PENN: Hello. Welcome to the Social Breakout, the podcast where we break down our complex world one topic at a time using our sociological imagination. We are your hosts, Penn.

OMAR: Omar.

ELLEN: And Ellen.

PENN: Today's topic is privacy and surveillance. We are watching you. I wanted to say that like a much creepier voice, like whispers.

PENN: This is gonna be a fun episode, but man, it took me a long time to plan this, because there's so much in privacy and surveillance. We're not gonna cover nearly everything that you guys, the listeners, will probably want us to cover, but we can always do another episode. But the main impetus for this topic is this recent news on this past January of Congress passing a controversial section 7.0.2 of the Foreign Intelligence Surveillance Act, also known as FISA reauthorization. So they reauthorized this section, which was expiring. FISA first came in effect in 1978 but of course, September 11 has already expanded its powers of surveillance essentially. Basically, the FISA allowed more or less domestic wiretapping programs during the Bush administration up to a present day.

But Section 7.0.2. in particular allows the US government to collect communications such as emails and phone records of foreigners on foreign soil without a ward. The law targets non-US citizens. Critics have warned that the government may incidentally monitor US citizens who are communicating with non-US citizens outside the US. Its proponents have argued the program helps keep Americans safe.

ELLEN: And they've already found evidence of US citizens being monitored via FISA.

PENN: The whole NSA, Snowden leak. We've all been wiretapped. All our phone records are just up for grabs. So this extends and NSA’s warrant surveillance programs for 6 more years with minimal changes, which also rejects a push by bipartisan groups of lawmakers to impose significant privacy limits when it sweeps up Americans emails and other personal communications.

So basically, companies such as Google and NTNT, they're gonna be compelled to hand over information to the government. And that will include American information as well. This is pretty controversial because even though it's supposed to be anti-terrorists or whatever, you know, we're protecting America, Americans are also swept up in the whole program. So it brings into questions a lot about privacy.

ELLEN: And they could use this provision to say that they are and I am doing air quotes, “monitoring non-US citizens”, but in reality, they're using it to monitor US citizens. They just say, Penn got caught in the mix, I'm sorry that I looked at all of her text messages and listened to her voice mails and tracked her movement. She was talking to somebody who is not an American.

OMAR: And then, of course, that makes a convenient circular argument cause like, this is the cost of fighting terrorism for national security, part of this great nation. Isn't this what you want? Don't you want us to protect you, keep you safe?

PENN: And it's also like, what are you so worried about? You shouldn't have anything to hide, right? This brings a lot of questions about what it means, what we mean by privacy and what we want privacy to be in today's society. And is privacy even possible in today's technological society?

ELLEN: I like that you touched on the whole moral aspect of privacy and the fact that a lot of the Representatives and Senators who are part of making this provision pass, they are saying, well, I have nothing to hide and you have nothing, right? We're all good citizens, so why do you care about this? And so that's like placing morality in the sphere of privacy, right, like, why do you want privacy? What bad things are you doing? What are you are afraid of?

OMAR: Though sometimes I catch myself thinking, I don't have anything to hide. But the same time, so what? That doesn't mean I also want a microphone always on in my house, and I know that someone else could be listening to my conversation, even if I am talking about basketball, like if it's a private conversation. It's a private conversation no matter what.

PENN: If you have nothing to hide, would you be happy if your neighbors just sat in your living room the whole day? You want that? That's basically what the NSA is doing, what the Government is trying to do. Do you still want something of your own time, you still want some privacy like if I am going to eat Nutella in the dark, I don't want anybody to know about it, with a spoon, you know, I do that. No one needs to see that.

OMAR: But now, with technology, I will know.

ELLEN: NSA will know about this behaviour.

PENN: I know, they are recording our conversation because we are recording it. That's funny. That was like the whole thing when they said Samsung TVs could be tapped by the NSA and they could listen into all your conversations and Stephen Colbert was like, all they would hear is where's the Ramone? Where's the Ramone?

The majority of the conversations aren't gonna be interesting to the NSA, like millions and millions of minutes of conversations aren't gonna be interesting to the NSA. But just that feeling that, oh, I thought this was secure and I thought this is private but that it's not, and that's really what it comes down to, is, there's nothing really secure, like if you use work email, you know they'll say, your work has the right to read your emails because it's a work email like there's nothing private that can happen in these public forums.

