1 Intro

Perhaps the problems raised for ownership of data so far can be easily sidestepped. Suppose you are a gardener. Your chainsaw breaks right when you start cleaning up a fallen tree for one of your customers. I lend you mine while yours is in the shop. You make money from using my chainsaw and return it to me without a share of the profits, but with a gift of beer out of gratitude. I let you use my property so you could make money. The fact that it is my chainsaw gives me no right to your revenues. (Obviously, that could've been part of the lending agreement, but it wasn't). So, perhaps the problems we've seen with data ownership can be avoided by referring to the fact that customers agree to allow companies to use their data.

2 Notice and Consent

The standard model of consent embodied in privacy policies, terms of service, user

agreements, et cetera often gets called 'Notice and consent'. This just does what it says on the label: The company notifies you about what data they are going to collect and what they are going to do with it. You agree (or don't use the service).

More broadly, the notice and consent model can be seen as extending standard ideas from contract law to these sorts of agreements. Generally speaking, as long as someone knows what they are agreeing to when they sign a contract, it will be enforceable. More importantly, courts will generally presuppose that you know what you agreed to when you signed the contract.

2.1 Consent intro

Let's get started by talking about consent in general. Once we've got a grip on that, we can turn to our particular topic.

2.1.1 Political obligation and consent

To get the hang of consent in this context, let's start with something completely different —the question of when people have political obligations. That is, when can a state (morally) demand that someone pay taxes, serve in the military, or otherwise do stuff.

2.1.1.1 Early days

As western Europe moved from feudalism to something more like democracy, the question of how we can justify citizens' obligations to their rulers took on a new significance. Where in the past , this could be answered via the alleged relationship between gods, kings, and nobles —god says the king gets to demand anything he wants from anyone in his lands, the king says I get to demand whatever I want from you, peasant, so give me your crops. Oh. And I'm gonna need you to fight in my armies.

Or, probably more commonly, just a naked exercise of the force and violence feudal rule was based on: I want your crops and military service. Why? Because I have swords and loyal retainers to use them on you. Questions?

But as the idea that political legitimacy and authority came up from the governed (I.e., land-owning white guys) rather than down from the heavens or just at the point of a sword, philosophers like Locke tried to explain how it is that the governed have moral obligations to their governments.

2.1.1.2 Explicit consent

The easiest way to get political obligations is to have explicit consent. Thus the easy case is something like naturalized citizenship. You hold your hand up or put it on a book or over your heart or whatever and say that you agree to be bound by the laws and obligations of the land. But that's not most people. Most citizens never agreed to be, well, citizens. Nor does it make sense of the political obligations non-citizens may have to the state in which they reside.

2.1.1.3 Tacit consent

For Locke, citizens and residents did in fact consent. Sort of. They didn't say they did, but they acted like it. This is the idea of tacit consent. It has a bunch of different versions. But, basically, if you accepted the benefits of living under a government — drive on the roads, get educated, survive because no steppe nomads sweep in and kill everyone in your town— then you have tacitly consented to be obligated.

Very few writers these days believe this form of tacit consent genuinely creates obligations. Folks like Nozick and Simmons have pretty well ways of spelling out how tacit consent would work like the so-called principle of fair play (if you benefit from the cooperative activities of others, you have an obligation to contribute).

For our purposes, that's fine. We just needed the idea of tacit consent to in order to start making sense of how users might be consenting to data use. Let's turn back to the topic at hand.

2.1.1.4 Wild west internet

Collection of data on the early internet may have relied on something like the idea of tacit consent.

There weren't a lot of rules and disclosures. The attitude was basically: You come to our website. Our website is ours. We get to keep any data you produce while using it. If you don't want that, then go away. No carefully crafted terms and conditions. No privacy policies. Just: if you use our stuff, you agree. Even if you weren't exactly clear on that.

But then money started being made. Websites were being put up by proper companies; you know, with corporate structures and everything. Once that happened, the legal department got involved. All fun stopped. As with other businesses, the web needed to

be well-defined agreements between the company and its clients.

In particular, customers needed to be actually consenting to the use of their data. To understand that, we need a more robust form of consent.

2.1.2 Informed consent

What we probably want is something more like the notion of informed consent that we use in fields like medical ethics.

As we'll talk about more below, fields such as medical ethics have been hammering out what informed consent looks like in practice for a few decades now. For now, let's just say that for there to be genuine consent to anything, the person needs to be at the least: informed, able to make decisions, and the choice must be voluntary.

2.1.2.1 Informed

Informed consent requires information. It's right there in the name. More specifically, it requires accurate and understandable information. Again, both parameters vary.

2.1.2.1.1 Accuracy

Obviously, the information must be true. But our understanding of accuracy here needs to go a bit beyond all the sentences being true.

For one, when the goal is allowing people to genuinely agree to something, in some cases, that may require telling them things which are strictly speaking false. Oftentimes the way people will understand specialized information is through analogies, metaphors, and the like. An immunology student will groan at all the disanalogies involved in the claim that 'White blood cells are like pac-men roaming your body eating germs, right now they are very weak and tired', but that may be accurate enough for the leukemia patient to use in reasoning about treatment options.

2.1.2.1.2 Understandable / level of detail

Similarly, the information must be understandable by the patient. This bar will be set in different places for different patients, depending in part on the background knowledge they bring to the exam room.

For example, through my research on pain I spend way more time around medical

journals than your average patient. I've had to explain to a surgeon that if he wanted me to sign the consent form, he would have to explain the procedure and risks as if he was talking to a colleague about my case. The point is not that I'm more comfortable with medical jargon than others. It's that I know enough about (some!) areas of medicine that I need a higher level of technicality for me to be able to make an informed choice.

2.1.2.2 Capable of deciding

Hopefully you still vaguely remember enough about autonomy and Holley's paper from before the first exam that you will not be surprised to hear that it's not enough to have the information in front of you, multiple options, and no gun to your head. If you are a very small child, your choice will not be genuine consent. You need to be capable of processing the information and understanding how the potential risks and benefits fit with your preferences and desires.

Thus whether you have the sufficient capacity for consent will depend to some degree on the nature of the choice. If the stakes are low, the required capacities will often be less. Children can consent to agreements around cookies and chores. When they are high, a higher degree of psychological stability, reasoning skills, background knowledge, and self-reflection will be needed.

2.1.2.3 Voluntary

As we've discussed throughout the semester, autonomous choice requires liberty —the ability to wiggle or refrain from wiggling as one chooses.

With Holley, we saw this built into his conception of a voluntary exchange with the non-compulsion condition. One must have more than one option for the choice to be legitimate.

2.2 What must be disclosed

Turning (finally!) to the topic at hand, what information will a user need to know to make intelligent choices about whether to agree to a company's privacy policy?

Very broadly, you need to know anything which is materially relevant to the decision about whether the benefits of the service you'll receive outweigh the costs (including risks) associated with the information you are giving up.

In a sense, what you need to know is anything which bears on the question 'How much

might surrendering control over this data hurt me?' Of course, this is unanswerable. Once your information is out there, it's not coming back. Who knows how clever smear artists might twist your college grocery store purchase history during your run for president.

Fortunately, the question isn't just what the consumer would need to know. It's what the company seeking her business must disclose to her. Presumably the grocery store has no more understanding of future political character assassination risks than you do. (Or do they….)

