CCTV and Public Anonymity

Introduction

Time was when the zones of public anonymity stretched unbroken for miles, like a pre-twentieth century Amazonia. A person, particularly if she lived in a city, could leave her house and expect to remain more or less anonymous wherever she went, whatever she did. However, like the rain forest, this idyll is today under serious pressure, thanks to the depredations of digital technology. Unlike the forest, though, public anonymity has no equivalent of the World Wildlife Fund or the National Geographic Society to stick up for it. The threats include toll passes, swipe IDs, credit cards, and the GPS devices that most of us walk or drive around with. This essay will focus on perhaps the most obvious threat to public anonymity (hereafter simply *anonymity*): CCTV cameras and their accompanying face recognition software (hereafter simply *CCTV*). Why worry? I argue that anonymity is valuable both because it generally sustains privacy and, in so doing, promotes autonomy. I deny that whenever people go out they are implicitly consenting to a loss of anonymity (Goold 2006). I am naïve enough to suppose that we can protect anonymity where it is threatened and restore it where it has been lost. I reject the quasi-mystical assumption that technology is driven by an inner logic that makes it largely resistant to human attempts to reel it in (see Rule 2007). The inexorable march of technology need not imply the inevitable retreat and eventual defeat of anonymity.

I propose first to look at the concept of anonymity and how it relates to privacy. Next, I will ask why anonymity is worth defending. Third, I discuss the specific threats to anonymity that CCTV presents. I then offer some suggestions about how we might turn, or at least stem, the tide of public surveillance. I close with some thoughts on the irrational fears that generate the clamor for mass surveillance.

The Concept of Anonymity

I will not attempt to provide an analysis of anonymity. Instead I will touch on some aspects of the concept that will animate the rest of this essay.

More is needed for anonymity than namelessness (Wallace 1999). The mountain of digital information that a person produces as she goes through her routines is now potentially available from a single point. Several pieces combined can easily identify a person even without her name (Nissenbaum 1999; Zimmer 2010). Following Kathleen Wallace, I will assume that social inaccessibility is needed for anonymity (Wallace 1999). Social inaccessibility obtains when "others are unable to relate a given feature of the person to other features" (Wallace 1999, p. 24). For a while Walter Scott was known only to his readers as the author of *Waverley*. To them, in this capacity, he was anonymous. To borrow Helen Nissenbaum's expressions, Scott was "unreachable," or "out of grasp" for the vast majority of the public (Nissenbaum 1999). Yet presumably some of his readers also knew him as a fellow club member. He was obviously not anonymous to them in this respect, even though he remained so as the popular novelist. Of course, since identity is transitive, in knowing Scott his friends and acquaintances also knew the author of *Waverly*. However, they did not know him in this guise: he was unreachable as the best selling author, unknown to them as the distinguished novelist. They were unable to coordinate Scott's trait as club treasurer or boon companion with his trait as a novelist (Wallace 1999, 2008). If asked, all would have denied that their drinking buddy or whist partner had any literary celebrity. Their false beliefs protected Scott's anonymity. By shrouding his identity as the author *Waverly* Scott sought to isolate this trait from his other traits (Wallace 1999).

Although *anonymity* and *privacy* are closely related, they are nevertheless distinct. A person can lack anonymity while still enjoying privacy. Imagine that the president of the United States has absolutely no anonymity. Everyone knows who he is in all his guises, and he is instantly recognized wherever he goes, whatever his disguise. In no respect is he out of grasp. Yet he still has privacy when he retreats to the White House residence at the end of his long day. Also, it is possible to be anonymous while lacking privacy. Imagine a fitting room with hidden cameras, the images from which are contemplated by the local voyeur. Although the pervert has violated the customers’ privacy, their anonymity can remain intact all the while. I suspect that what people often really care about when their privacy has been invaded is that they have lost their anonymity. I would be far less concerned to find out that my apartment was rigged with cameras and recorders if I remained anonymous than I would be if my identity were also revealed.

