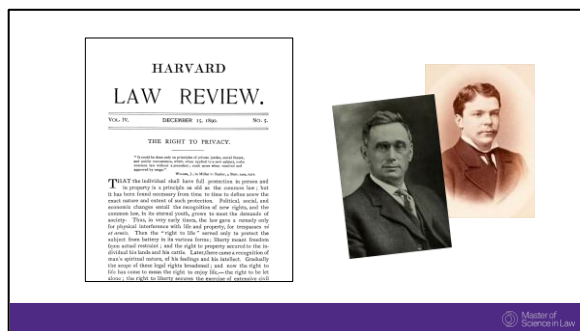


Week 1: Video 1 - What is Privacy Law?

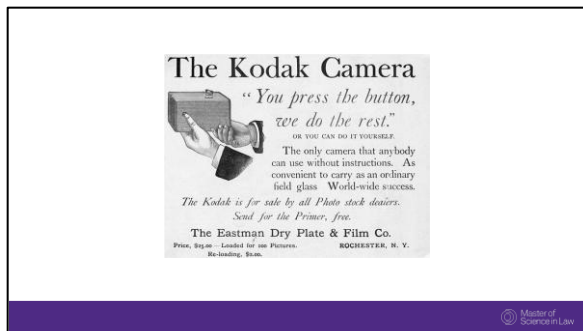


1. Privacy is a growing area of law both in the United States, and internationally. It touches every aspect of our lives. Privacy law is there when you get pulled over by the police, when you talk to your doctor, when you shop online. It governs how we apply for jobs and how we apply for loans.
2. Privacy is not a self-contained area. In this course we'll touch on a host of different issues, from consumer protection and data breach, to nonconsensual pornography, to nosey neighbors. That's why we are going to begin with the fundamentals. Where did this start?

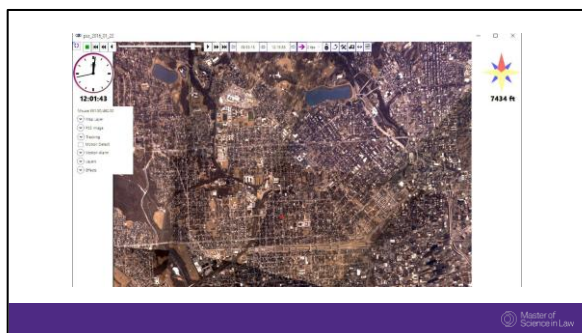


3. American privacy law began with the article you read by Samuel Warren and Louis Brandeis from 1890. One thing I really like about this article is that it is timeless. The authors are talking about how technology is challenging traditional notions of privacy, notions so basic that they barely needed to be articulated before these new technologies were invented. That's a theme we're going to see again and again in this course.

4. They begin their discussion by talking about how the law more and more begins to protect personal dignity. At first the law was concerned with violence of one person against another, then it also protected against threats of violence, and then against slander and libel, which are attacks on reputation. This consideration of intangible injuries is at the core of privacy, and one big question in privacy law is how far we should go in protecting against intangible or indirect harm.



5. The technology that Warren and Brandeis believe is causing this intangible harm in their time is the snap camera. This new type of camera allowed for instantaneous photographs. You could just take a picture without people having to pose for you. This meant that the tabloids of the day could run pictures alongside their stories of famous people.
6. Previously the person had to stand still so long that you more or less had to ask for permission. If the person didn't want to be photographed, they just had to move. That made photography more an issue of contract law – the people involved had to agree, or at least talk. But technology made nonconsensual privacy invasions possible, and that helps explain the rise of privacy tort law. Tort law is how we regulate interactions between strangers – that person you pass on the street.

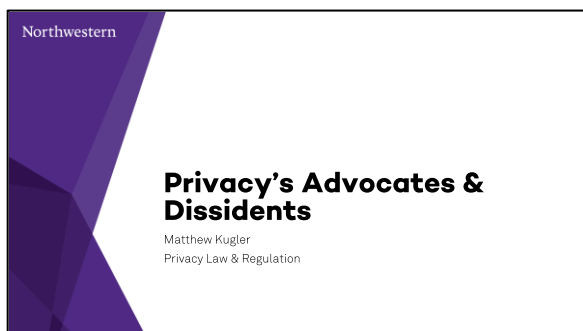


7. Think about a more recent camera-related change in privacy. More and more, we have security cameras on public streets. Some of these are owned by the government – just look up and down Michigan Ave in Chicago – and some are owned by private people. Think about how digital photography and digital file storage changes have allowed for this development. Basic video doorbells mean that you can now go back and check who didn't clean up after their dog, or to confirm a neighbors alibi for a murder.
8. In addition to technological change, another development that Warren and Brandeis worried about was the rise of gossip. They thought that allowing the press to report the goings-on of famous people – like, say, successful lawyers and their friends – was going to crowd out real news. Gossip is so much more fun than serious reporting. Better if you generally need permission to report this kind of stuff. This is a strongly paternalistic impulse, but that doesn't inherently mean it is bad.
9. Others defend the importance of gossip as part of a balanced diet of information. Gossip tells us what other people think is good and bad, and who other people think is good and bad. Gossip tells us which classes to take and which restaurants to avoid. It is both a mechanism for bullying as well as a way to share valuable information and learn from the example of others.
10. This brings us to the limits on privacy. Warren and Brandeis outline several. For one, they think that newsworthiness should be a defense to publishing private information. And, as you'll see, it generally is. Particularly, they think that political candidates should expect to have far less privacy than other people because their capabilities and character are directly relevant to the public. We'll talk much more about this later on.
11. They also think that there should be republisher immunity. This holds that once something that is private gets published by one newspaper, other papers are allowed to pick it up. This is again something that the modern law has adopted.
12. Mostly, though, I want you to think about how well this article would work today. Privacy law presents the same themes over and over:

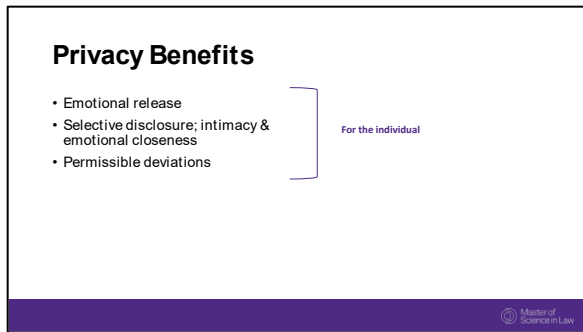


13. We have technological change enabling ever more efficient invasions of privacy. We have the debate over whether these privacy invasions produce socially-valuable information or meaningless gossip. And we have the question of what limits we should place on whatever privacy rights we choose to grant. Thank you.

Week 1: Video 2 – Privacy’s Advocates and Dissidents.



1. Today we’re going to talk about why we might value privacy. One idea is that privacy is valuable for itself. This most often comes up in discussions of bodily autonomy and sex. These readings, and most of this course, however, view privacy as an instrumental good. We value it because of what it produces, whether or not it makes people happier and the world a better place.



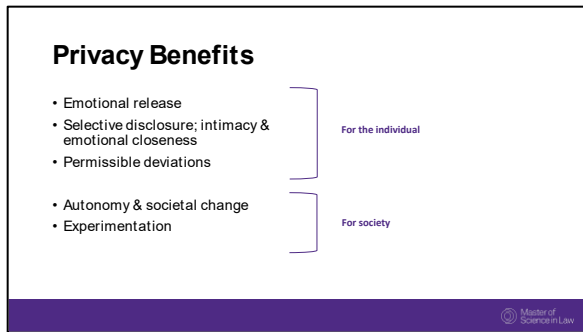
2. There are two ways to think about privacy within this instrumental perspective. One is by looking at privacy's benefits from the standpoint of the individual. This is largely Westin and Cohen in our readings. How does privacy help particular people?

a. One thing privacy gives us is the ability to take off all the masks we wear day to day. You might be a spouse, a parent, a worker, a friend, and an amateur softball player all in the same day. Each of these roles has a different set of social expectations, and potentially is draining. This also goes to the idea of privacy as giving us a space for emotional release. After that rough meeting with your boss, you go into your office or the bathroom, close the door, and then, only then, can you express how you feel. Out in the world, we must keep playing our roles.

b. Privacy also plays a role in helping us develop intimacy. It lets us filter and decide how much of ourselves to share with particular people. This kind of selective and reciprocal disclosure promotes feelings of emotional closeness. There is intimacy both in the selection of how much to share, and then in the ability to have unfiltered exchanges with those close friends around whom you can be your true self.

c. A final individual benefit of privacy is that of permissible deviations. The idea here is that minor sins – speeding just a little, sneaking a drink at a work lunch, are extremely common. There would be a risk of too much justice were all these exposed. This also gets to another idea. Privacy makes it more likely that you wouldn't be misjudged based on a small snapshot of behavior.

3. The key insight about this individual perspective to privacy is that we should generally be willing to let people trade these benefits. To the extent protecting your privacy is about making you a happier and more fulfilled person, you should be allowed to decide how much privacy you really want.



4. The other major pro-privacy perspective is that privacy is necessary for democracy and for society. This is mostly Cohen and Allen from the reading. This collective justification for privacy requires that you not be allowed to surrender or trade too much of your privacy; you having privacy benefits other people.
- This perspective says that we need privacy to have real autonomy, to make choices that are free from coercion. When we know we are being watched, there is a tendency to do not what we want to do but instead what we want to be seen to be doing. Think about how you might change your reading or TV watching if everyone got to see what you are consuming.
 - On a societal level, losing privacy could lead to two kinds of bad consequences for autonomy. First, it might be that many people would really like to be reading trashy romance novels but really don't want to be seen to be doing so. Without privacy, all of these people would have to forgo the pleasure of reading what they want to avoid being embarrassed in front of their peers.
 - The second concern is more serious. Imagine that you're in favor of something socially transgressive, like gay marriage was in the early 2000s or like marijuana legalization is today. If you can't explore this in private, then your options are to remain silent or take the chance and find out just how tolerant your boss really is. In a world with privacy, you can talk about it with your friends and engage in low-level activism without needing to make it part of your public identity. And it is often through such private conversations that we begin to see societal changes. Think back to how views on gay marriage evolved.

5. Related to these points is that idea privacy gives you space to figure out who you are and to try out new things. If you want to experiment with new ideas or experiences, you may not begin by telling those around you.
 - a. Not everyone wants their friends to know about that first standup comedy class they are taking, or that they are just beginning to rethink their sexual identity.
 - b. So privacy in this sense can contribute both to individual good as well as democratic health. It lets social differences evolve.
6. The key insight of privacy's social value is that we should sometimes demand that people not surrender privacy. It is important for you to be able to keep your privacy not just because it makes you happier, but also because our world doesn't work as well if everyone can tell what you read or what you search for on the internet.

Privacy Drawbacks

- Social fraud
- Little sins matter
- Knowledge is power
- People can be trusted to decide what is relevant



7. This brings us to our last major privacy perspective, that privacy is often bad. This is Richard Posner's point of view. To him, privacy is a form of social fraud. You need privacy only to pretend that you are something you're not. The world would work better if people knew more about each other rather than less. Exposing secrets is socially valuable.
 - a. Take the earlier idea of permissible deviations. On one hand, maybe the world is a better place if everyone is allowed the occasional "slip" on their expense account, or their occasional time speeding or running a stop sign. On the other hand, maybe the world is a lot worse for it. Stop signs exist for a reason, and cheating on your expense account is fraud. Maybe it would be better if we could punish people for the small sins before they had a chance to become large sins and cause real damage.

- b. The two contexts in which Posner's perspective is best considered are employee hiring and dating. In each case, the "applicant" probably has things they want to hide. Maybe they shave off a few years or a few pounds on their dating profile, or want to omit that job they were fired from on their resume. But if everyone does that then the marketplace doesn't work nearly as well because the people you are "applying" to need to know things about you. Your potential romantic partner has a legitimate interest in knowing that you have a history of road rage, and your potential employer may have a need to know that you've had trouble at your last several jobs. You'd like to keep these things secret, but maybe you shouldn't be allowed to.
8. The problem with Posner's perspective is that it assumes a lot of rationality. Take someone with a minor criminal history as an example. Some people won't want to hire him or her. Posner would argue that, if people are wrong to not want to hire such a person, then the market will solve. Someone will see reformed criminals as an untapped pool of laborers and will make their business stronger by hiring them. But it isn't clear the world works that way.



This is why "Ban the Box" laws - which forbid employers in some states from asking on a job application whether an applicant has a criminal history - has gotten so much traction. We don't always trust people to be rational.