So we can at least limit the scope of our question to information which bears on risks which the company is or could be aware of. Barocas and Nissenbaum give a partial list for what the user of a newspaper publisher's website would need to know :

> (1) Which actors have access…; (2) What information they have access to…; (3) What they do or may do with this information; (4) Whether the information remains with the publisher or is directly or indirectly conveyed to third parties; and (5) What privacy policies apply to the publisher as compared to all the third parties, assuming these are even known to the users. These still constitute…only a subset of what a user might need to know in order to be meaningfully informed {Barocas:2009ws}

Notice that this list may not translate smoothly to other industries and uses of personal data. The use of your purchasing history by a grocery store loyalty program may require more or less information along different axes.

2.3 Strengths of notice and consent model

The notice and consent model is appealing for several reasons.

2.3.1 Spells out all details

The notice and consent model makes everything completely clear by spelling out all the details of the agreement.

Okay, so 'makes things clear' is not actually right. A lot of times, the reason why the 'leagalese' of contracts and legal documents is so confusing and difficult to understand is actually due to the company's lawyers making things as clear as they possibly can. That's what lawyers drawing up contracts and agreements are doing: They are trying to think of every possibility, state precisely what it is, and state precisely who owes what.

We'll come back to this later.

This benefits the service provider by shielding them from various forms of liability that come from incomplete disclosures and by shifting risk onto the user.

It benefits the user by allowing them to pick and choose which companies they deal with on the basis of their preferences with respect to personal data privacy.

2.3.2 Gives consumer basis for trust

The notice and consent approach benefits the consumer by providing some legal basis for consumer protection and trust. With any rule-bound bureaucracy and especially the law, if it says in clear language in black and white on a piece of paper that the company will not do x, you can have decent confidence that they will not do x. Obviously, there are exceptions. It assumes people in the company know their own policies or that they are confident enough that their lawyers can keep the costs of paying lawsuits over their doing x low. But, on balance, we shouldn't ignore the consumer benefit of having everything spelled out in excruciating detail.

2.3.3 Opportunity for market differentiation

Leaving the management of personal data to be determined by be what companies and their users agree makes it possible for different companies in the same space to differentiate themselves through their privacy policies. For example, Apple seems to be putting a lot of effort —both marketing and engineering— to protecting privacy in their mobile devices.

Of course, consumer privacy advocates have long known that as a general matter this is not on its own sufficient. Consumers both chastise companies for misusing their personal data and are uninterested in paying directly for the services being funded by this alleged 'misuse'.

2.3.4 Other strengths

[ToDo]

Other strengths of the notice and consent model include

Individual

- Control of information: Allows individuals to evaluate options deliberately and

decide whether to give or withhold consent
- Respects individual choice

Company
- Allows for more collection of data and thus better trained models / better services

Economy level
- Efficient market: Allows market to function efficiently whereby individuals can decide when the price is right
- Efficient allocation of services

2.4 Problems with notice and consent

To explore the problems facing the notice and consent model, it will help to do a bit of rough taxonomy to keep the issues straight. Let's distinguish between problems with the notice part and problems with the consent part.

Obviously, this division is highly artificial. Since genuine consent requires being informed, many of the problems with the notice part undermine the consent part. I'm cutting it up this way just to help organize, so don't worry too much about the taxonomy, at least not until we're done worrying about the cases.

2.4.1 Consent part

Let's start with problems affecting the consent portion of 'notice and consent'.

2.4.1.1 Inescapable / no real choice

Anytime we're talking about people having adequate options / choices, we quickly run into difficulties judging whether a person really has alternatives. Take for example social media companies such as Instagram. Do you have a choice other than accepting their policies?

On the one hand, it's tempting to say that people don't need social media, thus they always have the option of not using the sites. Obviously, if we're taking 'need' here in the sense of immediate survival —I need water— then we don't need social media. Indeed, humanity was doing okay for the millennia up to the demise of Friendster and MySpace (no one needed those early social media platforms).

But on the other hand, we are social animals. If all your friends are using Snaptagram, using Snaptagram may be the only way of interacting with them. Loss of social integration can be a terrible loss. You can survive without food for a few months. Going without friends for that long may not kill you, but it can still be a signifiant hit to your well-being.

Indeed, one of the value propositions behind social media companies is network effects: Once your site's user base is large enough, it sucks in everyone who wants to interact with them. In other words, once such companies exist at scale, people need to be able to use them.

2.4.1.2 Hard to judge risks / consequences of agreeing

It is very very very hard to understand the risks different uses of your personal information may pose. This is in part because there are tons of uses of personal data which exist right now. But the uses which exist now are just the beginning. Once data escapes into the wild, it does not return. Every person will have to anticipate what kinds of problematic uses may get dreamt up in the future. That's incredibly hard.

But the task is actually much harder. There will not be just one list of concerns which we could all look at and make individual choices about where we draw the line. It also matters who you are. As is unfortunately too common with society's laws, being older, whiter, and male-r tends to insulate people from ill effects. The middle aged white guy gets a warning; the young black woman gets a speeding ticket. There is no reason to think that these patterns will not translate to the ill effects of various uses of personal data.

For example, there are companies which purport to use machine learning on job applicants social media presence to determine whether they are likely to be good employees. Guess whether these companies target low wage jobs or Fortune 500 companies for C-suite positions. Thus there is no one set of risks from the use of personal data.

In addition to there being tons of uses, it is difficult to know how to weight the risks. As we talked about at the beginning of the semester, it isn't enough to know how bad something might be. You also need to know how likely it is and weight accordingly. A lot of the relevant data you would need to assess risks of different uses by currently existing companies is proprietary or not well documented.

And just to emphasize this again, data outlasts the use. Maybe things folks are doing now are fine. But maybe down the road, data collected today will have completely unforeseen uses. I'm sure that companies five years from now will be substantially more enlightened, ethical, and scrupulous about their customers' privacy. Ok. That's a lie.

2.4.1.3 Difficulty of knowing competence of person agreeing

So far, I've mostly talked about the problems of the notice and consent model from the consumer side. But there are concerns from the company side too. Suppose you run a well-intentioned company and want to make sure your privacy policies are clear and that your users really will understand the trade-offs you are presenting to them. How do you know whether your users are actually competent to agree to use your service? You can't give a test. You have to aim for your average consumer. You might be able to estimate the level of education needed for the language. But you would also need to ensure that the users are properly weighing the risks. It's hard enough to know when, as individuals, we ourselves are taking risks seriously but not overblowing them. Imagine trying to ensure this for millions of users from myriad walks of life from around the globe.

2.4.2 Notice part

Let's turn to problems with the notice part of the notice and consent model.

2.4.2.1 TL;DR

Probably the biggest problem is that people do not and cannot be expected to read policies. They are long, legalistic, and difficult for the average user to understand. Indeed, even specialists have trouble deciphering the implications of some policies [ToDo: add ref]. We might call this the TL;DR problem, if we were stuck using internet slang from 10 years ago.

Now, it may be tempting to dismiss these concerns as the customer just being lazy or dumb. But even if they were written in the clearest, most accessible language, the length alone is serious burden and barrier.