Why suppose that anonymity is worth defending? I will assume for the sake of discussion that people rightly believe that their lives will go better if they are not surrendering their identity every time that they leave the house. They will feel freer to associate with whomever they like and will be less inhibited about behaving unconventionally. In short, they will be more autonomous. This is not to deny the obvious costs of anonymity. As anyone who has spent any time in a city knows, anonymity lowers the price of bad behavior, from gratuitous horn honking and car alarm “testing” to random violence. Would that this conduct didn’t exist. Nevertheless, in what follows I will assume that the benefits of public anonymity, particularly regarding autonomy, outweigh its costs.

Privacy and Anonymity in Public

Beginning with the publication of Jeffrey Reiman’s landmark “Driving to the Panopticon” in 1995, numerous philosophers and legal theorists have defended some degree of privacy in public and have warned of the digital threats to it (see, for example, Allen, 2011; Goold 2002, 2006; Nissenbaum 1997, 2004, 2010; Reiman 1995; Solove 2007; and Zimmer 2005). According to these authors privacy is about much more than concealing one’s dark side or preventing the revelation of intimate or embarrassing facts, information typically thought to be paradigmatically private. In fact, these thinkers deny that any information is inherently public. Yes, when a person heads off to work in the morning, she gives up some of her privacy. People can see how she is dressed, make judgments about her age, appearance, race or ethnicity, and social class. But in analog times her privacy was more or less sustained by the vagaries of memory and the scant and scattered records of her activities, particularly if she lived in a large city. When she shopped, she left no digital records of her purchases. Unless she were a regular at a given store, the odds were that by the end of his shift the cashier would not remember what she had bought. A day later there was a good chance that he would forget that he had served her at all. Moreover, no CCTVs tracked her way to or her movements in the store itself. If she drove, she used no electronic toll pass. If she parked on the street, she fed coins into a software-free meter. No longer: Now just by leaving the house she is helping to compose a detailed electronic narrative of her routines, as well as of her departures from them. Despite these changes, today's partisans of public privacy deny that just because the woman's business is performed in public she has surrendered all privacy there, that nearly all she does beyond her own four walls is "up for grabs," to use Helen Nissenbaum's phrase (2010, p. 213). Digital technology has raised the profiles of our public lives, since so much of what we now do begets digital records tied to our identities. Moreover, thanks to extensive digital networks, the information can be spread fast and wide to countless unknown recipients, which further diminishes our control over the information.

The above-cited theorists have called for protection of some measure of privacy in public. I agree but would like to add that what is more immediately at stake is anonymity. It is anonymity that chiefly protects one's privacy in public. The main reason that we could enjoy a greater measure of privacy in public in the old days is that our activities there were more anonymous then. I would like to look now specifically at how CCTV is adverse to anonymity.

CCTV and Anonymity

It is no secret that the number of CCTVs in public has grown dramatically in the last couple of decades. I do not assume that there is anything nefarious behind the trend. Law enforcers plausibly see CCTV as a promising and potentially cheap way to reduce crime. Governments reasonably look to the technology as an effective means of tracking terror suspects. In both cases the worthy goals are increased security. Businesses and other private organizations are also concerned about security, as well as about shoplifting and employee theft. Again, these seem like perfectly good reasons to set up cameras. Nevertheless, there are numerous reasons to be wary of the proliferation of video surveillance. I would like to discuss a few of these now, particularly in the context of police and government sponsored CCTV.

At first blush it might not seem that video surveillance threatens anonymity. After all, if a person is anonymous as he saunters down Fifth Avenue at lunchtime, doesn't he remain so even though his image is captured by a couple dozen cameras? Not any longer. With face recognition software a current image can be matched with previous images stored in a database, possibly resulting in full identification and partial tracking.[1] Thus, his stroll is a lot more public than it used to be.