- a. You could say much the same thing in the dating context. Even good people don't start out their dating process by airing their dirty laundry – it just isn't done.
 - b. In defense of Posner, though, some disclosures are made up front. More information is often clearly better. Does this person want a serious relationship or kids? Is this person approximately the right age? What does this person think is fun?
9. And even Posner, the privacy skeptic, says that one thing people should want to know about their friends is whether they are discreet. So everyone agrees that some kind of conversational or intimate privacy is important. But it is equally fair to say that even Westin, Allen, and Cohen aren't fans of all privacy. I have to imagine that they're not universally opposed to background checks.
 10. When thinking about Posner versus the advocates of privacy, it is helpful to begin with the assumption that each is right in different areas. So when do we want to force honesty, and when do we want to tolerate deception? How much should employers know about current and potential employees? Thank you.

Week 1: Video 3 –Intrusion Upon Seclusion?

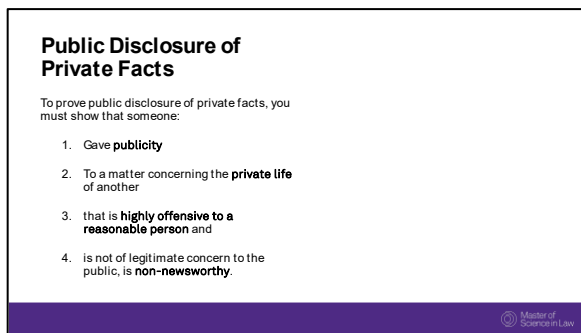
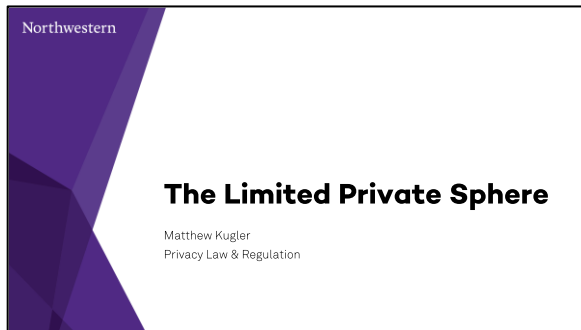
1. Now it is time for our first privacy tort: intrusion upon seclusion. Let's take a second and be explicit about the elements. To prove intrusion upon seclusion you need to show: a) Intentional intrusion, b) upon the solitude or seclusion of another in his private affairs or concerns, c) that is highly offensive to a reasonable person. So you need to intentionally violate privacy in a way that reasonable people think goes too far. Importantly, this is *not* about telling people or publishing what you learn. This is the "right to be left alone" part of privacy.
2. Our first case goes over a series of examples of things that are and are not intrusions upon seclusion. If you look at the ones that are, you might think "hey, aren't these already illegal?" Some of them are trespasses, or violations of

wiretap law, or even theft. But some are not, and many of these other laws have technical definitions and exceptions that can cause trouble. For example, it is said that “eyes cannot trespass.” Using binoculars to see into someone’s bedroom window is an intrusion upon seclusion, however.

3. The best way to think about intrusion upon seclusion is as protecting a person’s reasonable expectations of privacy, a phrase you might have encountered if you’ve taken a class on criminal procedure. People expect privacy in their hotel rooms, except from hotel staff. Though people know you can see into their ground floor windows, they expect privacy in their upstairs rooms that have the curtains half closed.
4. On the other hand, people generally do not have expectations of privacy on public streets. If a person follows you on a street and takes pictures of you, that will generally not be an intrusion upon seclusion. That sounds much more like basic private investigator work or newsgathering. Given how much can be learned from a person’s travels through public spaces, this is an important exception.
5. Also, recall that intrusion upon seclusion is about just that – intrusion. Repeatedly calling late at night or repeatedly knocking on a person’s door at odd hours could easily count as an intrusion even if it does not serve to gain information about a person.
6. One final note is that asking around about a person is not an intrusion upon seclusion. In a famous case, General Motors interviewed family and friends of Ralph Nader hoping to learn embarrassing information about him. This was held not to be an intrusion, though some of GM’s other conduct did leave them open to liability.
7. Now let us look at the *Safai Club v. Rudolph* case. Here we have a recording of a conversation that occurred in a restaurant. The court here swiftly determines that the key question is whether there was an expectation of privacy in the conversation. The person making the recording, Rudolph, argues that it was a public restaurant, so no privacy should have been expected. But Safari Club claims it is more complicated than that. No one was in an obvious position to overhear the conversation, and Whipple, the person being recorded, claims to have fallen silent when the waitstaff approached. So the court says that it is a question of fact whether there was an expectation of privacy, and leaves the matter for a jury to decide.
8. Key in the case is the role of a recording. It was certainly not an issue that Rudolph heard the conversation – he was part of it, after all. But recording something is different than simply hearing it, as the subsequent post to YouTube makes clear. The law is particularly sensitive about recordings, as we’ll see when we get to wiretap law. And, as you may have gathered, wiretap law itself doesn’t help Whipple here: whether the conversation is protected

against wiretapping under the wiretap statute turns on the very same expectation of privacy that is key to the intrusion tort.

Week 2: Video 2 – The limited private sphere.



1. This brings us to another privacy tort, public disclosure of private facts. Again, take a look at the elements. To be liable for public disclosure of private facts you have to a.) Give publicity b.) to a private matter c.) when the matter is of a kind that is highly offensive to a reasonable person and d.) is not of legitimate concern to the public, is non-newsworthy.

a. Note the differences between intrusion upon seclusion and public disclosure. Intrusion was about getting information and going into places. This tort is about spreading information.

b. And, importantly, this tort has a newsworthiness defense. If you obtain highly private information about a politician that is relevant to his or her character, you can probably publicize that without being liable under public disclosure– the information is of legitimate public concern. But you could still be liable for intrusion if you had to violate privacy to get that information.

c. These torts also have two common elements: privacy has to be violated and either the intrusion or the publication has to be highly offensive. This video is about the privacy question. What counts as private for these torts?

2. Let's start with the simple case of *Finley v. Kelly*. There we have an explosive lovers' quarrel, with shrapnel flying in all directions. From a public disclosure standpoint, it raises a basic question: is this a disclosure to the public? This tort is not meant to apply to mere gossip; it is aimed more at broad publication. But some courts, including this one, think that disclosure to a small number of highly relevant people can count as sufficiently public. In general, internet publication will always count (think Facebook, X, message boards). Disclosure to a small number of friends will almost never count. And in between is fact dependent.
3. Moving on to what counts as private, consider one of the classic public disclosure of private facts cases *Gill v. Hearst Publishing*. Gil is presented as if it is straightforward: the couple is photographed in an amorous pose at the Farmer's Market. Or perhaps I should say an allegedly amorous pose; opinions diverge on just how happy these people appear. The court says that a farmer's market is public, therefore their pose was not private, therefore there is no case. Simple.
4. Here, the majority is channeling what will be the dominant view of American law. "If in public, then not private."
 - a. As the majority says "it is significant that [the photograph] was not surreptitiously snapped on private grounds, but rather was taken of plaintiffs in a pose voluntarily assumed in a public market place"
 - b. You'll see this argument made again and again throughout discussions of privacy. Wherever you go, you will *probably* not be noticed. But you might be. And, if you are unlucky enough to be photographed somewhere that you'd rather not have everyone know you went, that is probably your problem.
 - c. Think about how this works in the more modern context of things going viral. I sometimes show a video in class of a little girl breaking into happy hysterics after being surprised by her mother with a kitten. This video has received millions of views and will presumably be available online this girl's entire life. There are also plenty of stories about people going viral after being publicly shamed – or, rarely, publicly praised – for what would otherwise have been a fairly obscure private act. The "if in

public, then not private” rule does a lot of work in these cases.

5. This brings us to the meatiest case of the day. In re Facebook is one of the Cambridge Analytica cases. People had made posts on Facebook and then limited access to those posts to “friends only,” meaning people they had pre-approved. Facebook’s conduct was alleged to have shared those posts more widely through third party apps. Facebook explains that this shouldn’t be a public disclosure because, after all, the people themselves had shared the information. How can a post visible to potential hundreds of “friends” be private?
6. The court here thinks it still might be. Though the posts were visible to potentially many “friends,” they were not visible to the public at large. All privacy is relative. Even sex is not fully private – it generally involves more than one person. So this court was not willing to say as a matter of law that information visible to Facebook friends was fully public.
7. The court then looked to the language of the terms of service to see just how public this information might have been. Facebook here wins some and loses some. Some of its sharing was covered by its extensive terms of service, and some was not. This leads into a theme that will be with us throughout the course: companies need to beware the privacy promises that they make.
8. In one case I worked on you could clearly watch the company’s privacy promises go from being vague and reassuring – “we care about your privacy and keep your data secure” – to highly specific and highly disturbing. Companies have learned that the PR risk of disclosing offensive privacy practices is sometimes less than the litigation risk of not disclosing them.
9. Both Facebook and Gill prompt us to think about what is and is not public, and that is the question I want to leave with you. If our baseline assumption is that everything exposed to the public is not private, when should we relax that? Because, if we hold to it, a world with lots of CCTV cameras is going to be a very public place. Thank you.

Week 2 Video 2 – Newsworthiness and Republisher Immunity

1. The question of what you should be allowed to find out about another person is one of the most fundamental in privacy law. Here we see it in the guise of newsworthiness. You’re not allowed to share private information about a person if doing so would be highly offensive to a reasonable person, unless the information is newsworthy. So today’s cases ask courts to decide what is newsworthy.

2. Let's start with Shulman. This case involves the publication of the suffering of a woman who was in a horrendous automobile accident. What I like about this case is the discussion of necessity. You certainly could have told a story about automobile accidents, or a day in the life of a flight nurse, without including identifiable footage of the victim and her exact words on being removed from the wrecked car. But the standard is not necessity. That they could have told the story without that information doesn't mean the information wasn't newsworthy. This is a critical distinction when you think about actual editorial decisions. Stories often include a lot of background facts about people that are not necessary, but serve to humanize them.
3. Doctrinally, the Shulman case tells us that a fact is newsworthy if a "logical nexus exist between the complaining individual and the matter of legitimate public interest." It also highlights the idea of balancing the strength of the public interest with the sensitivity of the disclosure, saying that intensely personal or intimate revelations might not be newsworthy if they bear only a slight relevance to the topic of interest. Later cases are even more explicit about this, talking about both the strength of the "logical nexus" and the "proportionality" of the disclosure.
4. In this way, the Shulman case also reminds us of the importance of narrative. The story being broadcast wasn't "shattered wrecks are gruesome, come and gawk." Instead it focused on the nurse, and the difficulties of her job. Part of that story is the challenge of dealing with victims in moments of trauma.
5. Thinking about narrative also helps us understand the YG case. There we have a couple that underwent IVF being inadvertently exposed in the course of a news report on a hospital sponsored party for families that had used the procedure. IVF was very newsworthy at the time – the party was in 1988. But no one made an argument that the plaintiffs themselves were newsworthy. Their inclusion was likely even accidental – they appear only in the background for a few seconds.
6. Ironically, the news crew would have been on firmer ground if they set out to expose and humiliate the couple. Then their exposure would have been more clearly linked to the story. As it was, the court thought that the highly sensitive medical and procreative fact of IVF should not be exposed for such a weak nexus to the story.
7. This brings us to the Sipple case, which I want to use to make two points. First Sipple introduces us to the idea of republisher immunity. Once something has been made public through publication in a source – however obscure that source might have been – others can safely go forward and publish it. This might sound like an obvious point, but this case points to its power. Here Sipple was well known to be a gay man in one location, and his sexual orientation was readily discernible to people who read a certain set of

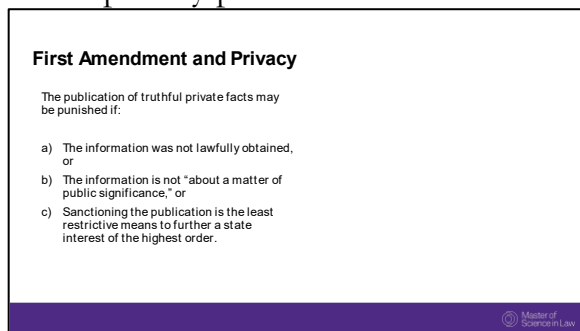
publications. But people outside that location, in particular his immediate family, did not know and had no way to find out. Nevertheless, republisher immunity protects the national publications that bring the information to everyone. Thinking about the needs of a news organization, particularly one in the modern era where even small publication outlets may be indexed online, one can see the value of such a rule.

