Tavani, H. T. (2013). *Ethics and technology: Controversies, questions, and strategies for ethical computing*. (4th ed.) Hoboken: Wiley.

Chapter Summary – Chapter 5.

> ***Please note*** *– this summary is no substitute for actually reading the chapter. I primarily develop these summaries myself to help with a lecture presentation but I am happy to make them available to you – they typically summarise the main points of the chapter – you'll need to read the chapter for the detail. I apologise for any typos or grammatical errors. As I say I mainly develop these for my own use.*

Privacy in Cyberspace

By Steve McKinlay 09.04.2020

Almost on a daily basis we hear about issues to do with privacy in cyberspace and from the context of government or corporations collecting data and information about almost all aspects of our lives. This chapter looks at many of the issues related to the use of cybertechnology and related privacy issues.

Tavani makes the point in the opening paragraphs of the chapter that even if you do not use a computer it is virtually impossible to avoid having electronic data collected about a variety of your everyday activities. Everytime you fill out a form, use a bank account or credit card, stroll around your local mall or public place (CCTV cameras) information is potentially being gathered and this could threaten aspects of your privacy.

Are Privacy Concerns Associated with Cybertechnology Unique?

Privacy is not a new issue – personal privacy concerns obviously existed prior to modern computing (cameras, telephone etc.) However, we consider the impact that computing has had on privacy with respect to the

- *Amount* of personal information that can be collected
- *Speed* at which personal information can be transmitted
- *Duration* of time that information can be retained for
- *Kind* of information that can be collected, and exchanged

Additionally to these particular issues consider the many different ways our personal information can be manipulated (merged, matched, data-mined) once it has been collected. Data mining in particular can be used to discover patterns in our behaviour (purchasing habits, or web surfing activities etc.) this kind of technology certainly did not exist prior to the PC.

So, while issues to do with privacy are not necessarily new we can certainly make the claim that cybertechnology has arguably exacerbated them.

What is personal privacy?

Like many general terms defining privacy can be difficult – the concept is multifarious. Privacy is often discussed in terms of something that can be lost or diminished – a metaphor which suggests privacy might be like a sort of repository of information that can be diminished or eroded. Alternatively we often consider our privacy might be intruded or invaded (invasion of privacy) – this constitutes some kind of spatial metaphor. Or we might consider our privacy breached or violated. Suggesting that our privacy deserves some kind of legal protection.

We can think of privacy in a descriptive way, the notion of us having privacy, and a normative way, in that we have a right to privacy.

The concept has changed over the years, most recently when we think of our privacy we often think of it as having control over our personal information (informational privacy). Tavani briefly explores two other conceptions of privacy.

Accessibility Privacy – freedom from unwanted intrusion.

Tavani draws upon work by Warren and Brandeis (1890) who suggested privacy could be understood as being left alone, or being free from intrusion. This paper was one of the first arguments that made reference to privacy as a legal right in the US. Interestingly there is no mention of privacy in either the constitution or the bill of rights. Warren and Brandeis suggested that the legal right to privacy is grounded in the "right to inviolate personality" and this was in response to new technology of the time – the camera. Photographs of people began to appear in newspapers, gossip columns for example along with stories that were defamatory and sometimes false. Warren and Braindeis believed that individuals had a legal right to not be intruded in such a manner.

Decisional privacy – freedom from interference in personal affairs

Interestingly this form of privacy emerged as a result of reproductive technologies associated with contraception. A US court (1965) ruled that a person's right to get counselling about contraceptive techniques could not be denied by state laws. These laws have been appealed in many controversial court cases such as those associated with abortion and euthanasia. The focus is on ones right not to be interfered with and as such this form of privacy is distinguished from accessibility privacy and informational privacy.

Informational Privacy

Privacy is often considered with regard to the amount of data and information that is constantly gathered about us – the typical analysis considers it in relation to one's ability to restrict access to and control the flow of one's personal information. Questions arise such as who has the right to access one's personal information? What kind of control do I have as an individual to control the ways information is gathered, stored, recombined, exchanged, sold etc.

Moor's account of Privacy.

James Moor (2000) introduces an account of privacy that includes the principles of nonintrusion, non-interference and informational views.

> *An individual has privacy in a situation with regard to others if and only if in that situation the individual is protected from intrusion, interference and information access by others.*

Note Moor uses the term "situation" which leaves the context wide open – for example a situation could be within an activity, or a relationship or it could be storage of information within a computer system.

Moor makes a distinction between *naturally private* and *normatively private*. This allows us to differentiate between situations and the conditions required for (a) having privacy and (b) having a right to privacy. This allows the distinction between a loss of privacy and a violation of privacy. A naturally private situation is characterised by Moor as one where one is protected by natural means such as physical boundaries, Moor gives the example of hiking along in the bush. Your privacy might be lost if you come across others, but we wouldn't say it has been violated. On the other hand when at home we have a normative right to privacy, if someone snoops around your house and peeps through your window, we would say our right to privacy within our own home is violated.

Tavani gives a couple of good examples on pg 137 worth reading.

Privacy as contextual integrity.