Second, as Benjamin Goold points out, being caught by a camera is not the same as being watched by a police officer (2002; see also Patton 2000). To begin with, unlike the police officer, surveillance cameras are often hidden or at least tricky to spot. If you're uncomfortable in the presence of the officer, you can slip away. But it is tough to move away from a camera you don't see (Smithson 2003). Also, you can't tell if the camera is zooming in on you, whereas you could see if the officer is reaching for his binoculars and training them on you. This violates one of Helen Nissenbaum's norms of information flow. For Nissenbaum the flow of all personal information, public or private, is governed by such norms (Nissenbaum 2004, p. 137). Violation of an information norm gives us a presumptive reason for objecting to the policy or practice that permits it. The norm in question here is *notice* (Nissenbaum 2010). We generally expect a heads up when someone is gathering information about us. In particular, if a stranger is determining my identity, I should know that he is doing so. If CCTV regularly transgresses this norm, the public has a prima facie reason for demanding that the technology be removed or at least for being notified of its presence. I accept Nissenbaum's point here.

Third, even when the cameras are in plain sight, we don't see the people behind them. This violates another of Nissenbaum's norms, reciprocity (Nissenbaum 2010). Crudely, this norm implies that, if you can see me, I should be able to see you. More to the present point, reciprocity implies that if you know my identity I should know yours. CCTV surveillance turns this norm on its head. Consider encountering a police officer in public again. Unless I am a celebrity or a notorious gangster, he won't know me from Adam. He on the other hand wears a name tag and a numbered badge. If I think that he has me fixed in a hostile stare, I can accost him and take note of his name and number. By contrast, I don't know the identities of those behind the cameras, nor is it obvious how I might find this out. However, with ever improving biometrics and lenses that can permit identification of me from hundreds of yards away, or at night, I may well not be anonymous to them. As in the previous paragraph, the fact that the practice violates an information norm does not show that it is wrong. It might be that the surveillance promotes some compelling social good, like security, that could not be achieved as effectively by other means. But a lot of video surveillance is devoted to catching double parkers, speeders, and red light runners, hardly acts that tear at the social fabric. Again, I accept Nissenbaum's point: where CCTV transgresses this norm, the burden is on officials or policy makers to justify the transgression.

Someone might object that nosy neighbors also violate Nissenbaum's two norms, and trivially they do (see Ryberg 2007). Benjamin Goold (2008) considers this kind of case. He contrasts a mildly voyeuristic neighbor who takes in my daily comings and goings with government-sponsored CCTV surveillance of me. The crucial difference is that the state, unlike the neighbor, has a legal monopoly on the use of force and thus can "under certain circumstances deprive me of both my liberty and my property" (Goold 2008, p. 45). Although the neighbor can come to know my identity, there is considerably less that he can do once he has determined it. Moreover, the images can be stored indefinitely. As implied above, this marks a significant break with the past, when we left no digital trail in public and most of those who did see us either would scarcely notice or would soon forget. Think of all people that you might have seen as you made your way to work today. How many could you pick out of a lineup by this time tomorrow? How many could identify you?

Another problem relates not so much to the surveillance itself as to its proliferation. Cameras tend to beget cameras (Rule 2007). One reasonable guess about why is that, as more parts of a city are blanketed in surveillance, the places not under the covers come to be perceived as less safe than the monitored areas (Goold 2006). Intuitively, the idea is that bad guys will focus on the neighborhoods without cameras. Few would choose to live on the only block in town without security cameras (Economist 1999). At the very least, people become inured to such technology, even if initially they might have been concerned about the amount of tracking that it permits (Rule 2007).

A second explanation is consistent with the first but takes the point of view of the surveillers. Once a given type of surveillance technology becomes established, it tends to take on a momentum of its own. We are now well on the way to having a growing surveillance-industrial complex. In this regard, the cameras are like superhighways: once built, a large group of people, some of them well-placed, comes to have a keen interest in maintaining them and, further, in persuading the rest of us that more are needed, even if the initial case for them was weak (Rule 2007). Just as the countryside now has a bumper crop of roads to nowhere, so our streets, buses, and subways continue to sprout surveillance cameras of questionable value. And just as it is unlikely that anyone in power will ever seriously propose ripping up that gratuitous stretch of interstate between Albany and Binghamton, so it becomes difficult to imagine a campaign to remove most public surveillance cameras, even if there is no evidence that they make the streets or skies significantly safer. Those government agents involved in security certainly have an interest in persuading the rest of us that the threats are greater than they actually are. Although there is no reason to suppose that any of this is born of some Orwellian conspiracy, we should nevertheless be wary of spiraling security budgets and increasing public surveillance.

