Privacy Essay

Introduction

In the last couple of decades society has been transformed by technology, but there is a growing sentiment that the technology we love is working against our values in ways that are not clear. Privacy is one such area where we ought to be concerned, because while technology is changing the way we live, it does so by integrating heavily with our minds. What before was the quiet comfort of our thoughts can now be examined and used by commercial and governmental actors in the name targeted advertisements, preventing terror attacks, politics, and much more. Modern technology has many aspects so we should resist taking a hard stance, but in this essay I look at ways in which technology works against privacy values that we seem to hold in Western society. I will tackle the most common objection to privacy concern, namely the "Nothing to hide" argument, and argue for a more nuanced view of privacy.[1]

What is privacy?

Defining privacy has long been a challenge for scholars. It is difficult because we use it in inconsistent ways, and it has come to mean different things to different persons. As Judith Jarvis Thomson observes (Thomson 1984).

> Perhaps the most striking thing about privacy, is that nobody seems to have any very clear idea what it is. But our inability to define privacy has not meant that we stop using the term. In legal and political debates, privacy is often invoked as a core value, but in the absent of a definition we struggle to compare it against conflicting interests. This has caused privacy to lose out in many situation, because courts and legislators might not be able to recognize when and how privacy is implicated.

There have been several attempts at conceptualizing privacy. One could for instance define it in terms of the private-public spheres. Information that is readily available to the public like race cannot be considered private information, as that is information we cannot keep out of sight. The sharp distinction between private and public gives maybe the clearest definition

[1] TODO: this intro needs to updated

of privacy, but it has some large problems that we will discuss later.[2]

A related and common approach is to define privacy in terms of intimacy. This was well put by philosopher Julie Innes.[3]

> The content of privacy cannot be captured if we focus exclusively on either information, access, or intimate decisions because privacy involves all three areas. ... I suggest that these apparently disparate areas are linked by the common denominator of intimacy—privacy's content covers *intimate* information, access, or decisions.
> This is also a narrow and bounded conception of privacy, but it comes at the cost of either being too narrow or broadening the definition of intimacy to mean privacy, which isn't a good solution. Many persons would not regard their email or bank account number as intimate, but they sure are private.

There are two big challenges in defining privacy. (1) The definition must capture the features of privacy in a wide set of contexts, and (2) the definition must be able to cope with the rapid advances in information technology. Following Solove's lead, we will resist the temptation of defining the core of privacy. Instead we will view privacy more as a family resemblance problem. Solove creates a taxonomy of four main categories with in total sixteen subcategories where he argues that privacy concerns are relevant (Solove 2007, p 758).

- **Information collection**: Surveillance, Interrogation
- **Information processing**: Aggregation, Identification, Insecurity, Secondary use, Exclusion
- **Information dissemination**: Breach of confidentiality, Disclosure, Exposure, Increased Accessibility, Blackmail, Appropriation, Distortion
- **Invasion**: Intrusion, Decisional Interference

Viewing privacy in this manner, Solove argues, will allow us to focus on the problems instead of getting hung up on the terms. Another way of focusing on the problems is shown to us by the European Unions (EU) General Data Protection Regulation (GDPR). GDPR defines the notion of *personal data*, as ("What Is Personal Data?" 2019)

> Personal data is any information that relates to identified or identifiable living individual.

When multiple pieces of pseudonymized data can be combined to identify a person, then it also counts as personal data. With GDPR, there is this idea that persons own their personal data, and personal data is any information about a person that has not been anonymized. Solove's taxonomy of privacy goes well with the notion of personal data, because the taxonomy lays out areas where personal data might be used.

Nissenbaum argues well for another view of privacy. I short, privacy is the expectation of contextual integrity. This view is able to explain well when and why we feel that privacy has been violated in some contexts. Should find a way to merge this with Solove's view.

[2] this hasn't been discussed yet

[3] Julie C. Inness, *PRIVACY, INTIMACY, AND ISOLATION*, 56 (1992)

For the remainder of this essay we will use this pluralistic notion of privacy and attempt to reframe questions of privacy in terms of personal data, as this might help us value privacy against other important values.

The value of privacy

Given the amorphous nature of privacy it can be hard to articulate ways in which it is important. Great works of fiction, like Orwell's *1984* and Kafka's *The Trial* , have shown us how societies completely lacking in privacy considerations can turn out. In *1984*, the state watches every move of every citizen depriving them of freedom of speech and even thought. In *The Trail*, the protagonist is goes up against a legal system which knows much about him, but excludes him from knowing what they know. Both *1984* and *The Trial* paint bleak worlds where individuals are powerless because of a lack of privacy. While these books are great for illustrating certain arguments, we should be able to defend privacy solely based on reality.