To illustrate this, let's do some rough math. A meta-analysis of studies estimating

reading speeds in English comes up with approximately 238 words per minute for non-fiction.[1]

I downloaded and very roughly estimated the word count of Ralphs supermarkets privacy policy on 31 October 2019. It was approximately 2204 words. At the 238 wpm, it would take 9.26 minutes. Doing the same with Google's privacy policy (not the terms of service) yielded about 7311 words. That's 30.72 minutes of reading. The LA Times privacy policy came in at 4343 words. That's 18.25 minutes of reading.

Thus with just three websites, and only considering their privacy policies, we're now up to about an hour out of your life. Hopefully it's becoming clear how big a task this is. Multiply the average word count in privacy policies with the number of companies that the average consumer will need to interact with; I can't imagine that the result would be anything like a manageable amount of time which each consumer would need to commit to reading privacy policies.

2.4.2.2 Policy revisions

Even once you've read the policy and agreed to it, you'r e not done. Companies may change their terms at will. Sure, they will usually notify you and summarize the changes. That lowers the burden of reassessing whether you still want to agree. But its nonetheless a burden. Multiply those changes across the number of user agreements we are bound by and we're talking about a not insignificant amount of time.

2.4.2.2.1 Lock-in

Indeed, as Hoofnagle points out, other costs of the reassessment may rise. Suppose you've spent several years using a company whose privacy policies are satisfactory to you, there may be a significant cost to switching to a new company when the company's policy changes. As Nissenbaum summarizes the concern:

> In July 2007, Susan Wojcicki, Google vice president of product management for advertising, suggested that OBA [Online Behavioral Advertising] was "not something that we have participated in, for a variety of reasons," and that Google wanted to "be very careful about what information would or would not be used" for the purposes of advertising And yet, as we know, Google is now potentially the most dominant player in the OBA field. This about-face should give us pause…[because] users who relied on Google's aversion to behavioral targeting from 2000-2006 may "have already used Google for years and may have some

1. https://psyarxiv.com/xynwg/

> lock in from adopting the company's many services" [On notice]

2.4.2.3 3rd party use

Perhaps the biggest concern —this will be a big driver of the Transparency Paradox below— arises from companies sharing and selling data to other companies.

Sure, you might decide that you can trust the company you're giving consent to. But what about the company who buys your data from the company who bought your data from the company you agreed to allow to harvest your data? Who's keeping an eye on them?

Once there is a market for personal data, businesses in possession of your data may change their partnerships at will. Customers can't really assess constantly changing web of business partners. Even identifying which companies these are will be prohibitively difficult. Assessing all of their privacy policies just multiplies all the problems we've already seen.

The online advertising space pours rocket fuel on the pace of such changing relationships. As Barocas and Nissenbaum note, brokers such as ad exchanges, who provide a marketplace for algorithmic auctions of ad impressions, muddy the waters with respect to the privacy policies actually governing your data.

> Ad exchanges replace semi- stable contractual relationships concerning the sale of impressions or transmission of user data with fleeting relationships based on real-time auctions that may nonetheless result in the equally permanent transmissions of user data. {Barocas:2009ws}

2.4.2.4 Legalese

Few of us can understand the policies. Let's talk a bit about why that is.

Obviously, these are legal documents, written by lawyers. That poses challenges to the consumer actually being 'notified'. Notice that in most areas of law this doesn't matter. The US legal system, excluding criminal law (sort of), presumes that if you have a legal dispute which you care enough about not losing, you will hire a lawyer.

But these aren't legal disputes. These are agreements between a consumer and a company. It is fairly unlikely that even rich customers run user agreements for social media companies past their lawyers. And they have lawyers.

2.4.2.4.1 Interpretation against body of case law

Why would you need a lawyer? Couldn't any of us pick up a contract and read carefully? Well, yes and no. On the one hand, a lot of dense legalese is actually just enumerating all sorts of scenarios and explaining what will happen in them. But on the other, any contract will be interpreted against the laws and (often more importantly) the case law of its jurisdiction. This is why people go to law school. Every profession has certain shared understandings, short hands, and fixed reference points.

If you're not convinced, here's an example from medicine. If you've ever seen a paper prescription[2] you might have puzzled over where the dr is saying how often or even how you should take it. For example, 'BID' means twice a day. If you are an amateur and relying on hasty google searches, you may confuse *p.r.n.* (as needed) with *p.r.* (stick it up your butt —per the rectum)[3] . (I confess I have waited years to find an opportunity to make this joke)

2.4.3 Other problems

While we are jumping up and down on the notice and consent model, let's get on the table some non-notice and non-consent problems it faces.

2.4.3.1 Economic externalities

Pressure toward either monopolies or data market saturation.

[ToDo: Figure out what this was supposed to be. This is from student suggestions during a previous class; it must have made sense then….]

2.4.3.2 Affects the value we put on privacy

Some writers worry that if people get too used to giving up their privacy, they won't value it as much. That in turn makes it easier for companies and other entities to chip away at our privacy, which makes people value it even less. Rinse and repeat.

That said, it's likely true that there is a lower limit on how much privacy we'll be willing to give up. The early utilitarian reformer Bentham thought that prisoners would benefit from being watched 24/7.[4] That would help them build good character since

---

2. And, seriously, you really shouldn't. Paper prescriptions are a huge source of medical error since the pharmacist has to interpret your doctor's handwriting.
3. https://www.drugs.com/article/prescription-abbreviations.html

they'd learn to act like they are always in public. Unfortunately, these ideas did get adopted by prison architects who built prisons so that the prisoners never could tell if they weren't being watched. I say 'unfortunately' because Bentham was very very wrong about what happens to people when they think they are being watched all the time. It is not good for their character; it is probably not good for their sanity.

2.4.3.3 Spider lawyers

A team of highly skilled lawyers churning out carefully vetted agreements is as close to a Star Trek deflector shield as we are likely to find in nature. If the starship Enterprise was a company, Captain Piccard commanding 'shields up' would be a call down to legal.

However, whenever you're developing a policy, you are always navigating between the need to keep it flexible enough to handle the random problem cases that you will never dream up while precise enough so that everyone can understand what it means. If a company's policies are complex and detailed, the chance that something unenforceable or, worse, illegal in a particular jurisdiction will sneak in (or fail to be removed when laws change) grows.

There are [ref] groups who use web-spidering techniques (spiders because they 'crawl' the web —don't look at me, I didn't make this one up) to digest user agreements by the thousands. If they find something actionable, they sign up as a user, light an expensive cigar and then file a lawsuit. Done correctly, the lawsuit will cost just enough that the company would lose money having it thrown out in court. So, detailed user agreements can pose some litigation risk for the company.

At the broader economic level, if there's enough of this sort of litigation, it can create economic inefficiency. That's not to say that economic inefficiency is always a bad thing. But it is something which we want to be attentive to when we are thinking about how to approach these problems at a national level.

2.5 Attempts to fix notice and consent

It does seem that policymakers, some sectors of the public, and some data-industry

---

4. https://en.wikipedia.org/wiki/Panopticon

actors are aware of the problems with the notice and consent model and interested in repairing it.

How exactly the repairs might work depend on what we think the problems are.

2.5.1 Standardizing and simplifying policies

If you think the problems arise from the policies being too confusing for the consumer to understand, the fix might be to find ways to make the policies more standardized and simpler. Indeed, finding more intuitive and clear ways of conveying the information might also help; this will probably require help from experts in visual communication and other aspects of consumer psychology.