Moor's conception of privacy includes the concepts of "situation" and "context". Some however argue that these concepts are too broad. Nissenbaum (2004, 2010) develops her model of privacy as "contextual integrity". How Nissenbaum's model differs is that she links adequate privacy protection to norms of specific context. Within certain contexts we would generally agree to share certain information appropriate to the context. For example, we agree to share our medical history and information with our doctor in exchange for appropriate medical care, we wouldn't however want this information shared with the general public or other authorities.

She refers to two types of norms

- Norms of appropriateness
- Norms of distribution

Questions to ask are – is it appropriate (or inappropriate) that a particular type of personal information is shared within a certain context. Similarly norms of distribution consider the restriction or limit of the flow of information within and across certain contexts. The contextual integrity of the flow of personal information is maintained when both norms are respected.

It's important to note here that we need to attend to the context within which the information flows not just the nature of the information itself. This is important in determining whether protection of privacy is required.

Tavani explores the contextual integrity approach via a case study. I urge you all to read this for yourself.

Why is privacy important anyway?

If you've watched the Mikko Hypponen Youtube video you'll notice that he argues that personal privacy is one of the foundations of democracy. What he seems to be saying is that privacy is an intrinsic value or right that we are all entitled to. Often we hear the call "if you have nothing to hide what are you worried about" however, this isn't the point. I think Hypponen's point is salient – quite frankly it's none of anyone else's business what I might be looking at on the internet, or what I am discussing via email with a friend, lover or family member.

Tavani wonders if the concept of privacy has different value for different generations. With many millennials and even gen X and Y quite happy to post "away" messages on messenger services disclosing their whereabouts. Add to this the variety of smart phone apps that geo-code our location when we post messages to twitter or Facebook. Earlier generations (and interestingly people that were raised in authoritative regimes such as the former soviet union states) are often far less liberal with their personal information.

Tavani quotes Westin, in arguing that countries with strong democratic political institutions might value privacy more. He goes on to argue that countries such as China and Singapore place a higher significance on broader social values than personal privacy. (Although there is no real evidence presented in the text for this). In any case it seems that while personal privacy to a degree appears to be a universal value, it also seems to vary in degree across cultures. As a result, it may prove difficult to get universal agreement on privacy laws and policy in cyberspace.

Is privacy an intrinsic value?

Recall the difference between instrumental (or material) value and intrinsic value – for example, happiness is intrinsically valued because we value it for its own sake. On the other hand money is instrumentally valued because it offers some means to an end, ie it can be exchanged for something else.

It is difficult to argue that privacy is intrinsically valuable. However it seems it is something more than just merely instrumentally valued. Privacy is essential to achieve some other ends, such as trust and friendship. Intrinsic values are associated with necessary conditions, whereas instrumental values with contingent conditions (philosophy speak for accidental or non-necessary conditions). Fried argues that while privacy in itself may not be intrinsically valuable it is a necessary condition for achieving other ends.

Moor agrees privacy is not intrinsic but believes it is an articulation or expression of the core value "security" which is essential for human flourishing. Due to the explosion of cybertechnology, privacy Moor argues is increasingly important for expressing the core value security.

Spinello (2010) argues that privacy plays a key role in promoting human well being. Recall Mikko Hypponen argues that it is the foundation of democratic societies, although he doesn't actually offer much of an argument for this. Interestingly Judith DeCew (2006) argues that the value in privacy lies in the freedom and independence it provides for us, thus Hypponen's argument seems to reflect DeCew's approach. Regan (1995) points out the social value of privacy and this approach seems to be closer to what Hypponen is arguing. Interests in this sense benefit the social good afforded by privacy generally overriding concerns about individual privacy. Tavani then goes on to suggest that since privacy can be of value for greater social goods such as democracy, then it is worth preserving.

Tavani then begins his discussion of privacy with regard to 3 different kinds of practices in cybertechnology

- Data gathering
- Data exchange
- Data mining

Data Gathering (this includes monitoring, recording and tracking – surveillance in other words)

Some is controversial – like when we find out about the Government collecting all sorts of data related to our use of mobile phones, email, social media sites etc – and some is not – census data collection for example.

The use of cybertechnology makes it possible to collect and store personal information as well as monitor and track the activities and locations of people.

Many people are concerned about the threats to our privacy with regard to the capacity organisations and governments have to perform surveillance and monitor our activities – others less so. Roger Clarke coined the term *Dataveillance* to capture the activities of surveillance and data monitoring and collection.

The controversies associated with surveillance are not entirely unique to cybertechnology individuals (consider private investigators and stalkers), organisations and govt agencies have been monitoring us for a long time.

However cybertechnology greatly expands the scope and the level of automation association with such data collection. Organisations for example can automatically monitor employees online activity – how many hours are day do you spend on Facebook or Twitter? Users are often not aware that they are under surveillance.

Cookies

Files that website owners send and retrieve from computers browsers. Of course cookies may perform different levels of monitioring/storing of information – they may just include your preferences so when you return to the website you get the config you prefer – or they maybe used for more sinister purposes.