In an article for teachprivacy.com, Solove gives a list of 10 reasons why privacy matters. One of the reasons he gives is that privacy puts firm limits on the power of organizations over individuals. By giving every person control over their own data and where it may or may not be used, privacy empowers everyone against encroachment of large organizations. Privacy is key to maintaining a successful democracy, because citizens need to be able to communicate or organize without government involvement. Privacy is also essential for individual expression, so that people are able to explore their values free of intrusion by others. For instance a christian person who is also an in the closet homosexual. He can be active on public online forums discussing with other people in similar situations, but until he is sure about his own feelings he wants to keep it hidden from his local community.[4]

Why privacy loses

argue that security and government surveillance is a problem distinct from privacy in public which relates more to private companies and value alignment. "The digital person" presents an argument like this

Privacy v. Security

Most people in western society agree that privacy is a value which is worth protecting in the abstract, but when the messy details of reality hits us, we struggle to defend privacy. The problem is that often privacy concerns come into conflict other concerns. In the aftermath

[4]We could have a counterargument here. Recently there have been revelations about secret Instagram networks, in which mostly teenage girls share self-harm images with each other. This is also a case of privacy allowing expression of the individual, but it seems damaging because there is now way for adults to discover it. One could construct an argument that children and teenagers are in a unique situation and should not have the same privacy protections from their parents.

of the September 11 attacks, the US government started an all out fight against terrorism which involved secretly giving the National Security Agency (NSA) the power to wiretap telephone calls without warrants (Solove 2007, 745). NSA and other government agencies argue that *data* really is the only way to prevent terrorist attacks. With data it is possible to look at previous attacks, understand how the terrorist behaved prior to the attacks, and use that to find terrorists before the next attack. This wiretapping program and several other government led surveillance programs designed to find criminals and prevent terrorist attacks created big debates over privacy. A common objection to privacy advocates is "I have nothing to hide, so I have nothing to fear". Alternatively, it is posed as a question "If you aren't doing anything wrong, then what do you have to fear?". This argument puts privacy interests as so low as to have nothing to say when competing interests are present. It is an example of what Nissenbaum refers to as a normative knock-down argument (Nissenbaum 1998, 571).

Obviously, mass surveillance isn't unique to the US. In London alone, there are 420,000 closed-circuit television cameras, equaling about 48 cameras for every thousand people.[5] It is the city in the world with most surveillance cameras per citizen, and the cameras have become an important asset to the police force. In Britain one of the key arguments for having more surveillance is the nothing to hide argument.[6] The nothing to hide argument is a strong claim that privacy interests don't really matter when weighed against security. In fact, it seems to be too strong so in its most extreme form it's easy to take down. Canadian privacy expert David Flaherty opposed the argument[7]

> There is no sentient human being in the Western world who has little or no regard for his or her personal privacy; those who would attempt such claims cannot withstand even a few minutes' questioning about intimate aspects of their lives without capitulating to the intrusiveness of certain subject matters.

This and other quick responses to the nothing to hide argument, seem to conflate "nothing to hide" with "everything to show". Judge Richard Posner has argued for the argument, by saying privacy is often, he claims, invoked as a right to conceal discreditable facts about one self. In fact Posner claims that modern computer technology can in fact be privacy enhancing, because the machines will be able to sift through enormous amount of data and filter out data which has no intelligence value. This would keep most data out of the sight of any intelligence officer.

Solove (2007) develops a stronger and more nuanced form of the nothing to hide argument. He grants that information gathering programs will result disclosure of information to a few government officials, but mainly to government computers. By being careful, we can ensure that very little sensitive or embarrassing information is ever leaked out of government. Granted there may be cases where limited embarrassing information is disclosed to more people than was necessary, but in total the security concerns around preventing crime and terrorist attacks are greater than the minimal privacy concerns.

[5] Adam Satariano, 2019 ,New York Times, https://www.nytimes.com/2019/09/15/technology/britain-surveillance-privacy.html

[6] citation needed. This was claimed by Solove in his essay, but there should be a better source for this.

[7] this is quoted from Soloves article, but should be able to find the direct source of this

When posed this way, the nothing to hide argument clearly lays out its assumption and limits. By stating that the disclosure of information has to be limited, it is not taken down by the common retorts. There are two fundamental problems with this argument. 1. A narrow view of privacy. 2. It stacks the decks against privacy in non-obvious ways.