The model here might be nutrition labels. Nutrition labels on food are imperfect. But they do a far better job conveying important information to the average consumer than a biochemist's report.

Similarly, in the wake of the Great Recession, legislation [ToDo: NAME? Was this in Dodd-Frank?] standardized a number of consumer financial documents. All credit card terms and conditions need to be formatted the same, use the same time-frames for interest rates, et cetera. Again, this is in the service of helping consumers understand what they are signing up for by standardizing and simplifying a complex financial arrangement.

2.5.2 Stavra example

Don't believe me that this is an approach folks like? Here's an email I received from the cycling app Stavra on 11/13/2019, note the first item:

> Hi adam,
>
> Privacy. It's something we all care about, but making the time to read the fine print can be tough. So as part of this Privacy Policy update, we've created a way to understand the most important details at a glance.
>
> **Meet our new Privacy Label.** Like the nutrition label you've come to trust, we've created a no-nonsense list of need-to-know privacy facts. Take a look.
>
> **We didn't sell your personal information before, and we don't sell it now.** We're excited to give athletes even more clarity about how information is shared and how you can control your privacy settings. Read about this and other updates in our latest Privacy Policy, effective December 11, 2019. By continuing

to use Strava after this date, you agree to our updated Privacy Policy.
The details you need, all in one place. Our Privacy Center has what you need to make informed choices about your data.
A new privacy law from California. We're giving all Strava athletes, regardless of your location, the same tools and controls as Californians under the California Consumer Privacy Act. And for athletes living in the European Economic Area, while nothing's changed about your rights these disclosures are always helpful to review.
We take your privacy seriously and are committed to making sure you can hit record, upload to Strava, give kudos and cheer on your friends with confidence that your personal information is safe and sound.
Cheers,
The Strava Team

2.5.3 Opt out vs opt in

Alternatively, if you focus on the 'take it or leave it' nature of the user agreements, you might try to find ways to allow users to 'opt out' of data collection without losing all access to the service.

This is attractive because it recognizes the reality of consumer decision making. The economist's idealized (and presumably ideally wealthy) consumer makes carefully considered purchasing decisions in the ideal competitive marketplace and thus opts out of any agreement that is not in her interest. None of us are the idealized consumer; at least not all the time.

2.6 Transparency paradox

Let's summarize the task that lies before anyone hoping to fix the notice and consent model.

For someone to evaluate the risks and benefits of sharing their data with a company, they will need to know at least:

1) What information will be collected
2) How long the information will be retained
3) How the information will be anonymized, if at all
4) How information will be processed and used (group level statistics; individual targeting; etc)
5) Which 3rd parties the data will be shared with, and what information will be

shared

Each of these will likely be complex and require detailed disclosures. Obviously, the level of detail and precise information involved will vary depending on the nature of the service and the nature of the data collected. So the task may be more difficult in some areas than in others.

Still, even the easy cases will be a significant challenge since it's not enough to simply disclose the information. The information must be conveyed to the consumer in ways that are relevant and meaningful, while still being digestible in a short period of time.

Nissenbaum thinks that this will basically be impossible. She argues that the notice and consent model is fundamentally misguided. The project of attempting to simplify, standardize, or otherwise fix up the way information about personal data is disclosed is doomed. This is due to what she calls the *transparency paradox*. The paradox is roughly the tension between two claims:

1) If a policy gives the consumer adequate information, they will not read or understand it.
2) If a policy gives the consumer understandable information, it will not adequately inform them.

2.6.1 Paradoxes

To keep the philosophy majors from going nuts, let's note that, strictly speaking, the transparency paradox doesn't involve a paradox in the standard philosophical sense.

When philosophers talk about paradoxes, we usually mean situations where (very roughly) we are forced to choose between two equally plausible but incompatible claims. The most famous and short paradox is the liar paradox. Consider the following sentence:

(LS) This sentence is false.

Is LS true? Well, if it is true it is false. So, it must be false. But, remember, false is equivalent to not true and vice-versa. (c.f., You: Are those tacos in the bag? Me: They are not not tacos). Therefore, if LS is false, it is true.

I'll wait while you pick up the pieces of your blown mind. Go[5] ahead. I'll be right here…

2.6.2 The transparency paradox

The transparency paradox comes about because, if the notice (privacy policy) details everything, the average consumer will not read or understand it. At the same time, if the notice is readable and understandable, it will omit crucial information.

However, we need to be careful about what's generating the problem. Otherwise, the transparency paradox might seem trivial.

After all, simplifying complex information virtually by definition leaves stuff out. That's obvious. Indeed, the fact that we leave stuff out when we summarize isn't usually a problem. Suppose your friend asks you what Game of Thrones is about and you answer "It's a fictional version of the English Wars of the Roses but with dragons and zombies." There are certainly better answers. But if your friend knows a bit of history or knows how to use Google, it's a reasonably informative answer. She could make a decision on whether to check it out.

But if the transparency paradox showed that all attempts at summary are doomed, you'd have to reply "It is impossible to tell you. Go buy the books, subscribe to HBO, and we'll talk in a couple of weeks." Alternatively, no introductory textbook would ever be usable.

Put another way, to understand the Transparency Paradox, we need to know why summarized privacy policies will never be good enough for consumers to make choices about using a service. This is because, Nissenbaum claims, attempts to simplify these policies will necessarily leave out essential information. The question is thus what

---

5. Mind not blown? Okay, how about the weaponized version, Godel incompleteness? Here's some videos
Computerphile: History of undecidability pts1 -3
https://www.youtube.com/watch?v=nsZsd5qtbo4
https://www.youtube.com/watch?v=lLWnd6-vSGo
https://www.youtube.com/watch?v=FK3kifY-geM
Another video from Numberphile:
https://www.youtube.com/watch?v=O4ndIDcDSGc
Obviously, while interesting and guaranteed to make you the life of any party, none of this is relevant to our class.

guarantees that this will happen when we are talking about privacy policies.[6]

2.6.3 What guarantees the paradox

Nissenbaum thinks that the nature of the data collected and the nature of the industries doing the collection will provide the guarantee that we run into the Transparency Paradox.[7]

Big data techniques which attempt to extract novel insights from data require huge datasets. (Hence the name, 'big data'). Generally speaking, the more data a company can snarfle up, the more useful it becomes. Thus, except for companies like google who keep all their data in-house and sell access to the products of it, in most cases you would need to know not just how the company you are immediately doing business with will use your data.

Indeed, you need to know several layers of business relationships down. These are complex webs of companies, which often change. Thus you would need to know how all of these companies are handling your data.

That's what drives the transparency paradox. The structure of the industry entails that you need to know the policies of multiple companies. That fact alone seems to doom the simplification project.

2.6.4 Objection: informed consent works in medicine

So far it looks like Nissenbaum has pointed to a genuine tension. All parties to this problem can agree that it is hard to resolve this tension. But she is claiming that it can't be fixed; that we should think that the notice and consent model is doomed. Let's think through how sure we are that the tension cannot be resolved.