So going back to surveillance, right? What does surveillance mean? Surveillance literally means keeping a watch over or guarding or supervising. It's originally from French. Within sociology,

surveillance has acquired a rather more technical meaning referring to the relationship between information and power. Exercise is a power, right? And we define power as the ability to compel someone to do something, especially from a state authorities, government. The exercises of power, whether at the level of the State or the organization, or between individuals, usually involve some form of surveillance. Because those in power need to gather information on their supportiveness, issue commands, and then ensure that those commits have been carried out. It doesn't always need to be like this super evil government surveillance program. It can just be like, oh, your boss needs to get to know who you are, so they can know how to work with you.

But the most famous discussion on surveillance systems is probably the Panopticon. Within sociology the Panopticon comes up a lot. There are different forms of the Panopticon. The Panopticon was originally a type of prison designed by Jeremy Bentham, who was a philosopher and social theorist in the eighteenth century. It's basically this circular prison with one guard tower in the middle that can see everything within the prison field. So that basically the prisoners are always being watched, but the prisoners cannot see the guards, because they're all high up in the guard tower, and they can never tell when they're being watched. And as a result, this was Bentham's theory, that psychologically the prisoners would start to control themselves, control their own behavior because they would feel like they're always being watched and so they would never know when they can behave.

ELLEN: So it's a psychological take on surveillance that we are surveilling ourselves, and we are controlling ourselves to fit what society tells us is right or legal.

PENN: And then the idea is that eventually there does not need to be a guard in the guard tower even because then the prisoners were basically self control.

OMAR: And of course that's the place, at least for me, I don't want to say that stuff like the problem with surveillance but like the idea that we would think that we would need to have surveillance to control behavior, even though it does, because it can be largely effective, but to assume that that's what the sole purpose of surveillance systems do, or at least that's what we would want the benefit to be, I think is unfortunate.

ELLEN: Think about like when you're a kid and your mom or your dad was like, Omar, you are not gonna go across the street. You're only allowed to stay on this one street that we live on, because we gotta be able to keep an eye on you. So you go out with your bike and you're with your friends and your friends cross over to that next street, but you're just like, oh, you know that thing inside you it's like, oh, mom, mom told me to, you know, I can't.

OMAR: This control factor comes in.

ELLEN. Yeah, the idea of the Panopticon is like that idea of like what if mom finds out? Oh, mom is gonna be upset, you know, like but it's not mom in this situation, right?

PENN: But if you knew that mom had a CCTV camera. And you know, she's watching me right now. S***.

ELLEN: Mom is the government in this case.

OMMAR: Moms are always omnipresent.

ELLEN: The ultimate Panopticon.

PENN: Bentham describes the Panopticon as “a new mode of obtaining power of mind over mind, in a quantity hitherto without example”. I don't even know that quote means anything. But basically it's a control of the mind.

ELLEN: And this is written primarily about and by Michel Foucault who is a French sociologist, philosopher, etc. And the specific book where he really talks about this is “Discipline & Punish” which will put a link to in our website.

OMAR: Great book. Great book.

ELLEN: Hard to get through honestly. It is not easy to read, but It has good ideas.

PENN: He came up with the theory of Panopticism, inspired by Bentham's Panopticon, but they actually never built a Panopticon for a variety of reasons, because architecturally it was actually very difficult for the guards to see the prisoners, but not the prisoners see the guards. It was actually really hard to manage that. So Bentham went through a number of different drafts of the Panopticon model. But there's actually never been one built exactly to specifications.

Moving from this area in prison for example, we talked about mass surveillance. This is what the original article we opened up with about the FISA Act, that mass surveillance and global surveillance, this practice really came to light during the Snowden leak that this was actually happening at a very large global scale. Snowden was a former CIA employee, who leaked a number of top secret documents from the NSA exposing a widespread surveillance program that allowed to NSA to collect Americans phone records from virtually every telephone company in the US. It also exposed another program, PRISM, which allows the Government to demand user data from companies such as Google, Facebook, Microsoft, Apple and compels these companies to comply. Sometimes they don't and they do go to court.