(1) The nothing to hide argument bakes in a view of privacy, which is that privacy is about concealment of information. But as we have seen concealment is just one aspect of privacy. Other aspects include exclusion, secondary use, blackmail. By buying into the assumption that privacy is concealment, the discussions end up being about what people may or may not want to conceal. Thus we should resist this narrow view of privacy. (2) The other problem is that is fails to recognize that privacy problems often are structural. With privacy, there are rarely any visceral injuries one can point to. As Bartow puts it, privacy has a lack of "blood and death, or at least broken bones and buckets of money.".[8] This may actually be a reason to value security higher, because security is actually concerned with "blood and death". The problem is that privacy harms by definition occur at the individual level, whereas harms from terror attacks also occur on a grander level. Phrases like "The U.S. is under attack." or "We need to protect London from criminals." do this implicitly. This places privacy concerns fo the individual at odds with security of the nation, which severely stacks the decks in favor of security. But loosing privacy affects more than the mere individual, because while privacy is inherently personal, it is also constitutive of western societies[9] and we must not forget to value privacy at the societal level.

While defending privacy, we must also acknowledge the strength of the arguments for security. The pragmatic truth of the matter is that we need some surveillance programs and they will inevitably encroach upon privacy interests. The discussion to be had is not whether or not to stop the programs, that would be futile or even dangerous as attorney general Alberto Gonzales puts it.[10] Instead we should focus on designing the programs such that they operate within bounds accepted by the public and the law.

one of the reasons the surveillance programs in London are controversial, is that they are primarily decided by the police officers. The public has no say in what kind of surveillance it deems ok and no way of affecting it. This point could be made to support the argument above, but it needs more research.

Privacy in public

Privacy in public presents us with entirely new challenges. Privacy in public distinct in that the problem only arises due progress made in technology. A big proponent of this concept is Helen Nissenbaum. She argues that there is a systematic relationship between privacy and information that can be drawn from public sphere, and that this public information often is ignored by theories of privacy.

To understand why privacy in public often has been dismissed, we will begin with the

[8] citation needed, from soloves paper

[9] solove claims, several scholar have argued this. Investigate claim and citation

[10] quote from Alberto Gonzales here

private-public dichotomy. We use the terms "private" and "public" differently depending on the context, but often it is used to separate individuals and private institutions from governmental institutions. "Private" may also indicate an intimate familial and personal realm, while "public" is everything outside. With the distinction between private and public in mind, it is intuitive to conclude that privacy is something which applies in the private realm alone. Nissenbaum (1998) rejects this conclusion and argues privacy in public is a genuine privacy interest.

Outline of an example to make the discussion clearer. Want to be able to argue that something in this example is a privacy violation.[11] - Alice is a person. - She usually goes to the same store to shop for daily groceries. - Before paying, she swipes her member card, giving her a small discount. - The store builds up a shopping profile of her over time. Based on the items she buys, they estimate her income, hobbies, dietary interests, whether she has pets. She shops at quite irregular times so the store infers that she is most likely a student. Based on her purchases they are able to estimate that she is a female, vegetarian, non-smoker, above average healthy person. - The store sells this profile to an advertisement company for further use.

todo: unorganized collection of notes

this section contains notes about things I wish to include but have not found a proper place for in the text.

What are the consequences of privacy violations? This will be dependent on the situation but it should be possible to articulate what they are in the example above

Stanley Benn: Privacy founded on utilitarian concerns are prone to misuse. Attempts to base privacy on a fundamental respect for persons.

> Covert observation—spying—is objectionable because it deliberately deceives a person about his world [that is, it transforms the situation he thinks is unobserved into one which is observed], thwarting, for reasons that *cannot* be his reasons, his attempts to make a rational choice.

Jeffrey Reimann builds upon Benn's view of privacy

> Privacy is a social ritual be means of which an individual's moral title is conferred.[12]

Health-monitoring and contextual privacy: If we buy a smartwatch which monitors our health, we give up privacy of that health data in a very specific context. We expect the data to be analyzed and help us make more healthy choices or understand our bodies. If the health data is also sold to and insurance company, it would violate our privacy because the data will then be used in an entirely different context.

Nissenbaum, Helen. 1998. "Protecting Privacy in an Information Age: The Problem of Privacy in Public." *Law and Philosophy* 17 (5). Springer: 559–96.

[11] write this in proper form

[12] conferred="granted/given/has"

Solove, Daniel J. 2007. "I've Got Nothing to Hide and Other Misunderstandings of Privacy." *San Diego L. Rev.* 44. HeinOnline: 745.

Thomson, Judith J. 1984. "The Right to Privacy." *San Diego L. Rev.*

"What Is Personal Data?" 2019. 2019. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data/_en.