When someone points out a problem and claims that it can't be fixed, it's usually a good

---

6. You might detect echos here of Holley's distinction between an ideal exchange and an acceptable exchange —in the former, the buyer knows everything about the product. But in the latter case, the buyer is informed enough (etc) to have a decent shot at there being a mutually beneficial exchange.

7. Discussed in Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus*, *140*(4), 32–48. http://doi.org/10.2307/23046912?refreqid=search-gateway:4971cc18293f6167ab2b2c12057373be

idea to look for analogous situations and consider whether we have solved the problem there. If we can find others where we have fixed the problem, that will cast doubt on her claim that the notice and consent model is doomed.

One place we might look is the use of informed consent in medicine. The relevant information for consenting to a medical procedure is often intensely complex and technical. It very often involves weighing probabilities and fitting those probabilities together with other decisions. Human beings are pretty bad at that. Thus it looks like the transparency paradox arises for informed consent in medicine too.

However, we know that informed consent in medicine generally works. It's not perfect. But in most cases, the patient probably is well-enough informed to decide to undertake a medical procedure. We have decent guidance for practitioners on how to inform patients; similarly, human subjects review boards are reasonably sophisticated.

So, if the transparency paradox can be overcome in medicine, it looks like we needn't be completely pessimistic about privacy.

2.6.4.1 Response: Nope not fixed in medicine

Nissenbaum's response to this objection is straightforward: No. We haven't solved the transparency paradox for informed consent in medicine. Instead, we have a system that relies on other factors to ensure patient protection. She writes

> "these protocols work not because they have found the right formulation of notice and consent but because they exist within a framework of supporting assurances....It is not the consent form itself that draws our signature and consigns us to the operating table, but rather our faith in the system. We trust the long years of study...that physicians undergo, the state and board certifications, peer oversight, professional codes, and above all, the system's interest (whatever the source) in our well-being" [36]

Medince didn't solve the transparency paradox. It evolved institutions which allow us to trust doctors.

2.6.4.2 Response: Unknowability

Indeed, Nissenbaum and Barocas offer what seems like an even stronger version of this claim, viz., that the things you would need to know are fundamentally unknowable:

> Complexity constitutes a challenge, generally, for achieving meaningful notice, but OBA is unlike surgery in two significant ways. First, given adequate time, training, and education, a person confronted with a medical decision could, in

> principle, fully understand what they were consenting to. In the case of OBA, however, there is a degree to which the tracking, analysis, and use (current and future) of data is not only difficult to grasp, but unknowable. As we noted above in our description of the capture and processing of information, there is potentially an unending chain of actors who receive and may make use of behavioral and other data. New companies bloom, novel analytical tools emerge, business relationships begin and end. In the currently preferred model, when people consent to OBA—or fail to opt out—they literally cannot know what they are consenting to. {Barocas:2009ws}

2.6.5 Alternative approaches to saving notice and consent

Suppose Nissenbaum is right that the institutions and norms around medicine are what create the ability for patients to make informed choices, not just the way the info is presented. Perhaps there are other ways to try to fix the model which follow in medicine's footsteps.

2.6.5.1 Privacy consultants

One suggestion, raised independently by several brilliant business ethics students, is to try to fix notice and consent by importing something like the trusted intermediary which did the work in medicine.

For example, maybe we just bite the bullet on the transparency paradox —we let the legal department keep writing the notice forms— and create an industry of privacy consultants who have the expertise to interpret them and provide a trustworthy opinion to consumers based on the consumers privacy preferences.

If you could trust that your consultant is evaluating privacy policies on your behalf based on your preferences, we would work around the paradox. As with medicine, professional standards of practice, social expectations, and other reenforcing norms would be crucial to making this work.

2.6.5.1.1 Concerns about privacy consultants

Of course, even if this strategy would in fact preserve the notice and consent model, we would then have to take up whether it is desirable.

Certainly, there will be economic concerns. It adds another layer of professionals

required for ordinary people to conduct their lives imposes costs.

There will be social concerns. If all consumers remain subject to such personal data policies but only some can afford a privacy consultant, the harms of personal data use may fall disproportionately on some groups in society.

There will also be political concerns. As is perfectly normal, a group of professionals will form an interest group. Presumably, such professionals will advocate for consumer interests. But that advocacy will be inevitably filtered through their professional interests. The union covering CSU professors is a strong advocate for CSU students in state politics. Of course, we believe that the best way to help students is to empower (and pay well!) full-time professors.

2.6.5.2 Ratings organizations

Alternatively, public interest groups could take up the work of parsing privacy policies and making recommendations to consumers. A quick Google search revealed one such organization called Terms of Service; Didn't Read: https://tosdr.org/

3 Nissenbaum's approach

If notice and consent is beyond saving for personal data, what should we do instead? How should we make policies that protect people's data online?

Instead of trying to extend ordinary contractual practices to online privacy, Nissenbaum wants us to stop treating issues of online privacy (and presumably privacy in other data-snarfling environments) as something special which requires a new approach. Instead, she wants us to recognize what tools we already possess and work from what we already know. We are to start by recognizing that

> "Online activity is *deeply integrated* into social life in general and is *radically heterogeneous* in ways that reflect the heterogeneity of offline experience." [37]

The online realm isn't separate from regular life. The issues it poses aren't generally distinct from what we already deal with. Instead of looking for new tools and new theoretical justifications, we should use what we already have.

3.1 Contexts

Let's start with what counts as a context. As sociologists and theorists have long recognized, in daily life we pass through many different socially defined contexts. Think of the differences in how you act / how you are expected to act within your roles

as a student, a roommate, an employee, a child in a family, a parent in a family, a patient in the doctor's office, a teammate, a friend, a lover. Each of those contexts has it's own rules. It may be appropriate to pat your lover or teammate on the butt in congratulations. Your doctor will react poorly to this.

3.2 Contextual integrity

Just like rules about what forms of intimate personal contact are appropriate, contexts have rules about information flows. Indeed, she claims that every social context, has certain norms and assumptions about data sharing and use.

The basic idea on Nissenbaum's view is that when we move to the online realm, we should preserve the norms which already govern information in similar contexts. The main task of informational privacy from her perspective is to try to determine how we can extend our norms, policies, and laws which govern information in non-online contexts, to newer arenas. She writes:

> A central tenet of contextual integrity is that there are no arenas of life not governed by norms of information flow, no information or spheres of life for which "anything goes." Almost everything—things that we do, events that occur, transactions that take place—happens in a context not only of place but of politics, convention, and cultural expectation. These contexts can be as sweepingly defined as, say, spheres of life such as education, politics, and the marketplace or as finely drawn as the conventional routines of visiting the dentist, attending a family wedding, or interviewing for a job. For some purposes, broad sweeps are sufficient. As mentioned before, public and private define a dichotomy of spheres that have proven useful in legal and political inquiry. Robust intuitions about privacy norms, however, seem to be rooted in the details of rather more limited contexts, spheres, or stereotypic situations. {Nissenbaum:2004uu} p.119

These contexts follow the information. Even when it leaks into another context.