And NSA was also found to be spying on world leaders and foreign governments, which led to some corrosion of diplomatic trust with our allies, that we were spying on the British government for example, and they're supposed to be our ally. And if all that doesn't worry you, there's also a tool that NSA use called Xkeyscore, which allows them to search nearly everything a user does on the Internet through the data intercepts. While many criticized Snowden for jeopardizing government intelligence efforts around the world and for potentially exposing sensitive

information that could lead to intelligent agents be harmed or these programs failing, the overall effect of the Snowden leak was something like enlightenment and rage is what I came up with. We always had that inkling like, oh yeah, government's always watching, big brother's always watching. But this was actually proof that yes, Big Brother is watching, and they will be collecting everything and they're watching everybody else in the peripheral as well. There was a lot of anger and confusion that came along with it. Because now it comes down to how do we protect ourselves. Is anything safe online? Is anything safe through technology? Bentham's concept of the Panopticon involved to the virtual Panopticon or the information Panopticon. There's a digital Panopticon, basically Panopticon on the Internet. It's not this physical prison anymore, but this virtual prison that we are all existing in because we use technology.

OMAR: I really I hate, though I think it's important and it is and it's I am not trying to take away from people's feeling of something has been personally breached on you, when something online is being viewed by other people that you might not have intended to. I think it's a little frustrating to ask the question, is there anything safe online, because mother f***ers, it is online.

ELLEN: Yeah, you put it online.

OMAR: Especially, especially Facebook. It's like you are only doing this because other people look at it. It's not like, you know, people write blogs for themselves. Yes, but ultimately they want other people to read them, and you have to do a lot of this like marketing and plugging to make your blog like available to other people. Hence our podcast, all the things that we do to mark our podcast, but with the Facebook, you already have friends who you know when you post something, you're gonna interact with them. So when you put something personal on there, you know other people are going to read it. So the reaction of, oh, it's Facebook, it's my private stuff, it's like, but you're also putting it in a public space, so I don't know how really private this is.

PENN: And you also understand Facebook is a corporation. They make money out of this stuff. This is a business. It's not like this free government service, that's like, oh, yeah, if you want to connect with your families and friends, that's fine. No. This is a business. It's a company that built this off of people's private information. That bullshit thing that people were posting on their Facebook accounts, you guys remember seeing that a while back where it's like, oh, this is a legal claim saying that everything that I put on Facebook is mine. So many people did that. It's like, no, that doesn't going to save you from anything when you signed in and created your first Facebook account and you agree to their terms of services, you're done. That's the legal contract that you made.

ELLEN: That's kind of like you know, say, I decided I was gonna change my clothes. But I changed my clothes out on the street, and I was like, hey, stop looking, is this kind of like, you did that out in public. Or if they see that, erase that from your mind, erase it. It doesn't work that way. Yeah, why are you outside?

PENN: But how can we become safe or private in this digital age? There is a book written not too long ago by Julia Angwin called Julia “Dragnet Nation: A Quest for Privacy, Security, and

Freedom in a World of Relentless Surveillance". It was written, I think, just after the NSA hack, but it was a very interesting experiment. Julia Angwin is a Wall Street reporter, and she tried to do a number of things to become completely off-grid, to become more private and more secure with her information, more untraceable.

For example, she stopped using Google. She deleted all her Gmail accounts, all her Google related things and started using this other website called www.DuckDuckGo.com . If you haven't checked it out DuckDuckGo.com is a search engine that doesn't track you. It makes you untrackable because it pings your location around the world. So that is like a VPN, it masks your true location. The problem with DuckDuckGo.com, she found was that it is super slow, is one thing because it's too busy pinging you around the world, to actually give you instant search results, and then it also makes it so that the search results are not customized to your locale, because it doesn't know where you are, of course trying not to show where you are. If you search like Nearest bank or supermarket or something like that, It's not gonna know that you're based in Honolulu, Hawaii for example.

She also wrapped herself on tin foil, and tolerated strange looks from strangers, whenever she had to open up her foil cell phone to use it. She also opened up credit cards with a fake name which is apparently legal and very easy. I didn't realize that. She opened credit card with a fake name to the point where her fake identity started getting spam mail of its own, and it seemed like the fake identity was living a life of her own. She said, that was pretty creepy. She concludes that the only way to live off-grid is to basically live like a criminal, like using burner phones and things like that, and not heavy using of any mainstream applications or websites. She says that as a person in this modern-day society, you can't function or keep up that way, and you would have to abandon so many things, so many things beyond and just like, oh, I'm just gonna uninstall Facebook, right? There's much more tied to it than that if you were going to really protect your personal information.