8. Second, I want to apply the logical nexus test to Sipple. One can easily argue that the disclosure of Sipple's sexual orientation was extremely sensitive - it predictably caused major problems with his father - but that it was also extremely relevant to the narrative that the news organizations were crafting. Specifically, the news organizations could make his sexual orientation relevant by talking about
 - a. First, the reaction of President Ford. Was the President responding appropriately to having been saved by a gay man? It turns out that Ford did thank Sipple in a private letter, a letter that Sipple apparently cherished, but he did not publicly thank him, and some interpreted that as a slight.
 - b. Second, the news organizations focused on the ways in which Sipple's heroic acts were counter to a negative stereotype about gay men.
9. These both sound like very legitimate news narratives. The problem with them is that they run the risk of making everything newsworthy. What if Sipple had cowered meekly, therefore confirming a negative stereotype? Would that also have been news?
10. The answer might be "yes." But that highlights a distributive aspect to privacy protection. If you're numerical minority, you're likely going to often be highlighted as one of the few or the first BLANK who BLANKS. If you're in one of these groups, there may be a good narrative for why almost anything you do is newsworthy. That this attention may often be positive does not mean it will always be welcome, and sometimes obviously it will be negative. When thinking about privacy costs, we should always remember that these costs are not born evenly across society.
11. For a particularly salient example of this, one of the first major news stories about Barack Obama was his election to the Presidency of the Harvard Law Review.
12. It may seem that very little is not newsworthy given these cases. But recall the distinction Warren and Brandeis drew between news and gossip. For these things to be newsworthy, they have to be discussed in the context of quote unquote legitimate news. If the inclusion is gratuitous, or the main story is the prurient nature of the material, then courts will not find the disclosures to be newsworthy. No amount of demand for, or interest in, celebrity sex tapes will make them newsworthy. And, even in the context of real news, courts will

sometimes find a lack of minimization to be enough to create liability. The great challenge is to distinguish that which cannot legally be published from that which, in the views of some person, was unwise or unnecessary to publish. Newspapers tend to get broad discretion in this area. Thank you.

Week 2 Video 3 – First Amendment and Public Disclosure

1. Whenever people are being punished for speaking or writing, you should start thinking about the First Amendment. The cases covered here should hopefully give you some sense of when the First Amendment is going to trump basic privacy protections.



2. The doctrine here is fairly simple. The publication of truthful private facts may be punished if
 - a. The information was not lawfully obtained, or
 - b. The information is not “about a matter of public significance,” or
 - c. Sanctioning the publication is the least restrictive means to further a state interest of the highest order.
3. The first rationale covers a lot of ground. This is why you can’t wiretap someone and publish the results. This is why you can’t leak classified information. As we’ll see in Bartnicki, this isn’t perfectly straightforward, but it largely tracks what you’d expect.
4. The second rationale should also make sense to you. Not about “a matter of public significance” sounds a lot like “not newsworthy,” and newsworthiness is already a defense to publication of private facts. At a minimum, this rationale means that the tort is constitutionally required to have that safety valve, that you can’t punish someone for publishing newsworthy private things unless one

of the other two factors is present.

5. The final rationale you can use to justify punishing someone for publication is that it is the “least restrictive means” for promoting a state interest of the highest order. The key part here is “least restrictive.” There are actually a fair number of state interests that might qualify as “of the highest order,” but often there will be better means of promoting those interests than stopping publication.

First Amendment and Privacy
The publication of truthful private facts may be punished if:

- The information was not lawfully obtained, or
- The information is not “about a matter of public significance,” or
- Sanctioning the publication is **the least restrictive means** to further a **state interest of the highest order**.

Cox Broadcasting v. Cohn / Florida Star v. B.J.F.

- Can media outlets be punished for publishing the names of rape victims when they get those names from the government itself?
- No. Not least restrictive means. Government should be more careful.**

6. We first see these factors tested in Cox Broadcasting and Florida Star. These are two very similar cases in which the names of rape victims are accidentally disclosed to the media and then published.
7. In Cox Broadcasting, the idea is that court records need to be open for public inspection, so if you want to keep something in court records private you should stop it from getting in the records in the first place. In Florida Star, the idea is that if you don’t want the media to publish the names of rape victims then you should not give the media the names of rape victims when you provide them with police reports.
8. Though the justices are aware of the importance of protecting victim privacy, in each case they believe that the government had better ways of doing it. This is the least restrictive means part of the framework. The government could have protected victim privacy while restricting less speech.
9. As the dissent points out in Florida Star, however, this is a little too neat. No system is fool-proof, especially a system that relies on busy civil servants. You’re much more likely to protect the privacy of rape victims, if reporters also bear responsibility for doing so. Also, a court or police department may simply provide less information to the media if it doesn’t have the security of knowing that the media has some obligation to protect victims. That isn’t exactly what we want either.

First Amendment and Privacy

The publication of truthful private facts may be punished if:

- The information was **not lawfully obtained**, or
- The information is not "about a matter of public significance," or
- Sanctioning the publication is the least restrictive means to further a state interest of the highest order.

Bartnicki v. Vopper

- Can the media be punished for publishing illegally obtained information if it was obtained without their involvement?
- No, if the information is exceptionally newsworthy.**
- Balancing of First Amendment harms.

10. The waters muddy, however, as we move into Bartnicki. The complexity now is that the information wasn't obtained lawfully, meaning that normally you could prohibit publication under the Florida Star or Daily Mail test. But the Court here takes a more nuanced view. Looking at the Breyer concurrence, it seems that the rule is as follows:

- First, if the person doing the publishing is also the person doing the intercepting, then the state can sanction the publisher. This is the straightforward application of the illegally-obtained exception.
 - Second, if the person doing the publishing was not involved in the interception, and if the publisher's receipt of intercepted communications is lawful, then the state cannot sanction the publisher *if the information is exceptionally newsworthy*. This is the clean hands part of the test. If a newspaper is handed newsworthy information on a silver platter, it can generally publish it.
11. This outcome comes from an explicit balancing of competing speech interests. There is a First Amendment harm to not protecting the privacy of the phone conversations – people will not be as willing to talk on the phone. There is also a First Amendment harm in preventing publication.
12. If you count votes here, you need Breyer's concurrence to get past 5, which is the magic number on a 9-person court. So let's look at that opinion. It suggests that it is only in those cases where the communication is especially newsworthy that the state can't forbid publication. Factually, it is a bit unclear whether this intercepted conversation is as newsworthy and as much of a "real threat" as Breyer takes it to be – this might just have been bravado by union negotiators. But the rule for the future depends more on whether Breyer thought the threat was serious – which he seems to – rather than whether he was right.
13. The rule in Bartnicki makes a fair bit of sense. It's hard to insist a newspaper sit on exceptionally newsworthy information because of a defect in the chain of title, as it were.
14. But don't overread this conclusion. The government can and does still publish a lot of truthful speech. People who have professional obligations to keep information secret, like doctors and lawyers, can be prosecuted for breaching

those obligations. Private nondisclosure agreements are still enforceable. And laws against the sharing of nonconsensual pornography have generally been upheld. In each case the law is furthering an interest of the highest order and doing so in the least restrictive means.

Week 3 Video 1 – Defamation and Section 230

1. Today we are going to discuss defamation. Defamation is important both for itself and as a window through which we can examine Section 230 of the Communications Decency Act.
2. Defamation has meant somewhat different things at different times. Under modern American law, however, defamation has a clearly defined meaning. It is a false claim about a person that will harm that person's reputation. For the statement to be legally actionable, the statement must be made to a third party – so not just you calling someone a thief to their face in private – and the speaker or writer must have some level of fault, how much depends on who the statement is about.
3. Defamation law has had something of a resurgence the last decade or so. Major defamation judgements stemming out of school shooting conspiracy theories, that's Alex Jones, or 2020 election conspiracy theories (Fox News, Rudy Giuliani), have made national news.
4. Key in any defamation case is a false statement of fact. I can be of the opinion that a politician is a scumbag and that will never be legally actionable – that is just my opinion. And if I say that a politician is “a crook” that too may just be opinion even though it looks like a claim of fact; most people would interpret that as me saying the politician is bad, not me claiming to know they have committed a crime. If I falsely claim to have seen a politician steal a candy bar, however, that is defamation per se – I have made a claim of fact that implicates the politician in a specific criminal act in a way that makes it seem like I meant it.
5. You might think that this means that people are defaming politicians all the time. To some extent, they are. But politicians face a major obstacle in bringing a defamation lawsuit: the actual malice standard. To prove defamation, a plaintiff needs to show fault on the part of the speaker. If the statement is about a random private citizen, that fault might just be negligence – the person should have known better. But if the statement is about a public figure and on a matter of public concern, the plaintiff has to show that the statement was made with actual malice, meaning that the speaker either knew it was false or with reckless disregard for the truth. This is intentionally hard to do. We hold public figures to this high standard because we want people to feel free to

Speak freely about major people and major issues, even though we know people will sometimes get it wrong.

6. Actual malice is easiest to show in cases where a person is making a false accusation or knowingly spreading a conspiracy theory. These are false and known to be false by the person speaking.
7. Section 230 isn't about defamation; it applies to all speech online. But it comes up in the defamation context and this is a good time to introduce it. Section 230 of the Communications Decency Act states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."
8. These are sometimes described as the 26 words that created the internet. Imagine I falsely accuse the president of a crime. I know the statement is false and I post it to LinkedIn. I am certainly liable for defamation in this context. But what about the website on which I post? Can LinkedIn be sued and required to take down the post? In short, no.
9. Though the defamatory post is sitting on LinkedIn, Section 230 clarifies that LinkedIn cannot be treated as the publisher or speaker of the post. It isn't their words. So if the president sues LinkedIn, their case will be swiftly dismissed. If the president wants the post taken down then they have to sue me and get an order compelling me to take it down. They could also ask LinkedIn nicely, but LinkedIn has no obligation to comply.
10. This kind of regime can create a huge problem for privacy plaintiffs. Imagine someone posts something about you on social media that is plainly a violation of some privacy law. You could sue the person who made the post, but first you'd have to find them, and that can be hard. And, if you do find and sue them, you might find them broke and unable to pay damages. The large and wealthy corporation that is actually distributing their illegal content to the world, however, is completely off-limits. You are reduced to, in effect, asking nicely.
11. Section 230 is not without limit. It does not give online services protection against criminal law enforcement, for instance, or apply to intellectual property crimes. But it does allow websites to host defamatory, doxing, and threatening content.
12. Given these evils, why have section 230? Well, consider the example of Yelp. I can post a review on Yelp explaining that I had a terrible meal at a restaurant. The world is a better place for us being able to post this kind of content; we would love to know which businesses to trust, which products are good, and where to get a good burger. But without 230, Yelp would have a major problem. Imagine the business complains to Yelp and says the review is false and defamatory. Imagine it claims I never even ate there? Under Section 230, Yelp can simply ignore this. Were Yelp potentially liable for defamation,

however, it would have a major problem. It would have to decide whether it thought the post was defamatory. It obviously cannot do that, so the only safe thing for it to do would be to take down reviews. This would rapidly make reviews worthless.

13. And we would see the same dynamic with political discussions. Platforms would have to either play gatekeeper, substantially censoring voices to avoid litigation, or engage in no content moderation whatsoever, because then they would plainly not be acting as publisher – publisher have to made decisions about what gets published.
14. So section 230 is enormously consequential, and you are likely to find it cropping up in current events decently often. Thank you.

Week 3 Video 2 – ECPA and Online Monitoring

15. Today we're going to be thinking about the Electronic Communications Privacy Act, the ECPA. This Act contains the Wiretap Act, which involves interception of live communications, and the Stored Communications Act, which stored communications. There is also the pen register act, which is less important for us.
16. The Wiretap Act covers the interception of wire, oral, or electronic communications. This is intentionally broad. Telephone calls, texts, emails, and data transfers are all included. So are live conversations in contexts where people would expect privacy. Think about store security cameras. If one of those cameras overhears you talking to your mother in the shoe department, that is an interception of oral communications. How do stores handle that? Well, it turns out that those cameras are often video-only – meaning no audio – for precisely this reason.
17. Intentionally intercepting such communications by means of a device, disclosing such communications, or otherwise using such communications is illegal. This statute is so broad that there is an explicit exception for hearing aids because, after all, they are a device to intercept oral communications.
18. The Stored Communications Act is similar and applies to electronic storage of communications. Think stored emails and chat logs.
19. The SCA governs Remote Computing Service and Electronic Communications services. Think file backup and email or instant messaging clients, respectively. Lots of websites are neither of those things.
20. The key thing to understand is that message content gets a lot of protection. Providers under the SCA cannot disclose message content without consent or legal process, think warrant and subpoenas. So Google cannot share the contents of your gmail account without your permission.