> One point of contrast with other theoretical accounts of privacy rights is that personal information revealed in a particular context is always tagged with that context and never "up for grabs" as other accounts would have us believe of public information or information gathered in public places. A second point of contrast is that the scope of informational norms is always internal to a given context, and, in this sense, these norms are relative, or non-universal. [125]

3.3 Informational norms

Nissenbaum believes that

> technologies, systems, and practices that disturb our sense of privacy are those that have resulted in inappropriate flows of personal information. Inappropriate information flows are those that violate context specific informational norms (from hereon, ''informational norms''), a subclass of general norms governing respective social contexts. {Nissenbaum:2015ki} p.839

She argues that there are 2 broad types of informational norms at stake: Norms concerning appropriateness and norms concerning distribution. As she writes:

> I posit two types of informational norms: norms of appropriateness, and norms of flow or distribution. Contextual integrity is maintained when both types of norms are upheld, and it is violated when either of the norms is violated. The… benchmark of privacy is contextual integrity; that in any given situation, a complaint that privacy has been violated is sound in the event that one or the other types of the informational norms has been transgressed {Nissenbaum: 2004uu} p.120

3.3.1 Norms of appropriateness

Concerning norms of appropriateness she writes that

> norms of appropriateness dictate what information about persons is appropriate, or fitting, to reveal in a particular context. Generally, these norms circumscribe the type or nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed. In medical contexts, it is appropriate to share details of our physical condition or, more specifically, the patient shares information about his or her physical condition with the physician but not vice versa; among friends we may pour over romantic entanglements (our own and those of others); to the bank or our creditors, we reveal financial information; {Nissenbaum:2004uu} p.120

And

> As important is what is not appropriate: we are not (at least in the United States) expected to share our religious affiliation with employers, financial standing with friends and acquaintances, performance at work with physicians, etc. As with other defining aspects of contexts and spheres, there can be great variability from one context to the next in terms of how restrictive, explicit, and complete the norms of appropriateness are. In the context of friendship, for example, norms are quite open-ended, less so in the context of, say, a classroom, and even less so in a courtroom, where norms of appropriateness regulate almost every piece of information presented to it. The point to note is that there is no place not governed by at least some informational norms. The notion that when individuals venture out in public—a street, a square, a park, a market, a football

> game—no norms are in operation, that "anything goes," is pure fiction. For example, even in the most public of places, it is not out of order for people to respond in word or thought, "none of your business," to a stranger asking their names {Nissenbaum:2004uu} p.121

She quotes the philosopher Ferdinand Schoeman to illustrate one way a person can violate norms of appropriateness by moving information between contexts

> "[p]eople have, and it is important that they maintain, different relationships with different people." [71-notes]

and

> [a] person can be active in the gay pride movement in San Francisco, but be private about her sexual preferences vis-à-vis her family and coworkers in Sacramento. A professor may be highly visible to other gays at the gay bar but discreet about sexual orientation at the university. Surely the streets and newspapers of San Francisco are public places as are the gay bars in the quiet university town. Does appearing in some public settings as a gay activist mean that the person concerned has waived her rights to civil inattention, to feeling violated if confronted in another setting?[72 —notes]

3.3.2 Norms of flow / distribution

Concerning norms of distribution she writes that her perspective is compatible with Michael Walzer's picture of different spheres of justice.

> According to Walzer, complex equality, the mark of justice, is achieved when social goods are distributed according to different standards of distribution in different spheres and the spheres are relatively autonomous. Thus, in Walzer's just society, we would see "different outcomes for different people in different spheres." Complex equality adds the idea of distributive principles or distributive criteria to the notion of contextual integrity. What matters is not only whether information is appropriate or inappropriate for a given context, but whether its distribution, or flow, respects contextual norms of information flow. [123]

And also that

> Free choice, discretion, and confidentiality, prominent among norms of flow in friendship, are not the only principles of information distribution. Others include need, entitlement, and obligation—a list that is probably open-ended. In a healthcare context, for example, when a patient shares with her physician details of her current and past physical condition, the reigning norm is not discretion of the subject (that is, free choice of the patient) but is closer to being mandated by

> the physician who might reasonably condition treatment on a patient's readiness to share information that the physician deems necessary for competent diagnosis and treatment. Another difference from friendship is that in the healthcare context, the flow is not normally bidirectional. Confidentiality of patient health information is the subject of complex norms—in the United States, for example, a recent law stipulates when, and in what ways, a physician is bound by a patient's consent: for example, where it is directly pertinent to diagnosis and treatment, where it poses a public health risk, and where it is of commercial interest to drug companies.[124]

3.3.3 3 elements

There are 3 key elements which Nissenbaum thinks affect whether sharing a particular piece of information is appropriate:

1) The type of information
2) The actors involved
3) The way the transmission occurs

She writes

> … informational norms are defined by three key parameters: information types, actors, and transmission principles….Whether a particular flow, or transmission of information from one party to another is appropriate depends on these three parameters, namely, the type of information in question, about whom it is, by whom and to whom it is transmitted, and conditions or constraints under which this transmission takes place. Asserting that informational norms are context-relative, or context-specific, means that within the model of a differentiated social world, they cluster around and function according to coherent but distinct social contexts. The parameters, too, range over distinct clusters of variables defined, to a large extent, by respective social contexts. {Nissenbaum:2015ki} p.839

3.4 Her opponent

THIS SECTION IS TERRIBLE AND NEEDS SERIOUS REWRITING. I CONFUSE THE DISTINCT AND DISTINCTIVE CLAIMS SEVERAL TIMES IN WHAT FOLLOW.

To get a better sense of how her view works, it will help to give her an opponent. That way we can see where she thinks the opponent is going wrong. Here's what her opponent is claiming:

> Online privacy is a distinctive venue defined by the technology and protocols of

the net for which a single set of privacy rules can / should be crafted.

The opponent is thus making two claims.

3.4.1 Distinct

First, her opponent is claiming that the online realm and thus online privacy is distinct from other social realms. It requires its own set of rules, which will be different from the rules which operate elsewhere.

It may be helpful here to think about sports.[8] Each sport is *distinct*. For one, it has its own set of rules. If you know the rules of cricket, you know nothing about the rules of baseball. The rules of cricket and baseball are *distinct*.

Similarly, if you invent a new sport, you need to invent a whole new set of rules that will be distinctive of that sport. When mixed martial arts became a sport, rather than just an organized brawl, it borrowed rules from boxing and judo. But because punching someone in a judo match or choking a boxer get you disqualified in those sports, the MMA's rules make it a distinct sport.

If you are trying to invent a new sport and come up with something that has all the same rules as an existing sport, you have failed to create a distinct sport.

3.4.2 Distinctive

Second, her opponent is claiming that online privacy will have a distinctive set of rule. Online activity has its own nature and presumably that nature is shared amongst everything online. It would be a mistake to mix up online and offline activities.

The rules of baseball are *distinctive* of baseball. They make an activity a game of baseball. Setting aside minor variations, if you are playing a game that doesn't involve hitting a ball in order to run bases, 3 strikes and you're out, 4 balls and you walk, you are not playing baseball.

3.4.3 Contra distinct

Regarding the claim that online activity forms something distinct from regular life, she claims that the online environment

"is not a single social realm, but the totality of experience to be conducted via the

8. Cross your fingers, Adam's going to try a ball-involving sports analogy….

> Net, from specific websites to search engines...crisscrossing multiple realms." [38]

To see the evidence for this, think of all the things you did online yesterday. Maybe you watched some movies on Netflix, checked out a cat in a dinosaur costume on a roomba on youtube, submitted your journal for class, scrolled through the pictures from your favorite celebrities and most attractive friends on Instagram, placed a refill prescription at the pharmacy, checked your bank balance, and impatiently swiped left before a lingering swipe right in a search for love (or whatever one finds on tinder).