What is the problem with cookies? Some might argue that any kind of monitoring and recording of an individuals activity while visiting a website, including the downloading of information onto a users machine without the individuals consent constitutes an invasion of privacy. Additionally just what website owners that use cookie technology might do with your information constitutes a largely unanswered question – are they entitled to sell that information to third parties?

Of course most browsers have the ability to disable cookies. On the other side of this coin however is the limited functionality (or websites simply not granting access) of some websites when cookies are disabled.

RFID

Some interesting ethical issues here – Tavani cites a situation where RFID tags placed in articles of clothing or other items could be used to track purchasers – critics of the technology argue that they pose a significant threat to privacy as the owners of the RFID tags and technology could potentially gather data long after the original use for the tag had passed.

Government Surveillance

Of course this is one of the most significant concerns and has received considerable media attention. We have mostly discussed private firms and commercial potential to track and gather data and the affect that has on our personal privacy however perhaps a more sinister “big brother” mode of surveillance is that imposed on us by Governments and government agencies – sometimes acting in

a non-transparent way and gathering data and monitoring civilians – sometimes called domestic spying. In NZ and I am sure similar concerns will be raised in Australia that government has actually been accused of illegally gathering data on civilian activities – and this has become increasingly pervasive, sophisticated and intrusive.

Tavani mentions the development of the massive Utah based NSA data centre that Hypponen discusses in his TED talk.

Data Exchange – merging and matching personal data

The next practice identified by Tavani is the way in which personal data can be cross-matched across difference agencies/govt departments etc. So, while the mere collection of data raises privacy concerns if that data is collected for the purpose of on selling, exchanging or matching across and between different databases this may exacerbate the problem.

While we all agree that it is not unreasonable for some organisations to keep certain information about us the critical question is

- What kind of control can we expect over our personal information that we have given to any particular organisation?

Do we have a right to expect that our information will only be used for a legitimate use within a specific context and remain within the organisation? Or is it ok for it to be used or exchanged with other organisations who might merge or combine it with other existing information?

Tavani goes through some detailed examples in the text worth reading.

Computer matching is a variation on the technology we are currently discussing that involves cross checking information across two or more unrelated databases. Governments are increasingly using this technology so for example – years ago if you had an outstanding fine or a warrant for your arrest it may have been unlikely that the Customs database used at airports would have picked you up as you tried to flee the country for a life in sunny south America (Ronnie Biggs style). These days however your chances are pretty limited.

I can give you an even more detailed example – a friend of mine, after a recent acrimonious split from his Scandanavian wife was extremely concerned that his wife would abscond with the children back to Scandanavia. After discussions with appropriate authorities and lawyers records were kept in several database meaning that any attempted departure would be blocked at the border – he was also subject to this order – recently trying to take his children for a holiday in Australia he was stopped at the border until all the appropriate paper work was in order.

There is an increasing trend across government departments to share information – so justice departments, welfare, internal revenue agencies, customs/border controls all share information. Civil liberty groups are often up in arms regarding the privacy issues related to this information matching. What do you think? Of course we think of all this surveillance is ok to some extent to catch the bad guys, the welfare cheaters and people trying to game the system. Tavani asks us to consider 24/7 video surveillance across an organisation and daily drug testing to catch the deadbeats – would you be ok with this in your work place?

Data Mining

The final category of concern regarding privacy issues according to Tavani is data mining.

Data mining is the process that works on very large database environments and identifies patterns or nuggets of interesting information against a background of indecipherable noise – patterns that would be impossible to discover manually. So the NSA for example use sophisticated data mining algorithms in an attempt to detect security/"terrorism" concerns in the millions of gigabytes of collected phone records.

While there may be laws that protect our personal data where that data is

- explicit in databases – that is typical electronic records about ourselves
- confidential in nature – ie, medical, employment records, financial data etc.
- and exchanged between systems

The laws are less defined where the personal information is

- Implicit in the data – that is information patterns perhaps inferred from vast pools of data across periods of time
- Nonconfidential in nature – social media data and the like
- No exchanged between databases

Tavani introduces a few case studies – worth checking out.

Customer profiling

Organisations develop their own normative processes in order to categorise customers based on credit ratings and the like – Tavani discusses some examples where customers credit rating has been affected after organisations having performed data mining activities determined a particular customer might be a risk based on where they shopped and their shopping habits and where they held a mortgage.

I have personally had the experience of a bank calling me on my cell phone to enquire if I was the person using my credit card at the time – I was having a holiday in Christchurch a few years ago and went on a spending spree – spend over $1000 in the space of a few hours – I live in wellington and normally don't go mental with my credit card – the banks data mining algorithms picked this up and obviously an alert of potential CC fraud was raised.

What kinds of privacy concerns do you think this raises – if any?

Boston Police use facial recognition technology to watch thousands of music festival attendees.

http://noisey.vice.com/blog/beantowns-big-brother

There are a few of other topics in this chapter which I'll leave you to study in your own time.

- Privacy in public spaces
- Search engines and disclosure of personal information
- Online public records
- Privacy enhancing software
- Legislation and regulation