Her whole point in the book is this dragnet. So the dragnet is basically something that scoops up information indiscriminately about everyone in their path. So something like these warrantless surveillance programs that the NSA and the Government is doing, that's basically a dragnet where they just basically have this huge net where there's dragging across a whole country or the whole world, and be like, well, maybe we're gonna pick up your stuff along the way, but we are not looking at it, but we have it, that kind of thing. It used to be a lot rarer, but that's no longer the case, as these dragnets are extending into ever more private corners of the world.

As a consequence, daily life is increasingly crosshatched by threat assessments, market research studies, nudges, and other data-driven enterprises designed to sort, score, manipulate or guide us toward desired outcomes. So it's not just the government that's surveilling you to save you from terrorists, it's also companies trying to profile you, this we talked about this in our family episode, too, that they're profiling you to market towards you, where they're like, oh, you googled this, we're gonna show you these ads.

There is a case of this teenager who was online, and then her dad gets an ad from Target saying, “Oh, you're having a new baby. Here's all these mom advertisements!” And it was because this teenager who was pregnant, but was hiding it from her parents, was trying to search all these pregnancy stuff online and then started getting targeted ads. And that's how the dad had found out that his daughter was pregnant.

ELLEN: I find out very regularly about car purchases that my partner is making based off of like he will google something. Sometimes he's logged into my Amazon or sometimes he's logged you know and then all of a sudden, I will be on Facebook and I'll look on the side panel on the right side, like you can buy this truck winch for $799 and I am just like, you're a buying a winch for your truck. Do you need that?

PENN: Nothing is safe.

ELLEN: Nothing is secret.

OMAR: I think that's obviously aside from the winch and the pregnancy. That is what's the real problem with this types of surveillance, because, of course, there are people, and I've thought this way too like, well, I mean I care, but I also don't really care if they surveill me because I'm not hiding anything. Do whatever you want, I'll plug in my Alexa and Google voice speakers, and leave them on all day. You can have my voice tapping into the servers all the time and I'll just scream F*** Trump into it just so you can hear that. But honestly, the problem is that by having these types of surveillance systems, you literally, as you just described earlier, have to almost look like a criminal to not want to be part of like being like on the grid or whatever. That's the problem, because with surveillance and all these technologies and now marketing schemes, it severely narrows genuine thought and ideas which, you know, ideas are not always genuine to the individual person. But you have very limited options to want to live your life in a particular way. It gets very hard to not want to have a phone or a computer or not want to be on social media, just seeing how hard it is and of course, that drives up consumerism like crazy because now you don't have to actually go search for these things that you think you might want. You can be scrolling on Facebook, just doing your thing and then Hello Kitty ad pops up, you're like, oh, that looks really cool! And then now you buy it because it's in your face and I've done that. I've already bought 2 or 3 things on Facebook.

PENN: I would click on Facebook ads. Although it gets ironically kind of funny when the ads don't match you, then you're like what the f***. That’s not me at all. Like my friend who is a homosexual, and he's like, Google hasn't figured out that I'm a gay yet. He keeps showing me all these other ads that I'm like, no, I go one way, and you know it upsets him.

OMAR: Netflix is a perfect example. If you watched this, you’ll like this. That pulls you into a binge watching of a whole another season or 4 seasons of something, and you just made Netflix a whole lot of money that you might not have done, had you not had that marketing. And I am not saying, don't watch Netflix. I am just saying, this is the world we live in.

PENN: And it shouldn’t be surprising to anyone. I'm sure everyone was listening was like, yeah, yeah, but you can't live always worried about those things because then you won't be able to move on in your life. You just have to ignore and just be like, well, yeah, whatever, they took it.

But in terms of other forms of invasions of privacy, we haven't talked about enough yet, but we mentioned doxing last episode. Sodoxing is a very interesting practice. It's a form of online vigilantes which I studied in my dissertation. It is basically exposure of private information, often with that pretty dark consequences, intended or otherwise, especially when they misidentity a person. Doxing is originally a slang term among hackers for obtaining and posting private information about an individual, usually a rival or an enemy. To hackers who prize their anonymity, doxing is considered a cruel attack, right of exposure, right? Because people function online anonymously, that's how they feel like they can say all these shitty things and be trolls, but also engage in their passions without fear of judgment from anybody. The internet is supposed to be that safe space, so to rip away that mask and to expose private information, that can be very harmful. But doxing has really emerged from subculture websites like 4chan and Reddit, to become something of a mainstream phenomenon. Just last year in August, there was the the Charlottesville March and then subsequent attack. I don't know if I would call it attack. It was just a mayhem. It was a complete mayhem and a woman died, and it was very bad, and it was basically this white supremacist march in Charlottesville. And people dox those white supremacists.