21. Noncontent information, or metadata, can be shared with “any person other than a government entity,” however. This distinction is hugely important. The classic example comes from physical mail. The address I write on a letter is noncontent information – the address is on the envelope, available for the world to see. But the contents of the letter, what is in the envelope, is content information.
22. Were this a criminal procedure course, there would be a lot to be said about the requirements for warrants and subpoenas. But you shouldn’t worry too much about that today.
23. The big defense to intercepting live communications or accessing stored communications is consent. As you may have gathered, consent is key in American privacy law. When you accept the terms and conditions of your credit card, fill out a HIPAA form with your doctor, or agree to workplace monitoring with your employer, you are consenting to privacy invasions and courts are going to accept that consent as valid.
24. Under the ECPA, a person can monitor or record a communication with the consent of any one party to that communication. Some states require the consent of all parties to the communication, so if you’re monitoring for business purposes be sure to know the laws of your state and of any other state that’s relevant.
25. To better understand ECPA’s use in private litigation, take a look at the Facebook class action.
26. You should initially be surprised by what this case is about. The ECPA is thought of as a wiretapping statute, but here we are talking about web cookies and URLs. This is either a key modernization of the statute, a recognition that more things are communications and more things should count as communications content than before, or a gross misuse of an antiquated statute.
27. Facebook created plugins that were then hosted by other websites. When those other websites loaded, those plugins recorded the URL of the hosting website and the identity of the person visiting it, via the person’s saved Facebook cookies. This happened even if the person was logged out of Facebook at the time. Since these plugins were widely used, this meant that Facebook was informed in real time where millions of its users traveled throughout the internet.
28. The main questions for the court are 1.) Is Facebook a party to this communication and 2.) do people reasonably expect that their internet travels will be shared with Facebook? The court answered “no” and “no” to these, but both are hard questions. Websites often host content from many other sites, and it is quite common for those other sources of site content to gather data about the people that load the website. Many ad networks work on this

principle, hence the repeated citations to cases involving Google in this opinion. If a website incorporates something I made, hasn't it made me a party to any communication it has with someone else? Perhaps, or perhaps not. Courts are split.

29. On the question of reasonable expectations, Facebook got itself into trouble with its various statements. Facebook made it sound like it would not, or perhaps could not, do the thing it was doing here. It's hard for a company to argue that a consumer should expect a company to break its own privacy promises.
30. The real kicker in these cases is the damage calculation. Damages for violating the wiretap portion of the ECPA are either 10,000 per violation, or 100 per day of a continuing violation, whichever is greater. Multiply that by the number of Facebook users and by the length of time this monitoring and these policies were in effect, and you end up with trillions of dollars.
31. This case illustrates a general feature of privacy litigation, and that is the power of privacy class actions coupled with statutory damages.
32. Some privacy claims you can only really bring yourself. If your spouse breaks into your personal email, you can sue them under the Stored Communications Act for that. If someone pries too deeply into your personal life, that's intrusion upon seclusion. But that's just you.
33. Other claims you'd like to bring on behalf of yourself and also everyone else who is in the same situation. Say your doctor mishandles patient data and commits a HIPAA violation that affects the entire office. Now you can't sue under HIPAA directly, but maybe you bring a claim in tort for a breach of confidentiality. You might be able to get a class action certified and have all the patients be part of the same lawsuit. This is a lot more efficient than everyone bringing their own claims.
34. But if you have a class action like that, where you're just suing in basic tort, you have the problem of proving damages. Often in privacy cases that's really hard. It could be that your rights were violated but that the dollars and cents consequences are either negligible or impossible to quantify. That makes for a hard lawsuit. You see this problem often in the data breach context.
35. Sometimes, though, the law makes it easy. When a legal statute gives you some clear privacy right and gives you statutory damages to enforce that right, just like we see with the ECPA, all you need do is prove that your rights were violated. You don't need to prove damages, you can just get what is in the statute. On one hand, that's great. You can get vigorous enforcement of privacy rights. On the other hand, it is immensely dangerous. You end up with attorneys going hunting for minor violations of the statute that affect lots of people, with the aim of assembling a large class and forcing a large settlement.

36. The other mechanism of enforcement is agency action. You complain to a federal agency, and they'll decide on how vigorously to pursue violations and how big the fine should be. That tends to lead to carefully considered enforcement, but generally a lot less enforcement overall. This is arguably the problem under HIPAA and with the FTC.
37. This creates one of the central problems in privacy rights. We know we get under-enforcement if people have to prove damages, but we also know that we get over enforcement if there are high statutory damages. That's why one of the central features of any privacy regime is the question of remedy. What should you get when your rights are violated? Thank you.

Week 3 Video 3 – Workplace Privacy

1. Workplace privacy isn't quite an oxymoron, but it is close. In general, employers can and do monitor a lot that goes on in the workplace. There are a handful of limitations to this, but successful privacy actions against employers are relatively rare.
2. Before we get into the details, it's important to think about why employers want to monitor their employees. Some of this is inappropriate nosiness; employers are people and people are curious. But a lot is aimed at basic business needs. Employers want to know that their employees are on task. They are concerned about employee theft, both of physical objects in the retail context and of intellectual property in the digital context. They want to head off issues of workplace harassment or unprofessional behavior. And they want to identify both good and problem employees.
3. Over the past 15 years, there has also been an increase in what is called talent analytics. Large employers have increasingly been using data from everything from employee surveys to wearable devices to predict and increase employee productivity. Some of this work is incredibly valuable, and some looks a bit like pseudoscience. Northwestern used to host an annual conference on it and presentations ranged from the heartwarming to the terrifying.
4. Whenever a data scientist is given the task of explaining something complex like employee motivation, they will tend to want as much data as they can get. So what are the risks of collecting everything? Honestly, the biggest risk is more practical than legal. Employees do not like to be monitored. This isn't high school, we don't want to get hall passes to go to the bathroom.
5. Another category of risk that is outside the scope of this course is antidiscrimination law. It is hard to win a discrimination suit if you can't show that your employer knew that you were in a protected group. If your employer

- has you wearing a health monitor and that monitor knows that you're pregnant, however, suddenly they have to think about the legal implications of firing you.
6. This brings us to privacy law. If you're employer is monitoring you and you think they're going too far, what can you do?
 7. In general, you can sue for the basic privacy torts like intrusion upon seclusion. If your employer is doing something truly egregious, you might be able to show that it is a highly offensive intrusion into your private life. But this will ultimately come down to a reasonableness analysis, and employers have a lot of tools at their disposal to make sure that analysis comes out in their favor. They basically need to create a situation where it is reasonable for you to expect privacy, they invade it, and their invasion is poorly justified.
 8. The biggest problem for plaintiffs is often the privacy expectation itself. All your employer has to do is post a sign saying that such and such is monitored or will be searched and suddenly the privacy expectation is unreasonable. One old case involved a retail employee whose store locker was searched without her permission. She won the case because she was allowed to bring her own lock – suggesting that the locker could not easily be opened by management – and there was no clear policy permitting locker searches. But she would have lost had the employer simply put up a sign.
 9. More troublesome for employers are the rare sectoral laws that apply to their conduct. One of the biggest of these is our old friend the wiretap act. As you know, a person has to consent to having their phone calls, conversations, and emails monitored. In general, courts insist on this consent being clear rather than implied. So employers are much more careful about recording audio of their employees than they are almost any other data.
 10. Video monitoring gets less protection, but this is very much a state by state thing. Some states have highly limited laws saying that employers cannot put cameras in bathrooms. Other states don't even have that. But then a few states require that employees have specific notice of cameras in non-public areas, like employee breakrooms. In general, however, cameras are permitted in any public space, hallways, garages, and the like.
 11. Another major issue is GPS tracking. If an employee drives as part of their job, then the employer wants to know where they are and how well they are driving. Accidents are expensive, and most employee driving happens out of sight of the employer, so they don't have an easy way of knowing what their employees are doing. But GPS and other vehicle telematics allow employers to have that information in real time. In general, state laws provide mixed protection on this. Some states require the consent of the vehicle owner. If that is the employer, then they can monitor whatever and however they want. Other states require notice and consent of the driver, meaning that the employee must be told and may have to even sign a separate consent form.

12. The final topic I want to discuss is workplace electronic searches. Here, the law tends to be clear. Employers own their own email services, so anything in your work email can almost certainly be viewed by your employer. This is why my consulting work is all through a non-Northwestern email address. It is also difficult for an employee to win a case about their internet activity on a work computer. The new frontier in this area is employer monitoring of what happens on employee-owned devices through mandatory work apps. That is still evolving, and employers do well to have strong and detailed consent forms if they want to limit their liability risk.
13. In general, the power balance here tilts heavily in favor of employers. Employees will generally sign whatever consent forms that their employers require and, absent a union, will not be able to exert a lot of pressure on employers to limit monitoring. This makes specific laws, when they exist, all the more important. State laws establish a minimum baseline of privacy protection – for example, no cameras watching you pee. That, at least, is not dependent on employee bargaining.

Week 4 Video 1 – Medical Privacy As Paramount

1. The theme of the course thus far is that you don't have a lot of privacy. If a company wants to interview your friends to learn your darkest secrets, it is generally allowed to try. If you're in a public place, people are generally allowed to take your picture. If you do something even remotely newsworthy, then that fact is generally something that can be published.
Medical privacy is different. You don't have as much privacy protection here as you might want, but you have a ton more than you do in other contexts.
2. Let's start with the duty of confidentiality. Someone bound by a duty of confidentiality can't blab secrets to the press or to your spouse, or even to their spouse. Most medical professionals in the United States operate under this kind of duty.
3. The duty of confidentiality binds physicians to keep secret private information that is conveyed to them while they are acting as physicians. So pretty much anything you tell them in a doctor's office that is related to your body or health would be covered.
4. But the duty of confidentiality is not unlimited. Many exceptions have been established through both statute and common law. Doctors have a host of reporting requirements for certain kinds of injuries, like gunshot wounds. And, as we saw in the *Lawson* case, HIPAA allows disclosures to avert serious risks to the health and safety of others.

5. Think for a moment about the facts of Lawson. We have an intoxicated person driving herself to the ER, rapidly getting discharged, and planning to drive again. A medical professional telling an on-site police officer about this might prevent a terrible car accident from happening right then. Medical confidentiality was less important than preventing imminent risks to others.
6. Importantly, Lawson could not sue for public disclosure of private facts, only one person was told and it isn't highly offensive to truthfully say that someone is drunk and about to drive. But a duty of confidentiality doesn't care about that. Here the question was whether the disclosure made by the medical professional was "unlawful." And it wasn't; the law specifically allowed for this kind of disclosure.
7. Now a duty of confidentiality is only one level of privacy protection. It means that a doctor can't write an unsolicited letter to someone spilling your secrets. But there is another possible level of privacy protection, an evidentiary privilege. When a relationship is protected by an evidentiary privilege, its secrets are also safe from being disclosed in response to a court order.
8. The Jaffee case asks whether federal courts should recognize a psychotherapist-patient evidentiary privilege. In this case, a police officer shot and killed a man whom she claimed was running after another man while brandishing a butcher knife. This officer, Redmond, then sought psychological counseling.
9. What is hopefully clear in this case is that we have a balancing problem. We want police officers to seek psychological help when they need it, and they are likely to need it after a shooting. In general, we want all sorts of people to be able to freely seek that kind of help, and for them to feel that they can be entirely honest with such counselors. You can easily imagine even a fully justified officer Redmond having doubts and wanting to confess them to a therapist. If people know their therapists can be hauled into court, however, then it is much harder for them to be honest in therapy, and therapy will be much less effective. So on one end of the scale we have the societal interest in letting people get the kinds of help they need.
10. On the other end of the scale is the desire for justice. Redmond was sued by the estate of the man she shot. Witnesses to the shooting, including members of the deceased man's family, claimed that the shooting was unnecessary. Their search for justice is hindered if we grant privacy protections to Redmond's conversations with her therapist. As is so often the case, we have a tradeoff between privacy and justice.
11. What I want you to take away from these cases is that, in the medical context, we balance between privacy and justice in favor of privacy. For psychotherapist testimony and notes, almost every state and the federal government recognize an evidentiary privilege. For doctor testimony and notes, most states recognize an evidentiary privilege – subject to a large number of exceptions, particularly

In the criminal context – but the federal government does not. In contrast, the duty of confidentiality is more or less universal.