What should we do? First, we should insist that the surveillance go no further for the time being. As James Rule notes, "*extensions of mass surveillance are far easier to forestall than to* *dismantle*. . . . Opposition to major surveillance systems has its best chance *before* they are up and running" (2007, p. 152; italics in original). Second, officials should to be able to demonstrate that the cameras would reduce crime or increase security not just on the block in question but in a broader area and that this couldn't be achieved by less intrusive means. Third, given that some public places will continue to have cameras, I suggest that the law enforcers and government agents responsible for them be fully accountable. As Benjamin Goold suggests, the program be could modeled on the transparency of Bentham's panoptic prison (Goold 2006). In this scheme, not only would the prisoners potentially be under constant watch, but so too would the guards and the warden, since the prison would be always be "thrown wide open to the body of the curious at large" for unannounced walk throughs (Bentham 1995, p. 47). The only people who could object to such openness would be precisely those who had something to hide. Surveillance programs should be subject to similar accountability, perhaps by granting the media unfettered access to the operation. The public should have full assurance that the cameras and the immense video files that they generate are only being used to achieve stated goals in a given area and not also for tracking or spying.

We also need to know how much it all costs. I reject the dogma that no amount of security is too much. Budgeting is a zero-sum game. The millions lavished on CCTV is money that is not spent on other potentially more beneficial programs, from expanded cancer research to improved public transportation (Chapman and Harris 2002). And as Bruce Schneier observes, "like all large infrastructure projects, the costs to operate and maintain these systems are significantly larger than the costs to develop and deploy them" (Schneier 2003, p. 245). These are points that surveillance advocates often conveniently ignore.

Additionally, the costs of CCTV surveillance fall disproportionately on city dwellers (Goold 2006). Rural people and suburbanites typically have backyards. Most city people don't. Their outdoors spaces are generally public. As parks and streets accumulate more cameras, it becomes increasingly difficult for urbanites to enjoy anonymity. The burden is especially great for the poor, who tend to live in cramped apartments (Goold 2006). In fact there is some evidence that public housing projects have among the thickest concentrations of the devices (Smithson 2003). The homeless too, obviously, bear undue share of the burden (Goold 2006).

Conclusion

I have tried to show that CCTV represents a signal threat to anonymity. I have suggested that anonymity is valuable, particularly insofar as it promotes autonomy. The trouble with losing great swaths of anonymity is that we are engaged in a grand social experiment, the outcome of which we can only guess at. As Anita Allen puts it, proliferating surveillance will "rewrite the rules of social exchange, adding to the risks of appearing in public" (Allen 2011, p. 136). As a result, "gone is the anonymity of the crowded sports stadium or the flaneur's city street" (Allen 2011, p. 137). I should point out that am not arguing that all CCTVs be scrapped, but I am attempting to draw attention to the social costs of unleashing this technology. Of course, a lot depends on whether or not the cameras actually make us safer, an empirical question that is beyond the scope of this essay. However, there are good reasons for supposing that the clamor for public surveillance isn't fully rational. People tend to fear events that kill many people at once, like plane crashes, significantly more than those that kill one or a handful, like a car crash, even if they're far more likely to be a victim of the latter (Chapman and Harris 2002). If the money that the US government has spent directly or indirectly prosecuting the war on terror is any indication, people also have an outsized fear of being a victim of terrorism. But the odds of being one are approximately zero. By one reliable estimate roughly 4000 people have died in terrorist attacks on American soil in the last 240 years (Schneier, 2003, p. 239). Compare this with other relevant figures in the United States for 2011. In that year accidents killed nearly 123,000 people. Of these more than 37,000 were so-called "transport accidents," that is, deaths involving cars, buses, and trucks. Terrorists killed no one (National Vital Statistics Report 2012). Of course, unlike traffic deaths, which don't vary dramatically from year to year, the risk of terrorism is difficult to assess.