How are those all the same thing? Sure you did them all on your phone, tablet, or computer. But why does that matter. You also called your mother on[9] your phone and texted your friend. Are those also the same? You worked on your paper or wrote a python script to make your life easier on the computer. Are those the same?

It doesn't seem like the instrument with which you did all these things should be decisive. If you found one of those weird phones which connect via a cord to the wall and called your mom on that, is that different?

Indeed, if you're like me, you may be extremely puzzled by the questions above. What would it even mean to say that all of these actives are the same? It just seems like they are different things which just happen to be done through the same device / medium. That, I think, is Nissenbaum's point.

3.4.4 Contra distinctive

Against the opponent's claim that online activity has its own is distinctive set of rules Nissenbaum argues that online activities are deeply integrated into social life. She writes

> "Not only is life online integrated into social life, and hence not productively conceived as a discrete context, it is *radically heterogeneous*, comprising multiple social contexts, not just one, and certainly is not just a commercial context where protecting privacy amounts to protecting *consumer* privacy and commercial information." [38]

For one, some online activities like shopping are continuous with real life activities. You might browse and purchase an item online and pick it up in a building made of brick-and-mortar called a 'store'.

At the very least, activities online have power to affect IRL communications,

---

9. You did call your mother, right? No? Go do it now. She's probably worried.

transactions, interactions, and activities (and vice-versa). Insult your friend online and then act like nothing happened when you see them in person. If they get pissed off, condescendingly tell them that you insulted them online so they shouldn't be mad at you in person. See how well that works. (Don't do this.)

Or, to use another helpful analogy, it seems like her opponent's reasoning is like someone who rants that all criminals should be executed. They insist on talking about 'crime' without recognizing that there are many kinds of crime (e.g., murder, arson, mayhem, larceny, and jaywalking)[10] .

3.5 Decision heuristic

Let's suppose we buy that there are already existing norms governing information flows which apply to real life contexts and that these contexts align with online contexts. How should we go about translating our in-person norms to online norms?

Nissenbaum proposes a four part approach for determining what to do with informational privacy within a novel area.

(1) Locate relevant existing contexts
(2) Explicate entrenched informational norms
(3) Identify disruptive flows for the online contexts
(4) Evaluate disruptive flows against norms based on general ethical and political principles as well as context-specific purposes and values.

3.5.1 Locate relevant existing contexts

The tasks embodied in the first two steps seems clear. Figure out what the relevant in-person contexts are. Then figure out what the norms around information flows are in those contexts. Though of course actually carrying out those tasks may be tricky.

In some cases the in-person contexts that correspond are obvious —online banking and in-person banking. In others, this is more difficult. We'll come back to that in a moment.

3.5.2 Explicate existing norms

Similarly, figuring out what the relevant norms are can also be difficult. She wants us to

10. Thanks to Johannah Caliban for this example.

start with things like laws and policies. Those are large scale reflections of commonly held norms.

It is worth noting that in a society that is diverse on religious, cultural, political, and other dimensions, going with the laws enacted by those in the political majority may be misleading. Indeed, different populations may have different norms around information. Think of how some families seems to share and fight about everything that's on anyone's minds whereas other families keep disagreements under wraps, save for the occasional passive aggressive comment over dinner. That may not be cultural in the relevant sense, but at least you get the idea.

That said, one strength of Nissenbaum's view is that it is flexible and can handle all sorts of messiness in actual norms. We'll come back to this later too.

3.5.3 Identify disruptive flows

The next step is to turn to the online context and determine how it is that information may be flowing across contextual boundaries.

3.5.4 Evaluate flows against norms

Finally, we are to "evaluate disruptive flows against norms based on general ethical and political principles as well as context-specific purposes and values."

Part of this makes sense. Once we know what the existing norms are and how online stuff may breach those norms, we evaluate what to do.

However, the other part, concerning 'general ethical and political principles' . That's where things get interesting. But let's put that aside for a moment.

3.6 Easier cases

Let's see how this picture is supposed to work with a couple of easier cases.

3.6.1 Privacy in medicine

It's easy to imagine (or, sadly, recall) situations where someone in a medical office fails to adequately protect patient information. For example, a doctor may fail to close the door when discussing test results; office staff leaving your chart sitting on the counter for any passerby to read.

Notice that this involves not just protecting information about the patient, but also the patient's questions. Would you ask the same questions with an audience?

Thus if we turn to online medicine —google searches, web md, etc— presumably these norms still apply.

3.6.2 Privacy in banking

Suppose you're a bank executive trying to decide whether to allow online advertising to your customers. The place to start (in addition to the law) is to think about customers expectations of privacy when they bank in person.

Most customers would be concerned if the next person in line stood right behind them as they talked to the teller. Similarly, a teller who shouts "Sir. You have $7.23 in your account. You cannot withdraw $20!" so everyone can hear would quite rightly be rebuked.

That tells us that customers have an expectation of privacy when it comes to exchanging information with bank employees. None of that changes when the transaction happens online. As she writes

> "Whether you transact with your bank online, on the phone, or person-to-person in a branch office, it is not unreasonable to expect that rules governing information will not vary according to medium" [39]

3.6.3 Netflix, youtube, etc

Nissenbaum argues that data about online video use should be governed by the same principles as privacy in video rental stores. In particular, she claims that the constraints binding West Coast Video based on the Video Privacy Protection Act of 1988 should apply to online videos as well. [2011; p. 39]

3.7 Harder cases

3.7.1 Analogs of social media?

However, when we turn to things like social media, it's harder to sort out the relevant analogous in-real-life practices.

What would be the relevant real life context be for a social media site facebook or instagram? The world's most awkward party where your relatives, friends, co-workers, exes, and random people you had a nice conversation with once all mingle?

What about Twitter? As far as I can tell, its nearest analog is an angry mob.

3.7.2 2 guidelines for locating contexts in hard cases

So how do we determine the contexts when it's not obvious? Nissenbaum writes

> "Where correspondences are less obvious, such as consulting a search engine to locate material online, we should consider close analogies based not so much on similarity of action but on similarity of function or purpose." [43]

More broadly, she suggests two guidelines for determining the relevant context when it isn't clear:

(1) Look at how the company presents itself to users

(2) Look to ends/purposes/values involved and work back to determine the relevant norms

3.7.2.1 How the company presents itself

The first guideline is fairly straightforward. We should follow how the online offerings present themselves to the consumer in determining which norms are relevant. Thus if a site presents itself as an online university, the relevant norms are those which govern universities. If a site presents itself as similar to a library, the norms are those which govern libraries

Interestingly, Nissenbaum wants this to apply even if the data has different uses to the consumer and investor facing sides. Thus if the data is collected from the consumer under the guise of being a medical site, it cannot be sold off as an asset.

However, we might wonder about situations where the company is completely upfront about collecting and selling your data. To construct a case that might be a problem, we would need the upfront company to be clashing with established norms from a context. For example, if the medical advice website tweeted all the search questions in real time so that was part of the appeal —you can go to the site for information about fibromyalgia or just to see all the weird stuff people are looking up.

