brandt and Stollenwerk filed their original claim. This article quotes Tri-West's president as stating that, 'It is unlikely that people were breaking in for resale value…. They left things that were more valuable and easier to hock'. See Adam Clymer, 'Threats and Responses: Privacy; Officials Say Troops Risk Identity Theft After Burglary', *The New York Times* 12 January 2003.

of decision, courts have concluded that the plaintiffs lack standing to pursue their claims. In *Giordano v. Wachovia Securities, LLC*, for instance, a customer sued her financial services company because a package containing information about customers' names, addresses, and social security numbers was lost in transit by UPS. The court found that the plaintiff lacked constitutional standing to bring this action on the grounds that, as the plaintiff's claims about the possibility of future identity theft were 'at best… speculative', she had been unsuccessful in proving that she had suffered a compensable injury.[48]

In another line of decisions, courts did rule that plaintiffs have standing to bring suit. In *Ruiz v. Gap, Inc.*, for instance, the plaintiff entered personal information on a website when he applied online for a job at Gap. A laptop was stolen containing his and other applicants' information. Unlike in the *Giordano* decision, the court in *Ruiz* relied on an expert opinion about the probability of suffering identity theft. It accepted that in the first year after the breach the probability of identity theft is about five times as high as the average probability of identity theft (it rises from 4% to 19%), and therefore concluded that the plaintiff had standing to sue. However, since the plaintiff could not demonstrate any actual damage, the court did not find the increased risk of identity theft a compensable injury.[49]

Rather than awarding damages in data breach cases, the trend is only to require that customers be notified of data breaches. Now, it is surely true that notification does not go against individuals' known freedom. Using the statistics from *Ruiz*, if my personal information is breached there is a 19% chance that I will become the victim of identity theft within a year. As a victim of identity theft has to spend, on average, about 80 h and $850 to alleviate the consequences of that theft, it constitutes a significant form of interference.[50] Accordingly,

[48] Giordano v. Wachovia Securities, LLC, 2006 WL 2177036. For other relevant cases, see Jay M. Zitter, 'Liability for Risk of Future Identity Theft', *American Law Reports* 6th, 50 (2009): 33.

[49] Ruiz v. Gap, Inc., 622 F. Supp. 2d 908. *Pisciotta* and *Stollenwerk* are similar. See Zitter, 'Liability for Risk'.

[50] Eric Eisenstein, 'Identity Theft: An Exploratory Study with Implications for Marketers', *Journal of Business Research* 61/11 (2008), 1160–1172.

learning about the increased likelihood of identity theft advances one's known freedom.[51]

Even though a liberal will favor mandatory disclosure of data breach, she has good reason to question the court's conception of the predicament of data breach victims. To start with, she will dispute the courts' belief that the larger risk of future identity theft is 'speculative'. There are reliable statistical data about identity theft in the US, and to set these data aside as speculation does not do justice to the methodology that underlies them.[52] Now, it may be that the courts' judgments about speculative probabilities concern the *size* of the probabilities rather than the *source* of information about the probabilities. But that line of reasoning is equally dubious. A chance of 19% that you will have to spend 80 h and $850 to right the consequences of identity theft is a very substantial risk. Moreover, from a statistical point of view, what best characterizes the situation is not the mere figure of a 19% chance of identity theft, but rather the *fivefold* increase from 4% (average citizen) to 19% (after data breach).[53] So there is no ground to set aside the probabilities as 'speculative'.

The second reason to find fault with the courts is that they embrace the view that a risk of future identity theft does not constitute an 'actual' harm. Following the approach to the liberal value of privacy advocated in this paper, there are two ways in which disclosure of private information may harm the subject of that information. The first is a decrease of freedom: it may lead others to interfere or to form dispositions to interfere. Admittedly, as no plaintiff was able to demonstrate such harm in court, this first form of harm does not apply here. Yet, as I argued, the second way in which disclosure of private information may harm the subject is that it decreases her *known* freedom: the person's beliefs about her freedom and unfreedom deteriorate. What is important now is that the inadequacy of

[51] See footnote 25, and my observation about no-fly lists in section IV, "Privacy and Knowledge About Negative Freedom".

[52] Eisenstein, 'Identity Theft'.

[53] To see this, suppose that the chance of identity theft for an average US citizen were 18% instead of 4%. An increase to 19% due to data breach would now be entirely negligible.

these beliefs is far from hypothetical. They are faulty, not in a hypothetical future, but at the very moment of the data breach, and a direct consequence of that is that the person's present decision-making capacities are frustrated. She is less well-positioned than she was before the data breach to engage in responsible planning and decision making, because she will have to incorporate, in her current planning, the fact that her beliefs about certain freedoms and unfreedoms are less adequate than before the breach.

To summarize, I have argued that there are good reasons for the courts to rethink their reliance on a principle of 'no harm, no foul' in recent data breach cases. To be sure, this is not meant to downplay the difficulty the courts will face in ascertaining whether, after the data breach, plaintiffs revise their beliefs in demonstrable and reasonable ways. Nor should it obscure the fact that the argument for the liberal value of privacy is aimed in the first place at the liberal privacy skeptic, not the courts. Nevertheless, there is no reason why my argument, if cogent, should not also inform jurisprudence. Invasions of privacy may decrease a person's freedom, or her knowledge about freedom, and both constitute harm to her liberty interests.

V. CONCLUSION

My argument about the liberal value of privacy is cast in terms of a rather narrow concept of freedom, but it applies equally to any broader concept of freedom that subsumes pure negative freedom. To the extent that a decrease in pure negative freedom constitutes a decrease in, say, republican freedom – or any other concept for that matter – my argument shows that privacy has *republican* value, too.[54] Moreover, while my argument has been directed at the liberal privacy skeptic who fails to be convinced by arguments from perspective change, relation-

[54] See, e.g., Ian Carter, 'How are Power and Unfreedom Related?' *Republicanism and Political Theory*, ed. C. Laborde and J. Maynor (Oxford: Blackwell, 2008), pp. 58–82; Matthew Kramer, 'Liberty and Domination', in op. cit., pp. 31–57. Cf. Boudewijn de Bruin, 'Liberal and Republican Freedom'.

ships, or dignity, my defense of the liberal value of privacy adds to these arguments rather than contradicting them. It is easier to weigh one person's privacy against another's freedom of speech, say, if we use one and the same currency for both persons' interests: the value of freedom; that is, it is easier to compare the value of your freedom with the value of my freedom than to compare the value of your freedom with the value of my relationships or dignity. As a result, champions of the arguments from perspective change, relationships, or dignity have good reason to complement their views of privacy with the approach offered here. Nevertheless, the primary aim has been to show that theorists operating with pure negative freedom do not remain empty-handed where privacy is concerned. Even for them, privacy is valuable.

ACKNOWLEDGMENTS

Warmest thanks are due to Constanze Binder, Luc Bovens, Bert van den Brink, Matthew Braham, Amitai Etzioni, Hans Harbers, Martin van Hees, Frank Hindriks, Jan-Willem van der Rijt, Dan Solove, Chris Zurn, to audiences in Amsterdam and Utrecht, and to an anonymous referee of this Journal, for valuable comments on an earlier version of this paper.

OPEN ACCESS

Faculty of Philosophy
University of Groningen, Oude Boteringestraat 52,
9712 GL, Groningen, The Netherlands
E-mail: b.p.de.bruin@rug.nl