12. Now that brings us to the Tarasoff case. Here we have a different balancing act. While in therapy, a very disturbed man named Poddar made threats against an identifiable potential victim. The therapist was so disturbed by these threats that he actually notified the campus police so that Poddar could be civilly committed, but for various reasons this did not happen and no further action was taken. Poddar went on to kill his victim.
13. Again we have the privacy interest in therapy. But now it is being weighed against a threat of imminent harm to identifiable third parties, namely Tatiana Tarasoff. The court strikes the balance now in favor of safety. Note the tension here. Redmond was also possibly a danger to other people, and her privacy was protected. What makes Tarasoff's case different is that Poddar was an imminent threat. Dr. Moore was quite possibly the last line of defense. This should remind you somewhat of the Lawson case.
14. This is the “danger to self or others” exemption that some therapists mention when promising confidentiality to a client. By last count, 23 states had adopted a Tarasoff style duty to warn by statute, and almost all of the rest either had established the duty though the common law or explicitly allowed counselors to breach confidentiality in such cases.
15. Nevertheless, it may comfort some of you to know that Tarasoff claims are rare and Tarasoff liability is even more rare. One problem with these cases is well-illustrated by Tarasoff itself: only Moore's initial attempt to protect Tarasoff established the extent to which he was concerned for her. It is really hard to establish that a therapist knew someone was a threat, and many therapists admit that it is hard for them to tell.
16. Despite liability being rare, this case has had a real impact on clinical education. Though data on this is imperfect, it appears that the duty to warn is covered in almost all psychiatric residencies, for instance. This does not mean that the duty is understood, but it is at least known.
17. To sum up, future, imminent, harm trumps privacy in therapy, which in turn trumps finding truth at trial. And, in medical privacy if in few other places, you can bring a lawsuit for breach of confidentiality. Thank you.

Week 4 Video 2 – HIPAA's Key Features

1. HIPAA: the Health Insurance Portability and Accountability Act. It is a misdefined and frankly often misspelled acronym. Prior to HIPAA's enactment, a patchwork of state regulations governed health privacy. HIPAA

was an effort to create a federal baseline for privacy protections. States can and do exceed that baseline.

2. The name gives a hint to its purpose. HIPAA was enacted at a time when electronic record keeping and standardized treatment and diagnosis codes were becoming common. This created a new problem: it was now possible for the records of hundreds or thousands of patients to be stolen from a medical provider and then understood by others. HIPAA was an attempt to protect patient privacy while still allowing for the great efficiencies of electronic storage and uniform coding.
3. The principal limitations of HIPAA go to the kinds of entities covered and the broad focus on potentially uninformed consent.
4. HIPAA (more or less) only applies to entities that file insurance or Medicare/Medicaid claims using HIPAA's "standard format." This basically means that if you take insurance, HIPAA covers you. If you don't, it very likely doesn't. Obviously doctors and insurance companies contract with a large number of third parties – billing companies and the like. HIPAA covers them too, and there are rules for how those contracts need to be written to ensure that privacy is still protected as healthcare providers share information with these third parties.
5. Right now, though, a ton of medical data is being generated and analyzed by those outside the scope of HIPAA. The information collected by, or submitted by you to, your various health tracking apps is not covered. Believe it or not, Apple is not an insurance-accepting medical provider, nor is the bar that wants to see your vaccine card. Now if your doctor's office has its own app, that's different. But the random diet and exercise tracking, heart rate monitoring, and sleep quality assessing apps are not. State laws are beginning to fill that gap, but they are not there yet.
6. HIPAA applies to individually identifiable health information, which it calls Protected Health Information or PHI. This term is defined broadly and the primary thing to understand about it is that it does not apply to deidentified data. If health data from a covered entity can be linked to a person, HIPAA covers it. If the data can no longer be linked to a person, HIPAA does not.
7. HIPAA requires that covered entities minimize when sharing information. So if a covered entity needs to share some of your information with a vendor, perhaps for billing purposes, they are not supposed to send your entire file over to them unless they actually need it. But HIPAA does permit doctors to share your entire file with each other as they work to treat you; that's an exception in the regulation.
8. HIPAA also requires that doctors accommodate communication preferences. This still causes major problems sometimes because disorganized doctor's offices make mistakes. If a patient requests that a doctor not leave messages on

their answering machine, or mail physical records to their home address, however, HIPAA requires the doctor's office respect that.

9. This brings us to another major point under HIPAA: Consent. Given patient consent, medical records can be shared. This is vastly empowering - your records go where you want and nowhere else. But people don't generally read the HIPAA disclosures they are handed. This leads to the problem of uninformed consent - people don't know what they're agreeing to. And even if you read a HIPAA disclosure, it may not make much sense to you. I've not personally seen this abused, but it is a lurking possibility
 10. HIPAA isn't quite as draconian as it is made out to be, however. Doctors can give you your own medical records. In fact, many states require them to do so. Doctors are allowed to send appointment reminder postcards, unless you ask them not to. And doctors can share information with your family members or let them pick up your prescriptions – to the extent that their professional judgement thinks is wise and provided that you haven't told them not to. It all comes back to consent. Many doctors now have forms asking you whether you want your spouse, parents, or children to be able to access your records. That takes a lot of the guesswork out of it.
 11. HIPAA also allows for a variety of disclosures even without consent. Health data can be shared with law enforcement under certain conditions, with public health authorities, to prevent imminent threats to health and safety, and in a variety of other circumstances. The thing to understand about HIPAA is that it works. HIPAA very rarely requires something entirely dumb or senseless.
 12. Private individuals cannot sue under HIPAA – we will discuss how government agencies can sue next time. But individuals can sue for negligence or breach of confidentiality and cite HIPAA to show how a medical provider should have protected their information. You see an example of this in the Shepherd case, where a pharmacist released prescription information to a patient's estranged wife. That was an arguably nonconsensual disclosure – the patient only wanted his wife to know about one prescription, and didn't want the other prescription at all. So this is potentially a violation of HIPAA and therefore also a violation of state law, and we see more cases like this each year. Notably Arizona law still protected the pharmacist from a private lawsuit provide the pharmacist's mistake was made in good-faith, and that was left to a lower court to sort out.
 13. Next time we will see how the government goes about enforcing HIPAA itself.
- Thank you.

Week 4 Video 3 – HIPAA Enforcement

1. Hello again. This video addresses the civil and criminal enforcement mechanisms under HIPAA. I've talked about the rights you have under HIPAA. Now we see what can be done to enforce them.
2. The central features of HIPAA enforcement are the lack of a private right of action and the lack of statutory damages. You cannot sue under HIPAA. That is very important. You can file a complaint with an administrative agency, and doctors take that sort of complaint very seriously, but you can't go file your own lawsuit under HIPAA.
3. The Department of Health and Human Services, however, *can* punish doctors and hospitals for merely technical HIPAA violations. Originally HHS took more of an educational role – there were very few fines pre-2008. But enforcement grew more teeth during the Obama years. The actions mentioned in your book are representative.
4. HIPAA enforcement actions are targeted at breaches of one of the three HIPAA rules. The privacy rule we discussed last time. There is also the security rule, which mandates extra protections for protected health information that is stored electronically, or e-PHI. Specifically, the security rule mandates technical safeguards to protect against hacks and workforce training to prevent employees from misusing their access to health data.
5. Finally, there is the data breach rule. A breach is defined as unauthorized “acquisition, access, use, or disclosure” of unsecured Protected Health Information. Note the word “unsecured.” That basically means unencrypted in this context. Affected individuals have to be notified “without delay,” meaning at least within 60 days. Further, the breach has to be reported to HHS if it affects over 500 people. HHS maintains a Wall of Shame for these.
6. Data breaches are a common source of HHS enforcement actions. Consider the Premiera Blue Cross case. There a hack exposed the PHI of 10 million people. From a HIPAA standpoint, the main concern is how the hack happened. How many security failures were required for this kind of breach to occur? Why were employees falling for phishing emails? Why was malware about to run undetected for months? From a technical standpoint, what do you need to do to prevent this from happening again?
7. Premiera gets fined 6.85 million dollars, but HHS's main interest is in preventing future breaches and creating a training and information security program to deal with issues going forward.
8. Take as a contrast the Yakima Valley case. There, security guards at the hospital have access to patient files and intentionally access the files of 419 patients. They are not supposed to do this. Consider the minimum necessary standard – hospital

- security guards don't need patient health information to do their jobs except in very rare circumstances.
9. Were you to file an individual lawsuit over the Yakima Valley case, you would have trouble. There is no allegation here that individuals were in any way harmed or humiliated by their files being shared with security. But this is still a major failure of training and of system access rights. Security guards shouldn't be able to access that information and, being able to do so, should know not to. Hence HHS's interest.
 10. There have been a lot of enforcement actions stemming from data breaches and far fewer that look like Yakima Valley. Though there was one from UCLA hospital where staff were looking up the records of celebrities – which, if they are not treating the celebrities, they are not supposed to do.
 11. In each case, we have 6 or 7 figure fines and 1 year corrective action plans. Most HIPAA enforcement actions that lead to monetary damages are related to failures of supervision and control, employees that are not adequately trained or supervised. HHS appears to be looking for policy-level problems rather than accidents.
 12. One very very important point, however. Between 2018 and 2021, HHS received tens of thousands of complaints under HIPAA, but found many were not even eligible for investigation, provided technical assistance to help the accused party comply with HIPAA in most of the remaining cases, and only imposed corrective action of any kind in 2.8% of the time. And that corrective action generally took the form of something like mandatory training. There were only 53 monetary settlements under HIPAA in those years.
 13. This is one model of enforcement. Fine the worst actors, require the rest to clean up their acts, and offer advice to anyone who needs it. Is that enough? What would you want to know to figure that out? Is the option of suing doctors for breach of confidentiality enough to fill the gaps?
 14. HIPAA also has a criminal provision. “A person who knowingly and in violation of [HIPAA] (1) uses or causes to be used a unique health identifier; (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person, shall be punished... .” So if, in violation of HIPAA, you knowingly obtain or disclose protected health information that is maintained by a covered entity, you can be prosecuted.
 15. As far as we know, “knowingly” applies only to knowing that it is protected health information and not to knowing that the disclosure was illegal. That's the *Zhou (joe)* case, where a fired employee kept accessing patient data. So you can't be convicted for picking up a folder that you didn't know contained health records, but you could be prosecuted even if you don't know the law.

16. Importantly there does not appear to be any reason why non-HIPAA covered people cannot be held criminally liable for taking and distributing protected health information, though I've never heard of it happening. The Department of Justice has never brought that kind of case.
17. HIPAA is an example of an agency-led privacy statute. Individuals enforce HIPAA primarily by complaining to the agency, and the agency determines whether to take a punitive approach, large fines and intrusive monitoring, or a training and advising approach. This leads to less enforcement, and more prioritization, than a system of private lawsuits. But it also prevents absurdities, as doctors and hospitals are not being repeatedly fined over trivial violations. Thank you.

Week 4 Video 4 – Genetic Privacy

1. We are moving on to another key issue in medical privacy – privacy in genetic information. What I really like about this topic is the way it forces us to think about how and why we value privacy. Is it to stop the government from using our genetic traces to identify us? To prevent companies from discriminating against us in insurance pricing and employment? To avoid having specific embarrassing information about us revealed to the public? Or to just generally keep other people from knowing about our business?
2. Odds are, you feel more strongly about protecting genetic privacy in some contexts than you do in others. For example, I wouldn't mind if the police wanted to check whether my DNA matched that in the blood at a murder scene. I would mind if my employer got a copy of my genetic profile. For one thing, even I don't have a copy of that and I'd feel very weird about my employer knowing more about me than I do.
3. Broadly speaking, there are two domains where you get genetic privacy questions: prediction and identification. Let's start with identification, which is mainly a criminal procedure topic.
4. The issue here is largely one of DNA databases and index systems. The big one is run by the FBI and called CODIS: Combined DNA Index System. CODIS only contains DNA codes of a limited number of core loci, 20 as of 2017. These codes are nonfunctional, as far as we know, so you can't predict personality or health from them.
5. CODIS has a unique focus. It contains DNA samples from criminal suspects and crime scene evidence. They don't have a database of everyone.
6. Under current doctrine, there is no problem with gathering DNA identification information from arrestees or parolees. The basic rationale is that the collection of DNA is more or less painless, usually a cheek swab or a prick of the finger.