Policy makers do have to consider people’s fear of terrorism, however irrational. Nevertheless, to paraphrase Hume, ideally we should base our public policies on what we have good evidence for and not on what we don’t have good evidence for. As for crime, it has plunged, at least in the United States, since the 1980s. Much of this fall happened long before video surveillance was common, yet the cameras keep coming. The burden should be on those who advocate the spread of this technology to make a strong case for its benefits and to show carefully that these benefits outweigh the social and very considerable financial costs.

Note

1. I concede that due both to the quality of images and to software shortcomings CCTV is not yet a surefire way of identifying passersby.

References

Allen, A (2011). *Unpopular Privacy: What must we hide?* Oxford; New York: Oxford University Press, 2011.

Bentham, Jeremy. 1995. *Panopticon writings*. Ed. M. Bosovic. London and New York: Verso.

Chapman C. and A. Harris. (2002). "A skeptical look at September 11." *Skeptical Inquirer* 26(5). 29-34.

Economist (1999). Surveillance society. *Economist* 351(8177), 21-23.

Goold, B. (2002). Privacy rights and public spaces: CCTV and the problem of the "unobservable observer." *Criminal Justice Ethics* 21.1, 21-27.

Goold, B. (2006). Open to all? Regulating open street CCTV and the case for "symmetrical surveillance." *Criminal Justice Ethics* 25.1, 3-17

Goold, B. (2008). The difference between lonely old ladies and CCTV cameras: A response to Ryberg. *Res Publica* 14(1), 43-47.

National Vital Statistics Report. (2012). 61(6), www.cdc.gov/nchs/data/nvsr/nvsr61/nvsr61_06.pdf; last accessed March 6, 2013.

Nissenbaum, H. (1997). Toward an approach to privacy in public: Challenges of information technology. *Ethics and Behavior* 7(3), 207-19.

Nissenbaum H. (1999). The meaning of anonymity in an information age. *The Information Society*, 15(2), 141-44.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review* 79 119- 57.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life.* Stanford: Stanford Law.

Patton, J. (2000). Protecting privacy in public? Surveillance technologies and the value of public places. *Ethics and Information Technology* 2, 181-87.

Reiman, J. (1995). Driving to the panopticon: A philosophical exploration of the risks to privacy posed by the information technology of the future. *Santa Clara Computer and High*

Technology Law Journal, 11(1): 27-44.

Rule, J. (2007). *Privacy in peril*. New York: Oxford University Press.

Ryberg, J. (2007). Privacy rights, crime prevention, CCTV, and the life of Mrs. Aremac. *Res Publica* 13, 127-43.

Schneier, B. (2003). *Beyond fear: Thinking sensibly about security in an uncertain world.* New York: Copernicus Books.

Smithson, M. (2003). Private lives, public spaces: The surveillance state. *Dissent* (Winter).

Solove, D. (2007). *The future of reputation: Gossip, rumor, and privacy on the internet.* New Haven: Yale University Press.

Solove, D. (2011). *Nothing to hide: The false tradeoff between privacy and security*. New Haven: Yale University Press.

Wallace, K. (1999). Anonymity. *Ethics and Information Technology*, 1, 23-35.

Wallace, K. (2008). Online anonymity. In *The Handbook or Information and Computer Ethics*, ed. by K. Himma and H. Tavani. New York: Wiley.

Zimmer, M. (2005). Surveillance, privacy and the ethics of vehicle safety communication technology. *Ethics and Information Technology* 7, 201-10.

Zimmer, M. (2010). “But the data is already public”: On the ethics of research in Facebook. *Ethics and Information Technology* 12, 313-25.