ELLEN: Good for them.

PENN: Who are these people marching down the streets? This is seen as a form of justice. Yes, we want to out these horrible white supremacists so that they can't hide anymore. And it's not like they're hiding, you know, they're on the streets. Doxing usually ends up with exposing who they are. You expose where they work, you expose where they live so they get harassed at their place of residence, and they usually lose their jobs. That happens a lot.

ELLEN: But that's totally okay in this case. If you're a vowed White supremacist who's carrying around a tiki torch, saying, the Jews will not replace us and your face gets caught on the photo, for sure, dox the mother f***er, like he doesn't deserve any privacy whatsoever for spewing that kind of no tread, you know.

PENN: But see, the problem is that they did misidentify some people as white supremacists, so they identified the wrong person. This is why, I said last episode, that doxing is a double-edged sword, because it can be very good when you're trying to correct a social injustice or you're trying to pursue social justice, but it can also be very bad when you misidentify an innocent person who gets caught up and then gets mistaken for white supremacists, for example.

OMAR: But not even misidentifying a white supremacist. There's also been police have done this for decades now, before the Patriot Act of finding where people in the Civil Rights movement or Black Lives Matter where their next meetings are going to be and then they'll show up and then they can already start arresting people and tracking people, following people. A lot

of social movements in resisting the state or fighting for justice will say things like, no, in our meetings, put your phones over there or don't post anything on the internet for those types of reasons.

PENN: So, then, another type of invasion of privacy is revenge porn. Revenge porn is pretty terrible. Revenge porn is basically when you post sexual or nude photos of somebody, usually in act. This is usually in corroded romantic relationships and post that online.

There's a really famous case now of a woman named Chrissy Chambers who was a Youtuber. She had like 50,000 something subscribers with her and her partner. She is Lesbian. But her ex-boyfriend, this is before she came out, her ex-boyfriend uploaded their sex tape onto the internet, before the revenge porn laws were passed in the UK. So revenge porn is a very new phenomenon that people are posting nudes or sexual photos as a form of revenge, as a form of retaliation.

CNN even titles the revenge porn article as “The Cyber War Against Women”. So it's very, very much misogynistic practice. But the UK did criminalize revenge porn but that it doesn't apply to historic offenses, which is so bullshit. They're like, we don't even want to deal with past offenses. So Chrissy Chambers, you know, whose ex uploaded before the law was passed, she had to spend 4 years battling this asshole in court, do different avenues like her claim got rejected a couple times, and she had to keep going back and back to sue this guy, and they ended up settling. And part of the settlement was that this guy gets to remain anonymous, even though her name and her body is already online, literally everything about her has been exposed, but she did get monetary compensation, and most importantly, she got the copyrights to the video, right?

It is not necessarily that it's been taken down everywhere she's gone, everywhere on the Internet. She has the rights now to demand that it be taken down or she has a legal right to do that . This won't stop revenge porn from happening, and this was just the first case of its kind, just in 2018 this year, that this was just happening. So this is still very much an up-and-coming legal process that we're trying to understand in terms of this type of invasion of privacy.

And then, of course, the last form that everyone knows and this is all the same, it's hacking. Hacking happens all the time. A couple famous cases of hacking in relation to invasion of privacy, that I thought of, was the Fappening which happened a couple of year ago. It's a horrible horrible name, but basically iCloud got hacked and over 500 nude photos of mostly female celebrities were posted on 4Chan.

ELLEN: For the Fappening. I don't even want to say that. We're gonna call the iCloud hack the iCloud hack. I know that a couple of the guys who were behind it, have been arrested, and have been charged and actually convicted of these crimes. So that's a good thing.