Though arrestees are still presumed innocent, we allow them to be fingerprinted and photographed, and the Supreme Court views the taking of a DNA sample as little different than those. This leads to a national DNA database of people who have been arrested for, or convicted of, many crimes.

7. Is this a problem? Well, quite possibly not. If you could wave a magic wand and ID every rape kit in America, would that really be so bad? And the limitations on CODIS, its restriction to 20 non-functioning loci in particular, are reassuring. Some people refer to DNA as containing your “future diary” because from your DNA one can predict later health. But the DNA in CODIS, as far as we know, doesn’t run that risk. There just isn’t enough information there about each sample.
8. On the other hand, one has to wonder if such a database can be as limited, and as secure, as we would want it to be. We probably don’t mind more efficient identification of evidence left behind at a murder scene – we do generally cheer for the cops when we watch CSI. But maybe this doesn’t stop there. Part of the reason that the government has been allowed to build this database is that it is hard to articulate the harm. But, because of the power of DNA in the predictive realm, there is still a lurking fear.
9. Going forward, there is also the issue of private DNA databases. The man suspected of being the Golden State Killer was arrested not due to a hit in CODIS, but instead when DNA evidence was uploaded to the private site GEDmatch. This site codes for far more than the 20 loci of CODIS. Though no one on the site matched the sample that investigators believed was from the killer, they could identify 10-20 people who were likely distant relatives of the killer. From there investigators were able to finger Joseph James DeAngelo is the most likely suspect. They then collected what is called “abandoned” DNA; they swiped the door handle of a car that he’d been driving to get a sample. That sample was a positive match.
10. Pivoting to private databases that encode lots of genetic information, let’s talk about genetic prediction. As we get better at understanding genetic markers, it will become possible to predict a person’s personality, capacities, and health prospects from their genetic information. How well will be able to do this? That’s very hard to say. We can currently predict some severe genetic disorders quite well, however.
11. The classic example discussed in this context is Huntington’s disease. Huntington’s is a degenerative disorder that manifests mid-life, generally when the person is between 30 and 50. It is incapacitating, necessitating expensive care, and drastically lowers life expectancy. It is also highly heritable – the child of someone with Huntington’s has a 50% chance of having it themselves.
12. If you are an insurance company, an employer, a spouse, or even a friend, you’d have good reason to want to know if someone was highly likely to go into

degenerative decline at an early age. So some have argued that it would be immoral for a person with the marker for Huntington's to conceal that information from a potential spouse or employer. This is the traditional social fraud argument. You present yourself as the kind of person with a normal life expectancy when, in actuality, you know better.

13. Think in terms of Huntington's and in terms of a spouse. That's probably the context where the privacy skeptics are most right. It's like the classic case of concealing one's infertility from a partner who wants to have children. But this argument starts weakening when we move from spouse to employer, and weakens still more when we go from a certainty of something drastic like Huntington's to a probability of something less debilitating. Should a potential employer know about an increased susceptibility to substance abuse? How about generalized thrill-seeking? Or, conversely, a propensity toward friendliness?
14. So what we have here is a privacy tradeoff. If employers and insurers can consider genetic information, they'll be moderately better able to assess risk. But this comes at a cost to privacy and to equity.
15. We tend to not like classifying people based on how they're born. We want to say that what matters is what you've made of yourself, and genetic discrimination flies in the face of that. This is particularly true as we move from the Big Diseases to the smaller traits, the Gattaca sort of model. We want to think of people being able to better themselves, not being forever judged based on an unchosen and immutable characteristic.
16. There is also a justified skepticism of sorting people based on genetics. There is a risk of bad science here, as genetic analysis involves a lot of fundamentally correlational data. For complex predictions – intelligence, aggression, conscientiousness – it's going to be really hard to disentangle causality. We don't want another round of racist pseudo-science.
17. So the law has stepped in. As of 2008 we have GINA: the Genetic Information Nondiscrimination Act. Insurers can't take genetic propensities into account when deciding who to offer health coverage to or what rates to set, and employers can't consider them when deciding who to hire or fire. Also the Affordable Care Act completely transformed how health insurance is priced and treats preexisting conditions, so don't forget about that. Life insurance pricing isn't covered under GINA, but health insurance is.
18. GINA has two basic requirements. First, employers and insurers can't require you undergo genetic testing. Second, even if employers or health insurance companies do get access to your testing results – say you post about them on Facebook – they still can't discriminate against you based on them.

19. Many states have laws that provide even more protection than GINA. As with HIPAA, GINA establishes a federal baseline of privacy protection, but states are free to exceed it.
20. Both genetic identification and genetic prediction can sound like the stuff of science fiction, but cases like the Golden State Killer show us that our ability to analyze and sort genetic data has advanced drastically over the past several decades. It is both exciting and scary to think where this area will go next.
Thank you.

Week 5 Video 1 – Data Brokers and Financial Privacy

1. Data brokers are key to understanding commercial privacy in America. When people interact with companies, they generate tons of data trails. Some of these trails are obvious – this person buys really expensive handbags, so we should try to sell her more of them. But some are more subtle. Imagine a woman has switched to buying unscented hand lotion, and has started purchasing vitamin supplements like calcium, magnesium, and zinc. If you're a big box store like Target or Wal-Mart, you would see this pattern and you might predict that the woman has entered her second trimester of pregnancy.
2. People get creeped out by this kind of prediction. In 2012, there was a famous series of articles that depicted a father going into Target to complain about the maternity catalogues his teenage daughter was getting – what were they thinking, sending these ads to a high school student? The story ends with the father, on a follow-up call with the manager of the Target, apologizing. In the intervening time he had learned that his daughter was due that August.
3. The problem here is that all the information given to stores like Target is fundamentally public. It isn't some kind of secret that you walked into a store, picked an item off the shelf, and then paid for it at the counter. And, with a customer loyalty program, they can easily link that single purchase to your broader profile. If you're like me and shop on Amazon, then you deal with a store that has your name, address, email, purchase history going back to 2001, and, importantly, a record of every product that you've ever looked at and not bought. It's an incredible wealth of information.
4. The Dwyer v. American Express case is almost quaint by comparison. The cardholders sue American Express for sharing information about them with third parties. American Express is classifying the cardholders based on their buying habits into groups such Rodeo Drive Chic (Shēk) or Value Oriented, and then sells lists of customers who fit particular profiles to merchants. They also offer to put together lists of customers interested in certain types of products, such as fine jewelry.

5. The cardholders are alleging intrusion upon seclusion. Their problem, in the eyes of the court, is that the information is not particularly private. The cardholders know they have shared the information with American Express so they are taking the risk that American Express will share the information further. The court points out that magazine subscription lists can also be sold under state law, for similar reasons.
6. From the perspective of sensitivity, it seems like the fact that someone reads a magazine can be very intimate – it might raise significant inferences about their political or religious beliefs or their sexual practices. And arguably what’s happening in Dwyer is even worse. People can avoid subscribing to magazines easily enough, but it is very hard to opt out of credit cards, and purchase records reveal a ton of information.
7. Fundamentally, though, your credit card company and your big box retailer are not your doctor. They have no duty of confidentiality toward you, and can do as they like with the information you so willingly give them.
8. Now you might be saying “but wait, don’t banks have privacy regulations?” They do, but those are not as helpful as you might think. Look at the Gramm Leach Bliley Act. It applies to nonpublic personal information held by financial institutions. It requires the institutions to have strong data security, circulate an annual privacy notice, and not disclose certain information in their advertisements to you – they cannot pre-fill in your social security number, for instance.
9. But none of that protects you from the kind of data-sharing that happened in Dwyer, which incidentally predates the GLBA anyway. Financial institutions can always share your information with their affiliated companies, so mortgage lending, credit cards, investing, and retirement planning can all compare notes.
10. Financial institutions can even share your information with nonaffiliate companies – which is anyone and everyone else – so long as they give people a chance to opt out. But this chance is generally buried in the annual privacy notice and virtually no one actually does opt-out; only about half a percent. Many people don’t even recall getting the annual notice, which makes sense because there is very little to be gained by trying to read page after page of barely-comprehensible text.
11. GLBA looks like HIPAA’s sickly cousin. It has many of the same features – agency enforcement, a focus on consent, a concern with data security – but it differs in that it leaves the door wide open for advertising uses. The statute isn’t useless – it makes banks think about privacy – but it is far from a remedy for that data broker problem.
12. Going forward, think about whether the kind of data broker enabled targeted advertising I’ve been discussing bothers you. If it does, why does it?

States have been moving to pass privacy laws that would address these issues very directly, and we're likely to see some movement here over the next five years.

Week 5 Video 2 –The Fair Credit Reporting Act

1. The Fair Credit Reporting Act, the FCRA, is one of the least sexy but most important laws in the privacy domain. You can basically divide all information brokering into two domains. In one domain, almost any truthful information can be collated and sold – absent specific laws, anything goes. In the other domain, everything is tightly regulated at the federal level by the FCRA.
2. Spokeo is the best example of a company that inadvertently ended up in the tightly regulated domain. The FCRA had long been applied to the traditional credit reporting agencies, Experian, Equifax, and Transunion. Spokeo thought that it wasn't in the same universe as those companies. It was wrong.
3. At the time, Spokeo was a bay area startup that collated information about people's hobbies, ethnicity, religion, participation in social networking sites, financial situation, photos, etc. In short, everything it could get its hands on. Looking for potential buyers for this mass of information, Spokeo marketed itself to private companies as a way of vetting new hires.
4. This is what attracts the attention of the Federal Trade Commission and generates this complaint. The FCRA defines "consumer reporting agency" as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties."
5. So you're a consumer reporting agency if you produce "consumer reports" for money.
6. A consumer report is any communication from a consumer reporting agency that has "bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" – note that is an incredibly broad list – and is used in whole or in part for A.) credit or insurance, B.) employment purposes, or C.) any of a short list of other things that are a lot like credit, insurance, and employment. Rental decisions are probably the biggest.
7. If you decode all of that legalese, it means that if you're in the business of collating or analyzing personal data and that data is going to be used for credit, insurance, or employment, you're regulated by the FCRA. If your data is going to be using it for anything else – marketing, politics, personal amusement, whatever, then you're not.

8. Ever searched for someone's name online and gotten hits on those people search websites? If you click through to buy someone's report, there is – in my experience – always a screen that asks you to affirm that you are NOT using the information for any of the FCRA purposes.
9. So, why is being under the FCRA such a big deal? It carries with it a ton of obligations. Some of these obligations are procedural, and some are substantive. Consumer Reporting Agencies:
 - a. Need to “maintain reasonable procedures to limit the furnishing of consumer reports for enumerated ‘permissible purposes.’”
 - b. Must implement “**reasonable** procedures to assure **maximum possible accuracy** of the information concerning the individual about whom the report relates.”
 - c. Must provide a user notice to anyone to whom it provides a credit report.
 - d. And, are barred from giving consumer reports to “persons that it did not have reason to believe had a permissible purpose to obtain a consumer report.”
10. These requirements go to a couple of underlying goals. One is to ensure the accuracy of the reports. The agencies need to take some steps to monitor the accuracy of their records, and companies that commission reports have to notify the people the reports are about – potential employees, potential renters, etc – when they take what is called an “adverse action” as a result of a credit report. The idea is that this gives the consumer or employee a chance to check the accuracy of the report and complain if it is wrong. This is all contained in the “user notice” that agencies are supposed to give companies that buy the reports.
11. Some of the other requirements are to stop people from buying all this sensitive information just to be nosey. This leads to one of the oddities of the FCRA. If you have a data aggregator that exists to market to nosey people, you're not covered by the FCRA. But if you assemble your data for employment, insurance, etc, then you can't sell to the merely nosey. The idea is that a “nosey people” version of people search will have a lot less information than one aimed at employment and insurance.
12. There are also a few other substantive requirements. Old bankruptcies and arrests (but not convictions) drop off consumer reports except when those reports are for high value jobs and loans. So if you're a consumer reporting agencies you have to remember to not include those. Google, obviously, can keep listing them.
13. Very importantly, both people and the government can sue you if you violate the FCRA, and for meaningful amounts of money. This comes up quite a lot.