Note also that this is similar to Sax. [todo]

[Sidenote] This might raise some questions about the data for our accounting majors:

Set aside for a moment the issues about amortizing the data. [If I'm understanding this correctly] For something to be an asset, it has to be tied to the company's main business operations. If a company provides medical information online in exchange for collecting data from its consumers, which it then sells, is the data an asset?

3.7.2.2 Looking to relevant values or purposes

When there is no clear analogy to reason from, we should instead start from ends/ purposes/values and work back from there. This is tricky to sort out.

She's basically saying that if we can't tell what the relevant context is, we should think about what sort of things are at stake in the use of the site (etc) and then go off of the norms that we already have concerning those things. So, for something like Twitter, we might think about values like free expression, public accountability of governments / companies, and the importance of public disagreement in a democracy. From there we would consider what norms are associated with those values. Perhaps, a general presumption in favor of non-interference by governments (or more generally powerful entities) would apply here. This might be in line with 1st amendment law and policy in the US.

Note that the relevant norms can come from law and policy. But they can also be found in commonly held reasonable expectations, i.e., what would an average person expect about privacy in that situation.

There are a variety of ways of testing when something is a reasonable expectation. I often find it helpful to think in terms of complaints. People complain about all sorts of stuff all the time. Sometimes when you hear a complaint, you wonder about the complainer's sanity or what else might be going on in their life. Othertimes, you think they have a point. If the bartender gives you a beer that's 90% foam, no one would bat an eye at your complaint. But if the bartender leaves a tiny bit more foam than usual, people will look askance at you if you start complaining; the bartender would be right to dismiss your complaint as unreasonable.

3.7.2.2.1 Problem: does this abandon contexts?

In cases where we're looking to values, purposes, et cetera, we might worry that we've thrown the contextual integrity approach overboard. It seems like her advice in these cases is to give up on the context based framework? Isn't she just saying, yeah, if you

can't tell, just give up and do ethics / political philosophy?

Not necessarily. In the worst case scenario for her picture, we're just acknowledging that some situations may in fact be brand new. That doesn't do anything to undermine the usefulness of her approach for many other cases.

Moreover, there's no principled inconsistency to saying 'Look for contexts and use those; if none exist, you're going to have to figure it out based on other tools we already have.' This is still consistent with her overall approach that we should deal with informational privacy using existing tools / norms / expectations, rather than thinking we need something brand new.

3.8 Objections

Like any good author. Nissenbaum spends some time answering objections she imagines her view will face. Let's go over a few.

3.8.1 Overly conservative

She acknowledges that her view is in tension with the optimism often associated with technological change and 'progress'. As she writes

> One is that by putting forward existing informational norms as benchmarks for privacy protection, we appear to endorse entrenched flows that might be deleterious even in the face of technological means to make things better. Put another way, contextual integrity is conservative in possibly detrimental ways [125]

Note that this isn't (necessarily) 'conservative' in the US political sense associated with the republican party. Instead, the concern is that our laws and policies don't change fast enough to keep up with the pace of technology and new uses of data.

Think of it this way. Suppose someone invents gunpowder for use in fireworks. Laws and policies around gunpowder get made to ensure that fireworks are safe. Then someone realizes that you can put the gunpowder in a metal tube with some rocks on top and point it at people you don't like.[11] Relying on the existing laws and policies

around gunpowder will not help you in managing this new use.

Her response [ToDo]

3.8.2 Contexts as cement shoes

Another worry is that if our regular life practices around privacy change for the worse, applying contextual integrity to the online world entails dragging down online privacy too.

> A second worry is that contextual integrity, being so tied to practice and convention, loses prescriptive value or moral authority. In this era of rapid transformations due to computing and information technologies, changes are thrust upon people and societies frequently without the possibility of careful deliberation over potential harms and benefits, over whether we want or need them. Practices shift almost imperceptibly but, over time, quite dramatically, and in turn bring about shifts in conventional expectations. These changes have influenced outcomes in a number of important cases, such as determining that the Fourth Amendment was not breached when police discovered marijuana plants in a suspect's yard by flying over in a surveillance plane. [126]

3.8.3 Commercial nature of the web

She also acknowledges that the commercial nature of most online activity pushes in a very different direction than her contextual integrity approach. As she points out

- Private payment is the overwhelming means of supporting online activity
- The physical and computing infrastructure is privately owned

---

11. By the way, I based this example on a common but completely false history of gunpowder and guns. This source doesn't matter for point of the example. But since this might sound familiar, let me take this opportunity to set things straight. The story goes that the Chinese invented gunpowder but used it for fireworks, never realizing that it could be a potent weapon of war. Europeans eventually learned of gunpowder from the Chinese and had this insight.
This is bullshit. (And, somewhat racist bullshit at that; it has a ring of "oh those poor simple asians weren't smart enough to realize what they had their hands on.") The Chinese made bombs and gun-like things from the start. The reason guns became important to warfare in Europe first was an improvement in the mix of the powder (more potassium nitrate), which probably came about during the transmission to Europe by Arab traders, and somewhat better metallurgy (to make the guns).

- Most websites are supported by payment for advertising
- The Net is almost completely privately owned by private, for profit entities

Given these considerations, it would seem that the norms of the competitive, free marketplace are the place to look for a regulatory approach.

Indeed, this is already a live alternative. When the FTC and other regulators approach privacy online, they tend to do so from the usual consumer protection mindset. In the US this often means protecting consumers from unfair business practices and subsuming the protection of personal information as a form of protecting the integrity of commercial transactions.

Nissenbaum's response to this is first to emphasize that the web is not entirely commercial. This is part of her claim about the radical heterogeneity of online activity. While many parts of the web are supported by advertising or subscriptions, that does not mean that the activity people engage in is purely commercial. Sure, some people post to Instagram with the aim of becoming a paid influencer. But many of us just want to share pictures of our friends, pets, or dinner.

More importantly, she borrows from Elizabeth Anderson to point out that many functions in society straddle boundaries between the commercial and noncommercial. The fact that private payment is involved does not require total concession to marketplace norms.

We expect things like education, health care, religion, telecommunication, or transportation to measure up to ideals. The fact that people pay for them is not decisive.

Consider, let's see, now what might be an example that everyone is sick of from me. Oh. How about higher education. No one serious thinks that higher education is a fully commercial enterprise. While a university requires money and some of that money comes from its students, there are other values at stake. If students were just paying for diplomas, then we would succeed if every student gets a diploma, regardless of what they learn along the way. (Obviously, we want students to graduate and graduation rates are part of how we should assess the effectiveness of college; the point is that there are other considerations at stake too.

The same is true for any professional (doctors, lawyers, athletes). Profit is important. But we expect more from professionals than just doing the minimum of what they are paid for. An emergency room doctor who maximizes the number of patients she sees

with no regard for whether they survive is a very very very bad doctor, regardless of how much she contributes to her hospital's bottom line.

Therefore, she claims, the fact that most online activity is supported by commercial activity does not establish that informational privacy should be handled as a commercial matter.

3.8.4 Basing on the real world better not mean the real world

[Todo]

There's a danger here that we should keep in mind when trying to use Nissenbaum's theory in a cosmopolitan society where some groups have historically been more powerful than others.