PENN: And then most recently that I could think of, was the Equifax hack where over a 143,000,000 social security numbers were compromised. It took Equifax 6 months to tell us. It

was just a total disaster. I mean when that happened, it was just like, all right, nothing secure anymore. Whatever, who cares. Just buy my credit card numbers, bye my social security numbers…

OMAR: Target has had that problem. Yahoo has had that problem. I think when it comes to people's personal identification things, like licenses, bank accounts, social security cards, I am a 100,000 times more concerned about people who hack, then the Government surveilling me. Because what happens when you start building up all of these safeguards and all of these private internet browsers and things like DuckDuckgo.com. I am definitely not saying that those things aren't important, they absolutely are. But then hackers know this too. So they are also building up their arsenal to continue to try to think of new innovative ways to not be seen. And that just means that the scale at which, when they are successful, is just gonna get more intense, more intense, more intense. Because if Equifax comes up with a $1,000,000,000 budget to have a system that is going to protect people's social security cards, but when they get hacked again, the effects can be way more catastrophic, because those hackers have to obviously get through that.

So they are also going to get stronger as well and I would be very pissed off if you go into your bank account and you have zero dollars because someone stole your shit.

PENN: It is so shitty in so many levels and that's why it is really shitty when Equifax was like, oh, we'll give you free credit monitoring for one year, and it's like, no, it should be for lifetime mother f***ers.

OMAR: Yeah, or getting my money back or something.

PENN: They basically suck on so many levels.

OMAR: Or if you have to go to court to get your money back, they gotta pay your legal fees too.

PENN: This is a really hard part is when something is already stolen from you through a hack or doxing or whatever, it's so hard to get that back. It took this lady 4 years to gain copyright to her own video. That's just like one small example. People whose identities get stolen, it can take decades for them to get back a semblance of their old life back. And that's super terrifying. To me, identity theft is the most terrifying, more terrifying than NSA surveillance, like whatever you can listen to my conversations talking about boy bands, I don't know what you're gonna get from that. But if you're gonna steal identity, oh man.

ELLEN: There's a really good portion of Jon Ronson who has a book called "So You've Been Publicly Shamed". Towards the middle or end of that book, he talks about, there's a few services out there where if you've been publicly shamed for doing something, he highlights a few different people. There's one girl who tweeted while she was flying to South Africa or some country in Africa.

PENN: Justine Sacco. Justine was flying to Africa. Before she got on this eleven-hour flight, she tweeted: "Going to Africa. Hope I don't get AIDS. Just kidding. I'm white!" She had a couple of hundred followers, because she was a publicist for some councillors.

ELLEN: And by the time she landed in Africa, it had blown up. She was trending on Twitter. She's getting death threats. She was getting all of these different things. So whenever you google her name, that's the first thing that pops up. So basically, it will ruin a person's future career possibilities etc.

So Jon Ronson, in his book, talks about how there are services who, if you have experienced something like this, where you've been publicly shamed, and there's people who have doxed you, you can get this service to go and create a ton of posts about you that are unrelated. Justine Sacco loves dogs. Justine Sacco is a dog breeder. They can create so many posts and have an algorithm that clicks into those posts, so that it pushes down all of the shaming posts that you would normally see if you were to google that person's name. You just see, Justin Sasco loves knitting or something like that. It's interesting to see these new services and new ways of getting around doxing or fixing your virtual presence online. And maybe there's gonna be some way to I don't know how you would fix the privacy situation that we have right now, but technologies is crazy. I'm sure something new will come up.

PENN: It's always changing. So basically, what these companies do, is play with Google's search algorithms, for example, to try and push down the best search results. Companies like that need to exist and they should become more and more prevalent for people who really need it. But it also goes to show that the law currently is very much behind on these new technological attacks against privacy, because the law doesn't understand what's an IP address. If you got a death threat on Twitter and you call the cops, they don't know that, they're like, what do we do with that? Does that even mean anything? And that's why one of the reasons, for example, that Jessy Sacco has so many problems, because no one could help her. Basically she just had to disappear. She went to the Dominican Republic or something for 6 months, just to go to a place where nobody knows her, so that she could actually put some time and distance between her and the haters.

Those are really interesting new law that's coming to light. And I think we're gonna end on this point with the right to be forgotten. And the right to be forgotten really came into life over a year ago in a decision that's impacted many American internet companies. Europe's highest court ruled that search engines were required to grant an unusual right called the right to be forgotten. Under the ruling, Europeans who felt they were being misrepresented by search results that were no longer accurate or relevant, for instance, information about old financial matters or misdeeds committed as a minor, could ask search engines such as Google to delink the material, basically make it so that it's not part of Google search database. And then, if the request was approved, the information would remain online at the original site, like if there was a news article about you drunk driving, but that it would no longer come up in certain search engine queries.