14. Spokeo's problem with the Federal Trade Commission was basically that they didn't realize they fell under the FCRA. So they weren't doing, well, most of the things they were supposed to. Once this was brought to their attention, they changed the terms of their web site to clarify that consumers cannot use the site for FCRA-covered purposes. They did not revoke the access of consumers who had previously signed up, however, which concerned the FTC given that a huge proportion of Spokeo's user base at that point had joined the site through Spokeo.com/HR.
15. So how is Old-Spokeo different than Google? Well, first, a Consumer Reporting Agency's information is generally assumed to be correct and about the person whose name and social security number are at the top of the page. That faith can cause a lot of harm if it is misplaced. If you Google me, you also see results for a voiceover artist and a bunch of other people. If you search for me on Transunion, you don't. The consumer reporting agencies also have a ton more information about me than is readily available on Google.
16. These non-FCRA people search engines are another story. They have access to a lot of the information that Consumer Reporting Agencies do, but they explicitly disclaim the FCRA's purposes. Right now, they can walk that line. Whether that is still going to be possible in 10 years is another question.
17. You also might be wondering how strict those "reasonable procedures" (note the weak language) to ensure "maximum possible accuracy" must be. The answer is that they can be pretty weak. Consumer reporting agencies are required to respond to reports of errors and to not misrepresent the data that their various sources give them. But they have no affirmative obligation to go through their endless reams of data to make sure it is correct. This is really a self-help system, and sometimes people suffer real harm before they are able to help themselves.
18. For now, though, I want you to keep in mind the two domains of data brokerage. If the data is for marketing, America has fairly few regulations. If for employment, insurance, or tenancy, however, we have the FCRA. Thank you.

Week 5 Video 3 – Data Breach Notification and Litigation

1. Data breaches consume an incredible amount of attention in privacy law. Here, I want to talk about two basic issues: Data breach notification and private data breach litigation
2. To start, notification. Data breach notification is governed by state law, so there are 50 different possible standards for each company track (or more if one counts territories). But two facts help simplify this problem. First, any data

breach affecting a national company will very likely implicate the laws of every state, so it doesn't matter as much if one state has weaker standards – the company is stuck dealing with the more protective states anyway. Second, the laws tend to only vary in a few different ways, so it's not that hard to group them by category.

3. At this point, every state has a law about data breach. The last two states – Alabama and South Dakota – passed theirs in 2018. In general, these laws require that people be promptly notified if their data is exposed in a data breach. The companies must also say what data they believe was exposed and a bit about how the company is dealing with the situation. One difference across states is whether companies must notify people whenever personal data is improperly obtained, or whether the company can refrain from giving notice if there isn't a reason to think the data will be misused. Most states require notice whenever personal information is obtained by an unauthorized person, but some states do not.
4. In a minority of states, but including many of the largest, the State Attorney General or another state agency must be notified when breaches occur, which is part of why we have decent statistics in this area.
5. Very few states explicitly grant a private right of action that allows consumers to sue for failure to provide notice, but a number of others allow suits under the common law, or under a general “unfair business practices” style tort. More on that later.
6. California has been a leader in this area, so let's look at its data breach law. Notifications have to be sent if unencrypted personal data is released. Personal data in this context is defined as several specific pieces of information, or combinations of pieces of information. The California list is actually broader than that of some other states. It includes biometrics and health data, which are sometimes omitted elsewhere.
7. A breach is defined as the unauthorized acquisition of personal data, without any need to consider whether there is a probability of misuse.
8. Notification must be prompt, but can be delayed at the request of law enforcement. And the state attorney general must be notified of large breaches.
9. Notification must also have certain elements. California even includes specific headings the notification must include.
10. Companies are required to guard against data breach, though the standard they're held to is vague. And there is a private right of action – important to national firms given the millions of consumers in California – but no statutory damages.
11. Consider the impact of this statute and the many like it. Once a company has realized it was breached, it must investigate the breach to determine what information was exposed. It then needs to compare the list of exposed

information to the laws of each state whose residents were affected to see whether notification is required in that state. If notification is required, it has to consider exactly how that notification must be given. This all consumes an incredibly amount of resources and, importantly, happens even if the data breach is not the company's fault.

12. With all of that in mind, let's turn to data breach litigation. Most data breach litigation is not about notification; it is about the breach itself. Think about why this is. A notification statute only requires that people be told after a breach occurred. A delay in notification could hurt people, but generally not all that much compared to the fact of the breach itself. So plaintiffs devote much more energy to establishing that the breach was caused by misconduct than that notice was inappropriately delayed.
13. Let's think about the kinds of harm that people might suffer from a data breach. I group these into five categories: emotional distress – the people are upset and afraid. Increased risk of future identity theft. Liability for charges from ID theft. Precautions to reduce the risk of ID theft – so spending money on credit monitoring. And sorting out costs, all those phone calls you have to make.
14. Set aside emotional distress for a moment. Identity theft is relatively rare even in data breaches. In breaches of thousands or millions of people, only a very small fraction will actually have their identities stolen. Of those who suffer identity theft, most of that will simply be fraudulent use of an existing credit card, and most credit card companies will refund consumers for fraudulent charges. At the end of the day, almost everyone whose credit card number is improperly acquired will have the same mundane experience of calling their credit card company, making a report that the number has been compromised, and then getting a new card in the mail a few days later.
15. You could say that, even though the harm to you from identity theft is likely to be very low, it still makes sense to get identity theft monitoring of some sort. And it very well might. This is why companies often provide that for free after bad breaches. It is good PR, and also something that you can't sue them for because you're already being given it.
16. Now, if you've talked to enough people about these issues you'll know that sometimes it isn't quite this neat. Sometimes the time it takes to sort out identity theft imperils the purchase of a home. Sometimes it takes years for things to return to normal. But that isn't the common experience, and many times those people aren't the named plaintiffs in data breach cases.
17. Look at the Tsao case as an example. Here we have a breach. The plaintiff's information was exposed and, in theory, he could have suffered identity theft. But he didn't. In fact, the lawyers representing him and the other people whose

data was exposed in the breach cannot find anyone who has yet suffered identity theft as a result.

18. Tsao tries to get around this with a list of harms he did suffer, but all of these are abstract, distant, or small. So Tsao isn't being allowed to bring his suit, even if the company is at fault.
19. Tsao is part of a line of cases that dismiss some data breach lawsuits on standing grounds. To have standing is a legal requirement to be in federal court. Under Article III of the constitution, those bringing cases in federal court must show that they have suffered a harm that is concrete (meaning real and not hypothetical) and particularized (meaning about them and not about society at large). Future harms can count, but only if the harms are sufficiently imminent. Most courts have said that there is only standing when at least some people have suffered identity theft. That both is a harm itself as well as a reason to believe that future identity theft is imminent for others.
20. This brings us to Equifax. There is a ton going on in this case, and it is worthy of a close read. Two points I want to highlight for you. First, this is a massive breach that caused real harm to millions of people. So we don't have an obvious Tsao problem.
21. Second, the plaintiffs in this case sued under a bewildering array of legal causes of action. Some of these applied nationwide – for instance, there was an FCRA claim in there – but many were restricted to the residents of a single state. Imagine the sheer amount of research that both sides needed to conduct for this case. So many states, so many people.
22. We often therefore have two kinds of data breach cases. Some are like Equifax – obvious harm, and a flood of mostly-successful litigation. Others are like Tsao – potential harm, but hard to pin down and hard to sue about.
23. That's often the problem in data breach cases. Even when someone is getting hurt, it can be hard to find them. Not everyone whose credit card number was stolen is going to be affected in the same way, or even at all. But someone is out money for all those fraudulent charges. Hackers are generally not stealing this data for the fun of it; they intend to make money.
24. Second, not all data breaches are the same. Sometimes a data breach is likely to lead to fraud, at least for some people. Sometimes, a data breach pretty clearly hasn't led to fraud. It may make sense to treat these cases differently.
25. Third, there is a real problem of causality when you think about how many data breaches occur. My credit card number was stolen around 2012. I have no idea where it was stolen from. Presumably there was an unreported data breach. Other times, people receive multiple data breach notifications in the same year. In a lot of cases, it can be hard to establish whether identity theft is traceable to this data breach or that data breach. That makes it even harder to bring these lawsuits.

26. What we would really like is for companies to not get breached in the first place. To mandate that they have good data security and enforce that requirement. And this kind of post-hoc litigation can only do so much to bring that about. Thank you.

Week 6 Video 1 – The Federal Trade Commission As Privacy Enforcer

14. The Federal Trade Commission is the most important regulator in American privacy law. Private lawsuits are powerful in some contexts, but they fail in others. There are many reasons for this, but the biggest one is often that the harm of a consumer privacy invasion is spread across a large population of people. A company might improperly exploit the personal information of thousands of people, but leave none of them measurably worse off at the individual level. Or a hacker might breach a company's security, inflicting millions of dollars of harm on the economy, but again not leaving obvious wounds on particular people.
15. Enter the Federal Trade Commission. Section 5 of the Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce." This is incredibly broad. The language stands in sharp contrast to the nitty gritty we've seen in other statutes, like HIPAA and the Wiretap Act. I sometimes describe it as the FTC's mandate to go forth and do good. The FTC can act on behalf of consumers as a whole, without needing to rely on single individuals to file lawsuits.
16. Some sectors of the economy are explicitly exempted from FTC authority under Section 6 – nonprofits, airlines, telecoms, many financial institutions – but usually because they're being extensively regulated elsewhere. The mainline of corporate America, however, is firmly within the FTC's sphere of influence. Importantly for our purposes, the Googles and Facebooks of the world are covered.
17. Individual people can't sue under the FTC Act, only the agency itself can. That means that we don't see a flood of litigation. The agency picks and chooses its cases, generally going after the worst offenders and the best examples.
18. The biggest line of FTC privacy work involves the deceptive practices part of its authority. A deceptive act or practice is:
- a. a material representation, omission or practice that is likely to mislead the consumer
 - b. When the consumer is acting reasonably in the circumstances,
 - c. to the consumer's detriment.

19. The FTC looks for deceptive acts in corporate privacy statements and public declarations of corporate policy. Take a look at the 2019 Facebook case, and by extension the earlier one as well. Each of these involves Facebook misrepresenting the extent to which apps – particularly apps installed by your friends - could see your data. These are representations that Facebook chose to make. It isn't that it was inherently wrong for Facebook to take the data you share with your friends and to also share it with your friends' apps. It is that Facebook claimed – in so many ways – that it wouldn't do that.
20. This isn't quite like a breach of contract case. Press releases and public statements don't generally create new contractual terms. But they can easily mislead consumers, and that is what we are concerned with here.
21. Up until 2020 or so, pretty much every FTC privacy enforcement action looked the same. A company promises to either not collect information or, having collected it, to not further share it. The company then does the thing it promises not to do. The FTC then intervenes. This is a self-regulation model. Through their privacy policies, companies set the standards to which they will be held. The FTC is just forcing them to keep their word.
22. This raises a key question: What's the point of holding a company to its privacy policies when, as we all know, people don't read them? There are many possible answers and most revolve around transparency. When it matters, so this argument goes, someone actually does read the policy. And then they write an article about it, and then someone reads the article and writes another article. And then it hits the New York Times and CNN. And so the public is informed. But, in a garbage in->garbage out fashion, the privacy policy needs to be accurate otherwise even this limited system doesn't work.
23. Another framing is that this is literally the least you can ask a company to do: whatever you do with consumer data, at least don't lie about it. When you think about discussions around Uber, there is definitely concern about the creepiness factor in location tracking. When Uber promises to be better with user data, we want that to mean something. The FTC can make sure it does.
24. Look at this from the perspective of private lawsuits. In so many cases the harm in question is remote and diffuse. People are hurt – they might not have used these products if they knew what data would really be collected – but it is hard to put a dollar value on it. And it is hard to hire a lawyer when you can't put a dollar value on your harm. But the FTC has different incentives. It can sue, using government resources, to make a company stop and to send a message to an industry that it needs to do better.
25. More recently, the FTC has leaned into the other portion of its authority, the banning of unfair acts. Some corporate privacy practices hurt consumers so much that the FTC will sue over them even absent obvious consumer deception. We are still figuring out how far the FTC is going to push this point.

In general, however, the FTC is very concerned with medical data, biometric data, and location data.

26. Each of those kinds of data implicates core aspects of privacy. Facial recognition has the potential of abolishing privacy in public spaces. Medical data gets at basic human needs, and much of it is outside the scope of HIPAA and the duty of confidentiality. Location data tells a person where to find you, making it easy for them to do you harm. But complex networks of companies, apps, and data brokers have moved into each of these spaces, and privacy activists need to play catch up if they want to impose meaningful regulations.
27. I want to close by talking about the terms of the settlements in these cases. In initial actions, they're always about the same. The biggest term is that the companies agree to 20 years of monitoring by the FTC and pledge to avoid further violations of the FTC Act. Even with the small number of FTC actions in a given year – and it is a very small number, like 10 - this means that the FTC is watching pretty much every major tech company at this point. And the FTC can fine companies for violating prior consent decrees - meaning for being repeat offenders. That's why Facebook got hit with a 5 billion dollar fine in 2019.
28. These 20 year monitoring terms are long and annoying by any standard. Recall the short 1 year monitoring terms that are common in the HIPAA context. That's why big companies pay so much attention to what the FTC does. And, as we'll see, the FTC is active in data breach in a similar fashion. Thank you.

Week 6 Video 2 – Children's Privacy and COPPA

1. Society is perpetually concerned with the protection of children. Sometimes this concern is well-placed and sometimes it is misdirected, but it is almost always there. So we shouldn't be surprised that both states and the federal government have taken steps to protect children online. State efforts have sometimes been very bold and have run into a lot of constitutional challenges. By contrast, the federal Children's Online Privacy Protection Act, or COPPA, has been in operation for over 20 years. So let's look at it.
2. COPPA applies to websites and online services that either are child directed or have actual knowledge they are collecting data from children. Those services need verified parental consent before collecting children's personal information. And personal information is defined very broadly and includes, for instance, a lot of basic web tracking indicators.
3. Think about the kinds of websites that are and are not covered by this. The Washington Post website is not directed at children. Children certainly do visit it, but the Washington Post has no way of knowing who is and is not a child.

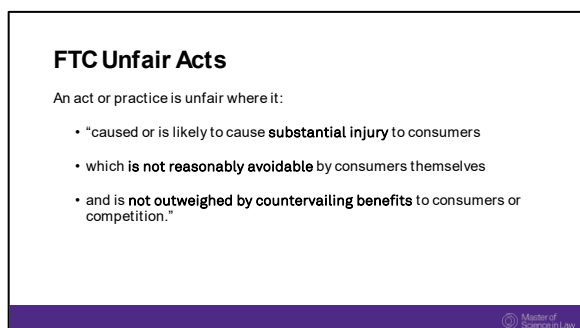
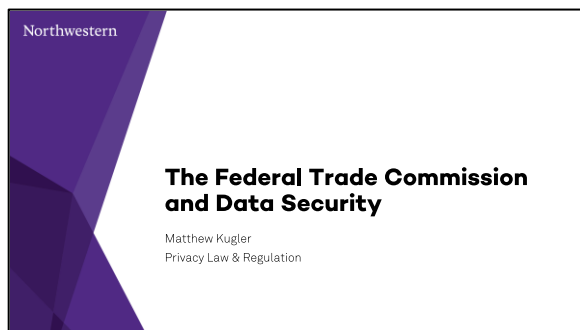
So the Washington Post is free to collect information from people so long as it does not come to know that a particular user on the website is a child. That's the actual knowledge piece

4. How does a website gain actual knowledge? Most commonly websites run afoul of this when they ask people to report their birthdate. If they know your day and year of birth, they know your age. So websites either don't ask, ask only for the day but not the year, or ask for the full date but block those under 13 from signing up.
5. Websites don't care if you lie. If an 11-year-old claims to be 14 to make an account on Facebook, that does not cause legal problems for Facebook. Though Facebook knows millions of children may do just that, it technically doesn't know which of its users are lying.
6. Now what about websites and online services that are "directed at children?" This is less complicated than you might think. Imagine a YouTube channel directed at 4 year olds. Then one directed at 20-year-olds. They're rather different. 4-year-olds are getting bright colors, actors and models that are their same age, and cartoon characters like Mickey Mouse. A monster fighting anime series featuring high schoolers is not like that at all. Yes, it is animated. But the amount of blood, death, and sex would generally not appeal to 4-year-olds.
7. This brings us to the YouTube case itself. YouTube is a general purpose website, but it has channels that are plainly directed at children. Under COPPA, those channels are child-directed and cannot collect data without parental consent. Also under COPPA, a website is "deemed directed to children when it has actual knowledge that it is collecting personal information directly from users of another Web site or online service directed to children." YouTube knew these channels were child-directed, its own advertising and internal documentation made that clear.
8. The YouTube case has two unusual elements. First, there is a massive dispute about whether the fine was large enough given the size of YouTube. How hard to you have to hit a company like that to make it pay attention?
9. Second, there was a large discussion about contextual versus behavioral advertising. Behavioral advertising looks at everything a person does online to target them the best possible ads. So if a person searches for toilet seats and then reads communist political thought, the communist website will show them ads for toilet seats – even political radicals need to poop somewhere. To serve this kind of advertising you need to track people across websites with exactly the kind of persistent identifiers that cannot be collected under COPPA without parental consent.
10. Contextual advertising instead serves ads based on where you are online right now. So the communist website will serve you advertisements for things of interest to communists, and Gabby's Dollhouse videos will serve you

advertisements targeted to people who like Gabby's Dollhouse. Contextual advertising ignores what you were doing online 5 minutes ago.

11. Behavioral advertising is much more profitable than contextual advertising. This is essential to understanding why companies keep collecting all the information that they do. Behavioral advertising is the core of (particularly Google's) online business.
12. We do need to wonder if COPPA is actually doing any good. Is it a problem if children are tracked online? Or, rather, is it a bigger problem if children are tracked than if adults are? And why 13 as an age cutoff?
13. Part of what is going on here is that COPPA gives parents a lot of control over their children online. Parents can demand websites turn over data collected from their children. So if a 12 year old somehow gets permission to post on a message board, their parents could demand to see everything they've posted. This sounds sensible for an 12 year old – you likely don't want 12 year olds having private conversations with strangers online. But it gets less sensible every subsequent year, to the point where you would be deeply concerned were a 17 year old's parents wanting to exercise the same total control.

Week 6 Video 3 – The Federal Trade Commission And Data Security



14. We have already talked about the role of the FTC in holding companies to their privacy policies. In addition to its authority over deceptive practices, however, the FTC can also pursue companies for unfair acts or practices. An action or practice is unfair if it
- a. causes or is likely to cause substantial injury to consumers
 - b. which is not reasonably avoidable by consumers themselves and
 - c. is not outweighed by countervailing benefits to consumers or competition.
15. This again seems quite broad, but it isn't as crazy as it initial appears. Think about how a lawsuit over a simple accident works. Person A hurts B and B then sues A for negligence. A court hearing that case is basically being asked whether A was taking a reasonable level of precautions, whether they were negligent or reckless in causing the injury. Judges have to make that kind of reasonableness determination every day.
16. Imagine a company has bad data security. This may be unfair to consumers because it a.) is likely to cause injury and b.) consumers can't avoid the injury themselves. But first the FTC asks c.) whether there is some benefit to consumers in not having better data security. We can always have MORE security of some sort, extra levels of verification and the like. But those extra layers of security slow things down. Sometimes that slowdown is well worth it, and sometimes it isn't.
17. What this means in practice is that the FTC is often trying to enforce industry standards. If your competitors can make a given level of security work, then odds are that you can too.
18. The FTC puts out data security guidelines. These are more best practices than they are legal requirements. Some of them are a bit more aspirational. For example, the FTC would love if companies only collected information that they need as opposed to vacuuming up everything. But other guidelines are more focused. The FTC wants companies to limit who within the company has access to various pieces of information. Think about every time you've called customer service and they only had the last four digits of your credit card number; that's a good thing. Limiting access this way both stops employees from snooping and limits damage if their credentials are hacked.
19. Most frequently discussed, however, are their guidelines for network security. These are expressed at a high level of generality, as you saw in your book. The main goal here is for companies to segment their network and control external access to it. Lots of major data breaches occur because a security failure in one part of the system gave access to the system as a whole. Also the FTC has had a multiyear push toward two-factor authentication.

FTC v. Wyndham

- Wyndham Worldwide suffers repeated data breaches. FTC brings suit.
- 10.6 million in fraud losses from 600k sets of data (~\$16 per
- Wyndham argues:
 - the Section 5 unfairness authority does not extend to data security; and
 - the FTC has failed to give fair notice of what data security practices are required by law.

Master of
Common Law

20. So have that in mind as you read through the Wyndham case. Wyndham is a hotel chain that experienced three successive data breaches. As a result of the breaches, 619,000 credit card numbers were exposed and leading to an estimated \$10.6 million in fraud. The FTC alleges that Wyndham acted unfairly by failing to employ reasonable data security measures.
21. Wyndham made mistakes like not using firewalls, permitting brute force attacks on firewalls, failing to inventory their computers, using easily guessed passwords, and storing payment information in clear text.
22. Now, for years the FTC had been enforcing section 5 against companies responsible for lax data security and no one had litigated against them. That's why you were reading settlement decrees from a lot of FTC cases – pretty much everyone settles, so you don't get court decisions. But Wyndham decides not to settle and they challenge whether the FTC has the authority to do what it has been doing under the statute.
23. Wyndham's arguments here are pretty decent. The FTC has been given explicit authority to sue over data breaches in some contexts - like HIPAA and the fair credit reporting act – and Wyndham argues that means the FTC doesn't have general authority to sue over data breaches. But the court isn't interested in that argument, and likely it is right to be skeptical. The FTC has very broad authority to protect consumer welfare, and there is no sign that Congress meant to bar it from acting in this particular domain.
24. The better argument is that the unfairness standard is really vague. Though Wyndham could have been expected to “be better than this,” it's hard to say exactly where the problem is. In a lot of contexts the answer would be “look to precedent.” But, since no one has litigated against the FTC in this area, there isn't any.
25. The FTC does, however, have a pile of consent decrees showing what security failures other companies have been forced to remedy. And it puts out those best practices guidelines. Though Wyndham may not have known exactly what was required to avoid liability under unfair practices, it certainly had some

notice. The court here holds that it knew enough for it to be fairly punished. “Unfair” is not too vague to survive constitutional due process scrutiny.

26. I want you to pause and do some quick math here. I told you that there were 10.6 million in fraud losses from 600 thousand sets of info lost. On average, then, each person whose data was lost received about ~\$16 in fraudulent charges. Obviously the losses weren’t evenly distributed, but likely all or almost all of those losses were reimbursed by the credit card companies. But, as you think through the math, you see why individual suits are so awkward here. People don’t sue over 16 dollars.
27. The loss of almost 11 million dollars, though, is a big deal. Fraud raises the cost of borrowing for everyone. Whomever gets stuck with the bill – VISA, Best Buy, Macy’s – has to make up that money somewhere, generally by charging their customers more. The harm is real, it is just diffused across all the law-abiding customers of these companies. The FTC gets to focus on consumers as a whole, rather than a subset of plaintiffs, and when dealing with that large group of consumers it’s less necessary to prove that any particular consumer was harmed. It can aggregate across the various risks and say that the conduct “causes or is likely to cause substantial injury to consumers,” meaning consumers as a group.

A company cannot be compelled to adopt “a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers [and] shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity [etc].”

- LabMD, Inc. v. Federal Trade Commission (2018)

Master of
Science in Law

28. If you’re feeling some sympathy for Wyndham here, know that an argument like theirs won in a different federal appellate court in 2018. The court there held that a company could be required to fix a specific set of data security problems that it had previously had, but it couldn’t be compelled to adopt quote:

- a. “a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers [and] shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity [etc etc].”

29. The court held, basically, that the company couldn't be fairly ordered to do that because neither the company nor the court knew what that was.
30. The FTC has started writing more detailed orders - more checklists and less vague standards. The consent decree in the FTC Equifax case is much more precise. Take a moment to look at these requirements. They are a fairly good fit for the guidelines I discussed at the beginning of this video. There is a lot of focus on network segmentation, the tracking of both authorized and unauthorized access, the use of multifactor authentication, and the training of employees.
31. Both FTC orders and the failures of the companies addressed by those orders have not changed much over the last several years. Chegg, the online education company, suffered four breaches over a five-year period. Three of those breaches were tied to successful phishing attacks that compromised employee accounts – accounts that had access to far more information than was reasonable. And then the breaches were not promptly detected, because the activity of those accounts was not sufficiently monitored. This pattern is sadly all too common.
32. The FTC is using these actions to discover and proliferate best practices, so that companies can look at where other organizations have failed and learn from their mistakes. Keep in mind with all of this that the FTC only has a limited pool of resources. It will only bring a handful of these data security actions in a year, and those actions are usually against the worst offenders.