This was pretty controversial because this passed in Europe. And then there have been a lot of questions about in America. And Google is really at the center point of this because they are the biggest search engine in the world. And it calls into a lot of questions about what is truth and what are the ethics behind Google search engine. So something like the company that you were talking about, Ellen, plays with Google search engine. You can argue for the ethics and morale of that as well. Now the people who are using that service are people who've been harmed, and so I can see why they need it. But for other people, who've done something criminal for example, do they also have access to these services? So when we're talking about a broadly scoped right to be forgotten, that's about altering the historical record or making information that was lawfully public, no longer accessible to people. I don't see a way to square that with a fundamental right to access to information. There's a quote from Elm Alonso, who's a free expression scholar at the Center for Democracy and Technology. Basically there are 2 sides. People who think that, no, you cannot alter history. If it's on there, you did drug drive it, you should be, that's it. People should know, your employers should know.

ELLEN: You reap what you sow.

PENN: But then there's also doesn't give anyone the right to a second chance, right or the right to start over if they have recovery from alcoholism, for example. They point out that the number of removals so far has been relatively small, although I don't know if I agree with that. Since May 2014 Google by far Europe’s most popular search engine has received requests to forget about a 1,000,000 web links and has removed about 41% of those from certain search results.

OMAR: I mean you can make things publicly accessible, but that doesn't necessarily mean they have to be transparent or not transparent. Think about the type of people who would want to know or need to know someone's criminal background. I don't think it's right to necessarily be able to type someone's name to the Internet and find it. You should have to maybe go down to the local police department, ask for the documents, pay 10 cents, then you can get it, because if someone actually really needs it, they will go through all that to get it, because it should be publicly available. But I think it gets into too much fog when you can just type in someone's name, and then boom, all their private information just pops up.

PENN: But that's what people really do now. People who are hiring for jobs and things like that, they'll look at your social media life, they'll go to Facebook, they will go to Google and that's why people who are on the job market tend to change their Facebook names and things like that because they're like, well shit, I don't want them to search for me, even if you have nothing to hide, but who knows what will make them like you or hate you?

Since this passed in Europe, this conversation has moved to America because people are like, well should we have the same thing in America? But in America if you try to do that, that basically goes against the first amendment, basically like freedom of speech and expression. Basically, you are trying to censor information that Google has about you.

OMAR: I hate the first amendment. And I don't hate it, because I don't agree, I hate it because of what people do with it and how people use it in arguments, because you don't have freedom of speech. You can't just walk into a classroom, and be like, teacher, piss off, I hate you. You can't just do that and you wouldn't do it. You also wouldn’t do that. You also just genuinely wouldn't talk to certain people in a certain way,

ELLEN: But it's the right to legally be allowed to say that, that's the power of it. There's that possibility that you could.

PENN: So freedom of speech and expression, the right to be forgotten, right to privacy, hacking and doxxing, surveillance. These are all like very messy topics. I think we've covered a good amount today.

Just on a final note, I will mention the concept of sousveillance in opposition of surveillance. Sousveillance is basically ground up surveillance where basically the people are watching the government.

OMAR: That's cool. That we need more of.

PENN: Sousveillance is a way for us to fight back against mass surveillance by the government. We're basically checking on the government. I think a good example of this is a Black Lives Matter Movement, how it exploded through these videos that everyday people shoot of police brutality. They gets posted online. They're horrible to watch but it's one way that we expose police brutality, and that's one way that we watch authority. So the point that now it's so small but some police departments are starting to put cameras on their police officers and things like that, or starting to check on the behaviors of their officers more and more.

OMAR: The sad thing about that is that is hasn't been hugely effective unfortunately.

PENN: So there's that other thing. Is the Panopticon really effective?

ELLEN: There's a really good another podcast out there called Embedded, and it comes from, I think it comes from NPR and they did a series, I think it was 4 or 5 episodes on police shootings. They looked at it from the police perspective, and how the police, like academies teach their officers what to do and how to handle guns. Then they also talk about having body cams on policemen and women and how that's changed. If you're interested in this topic, that would be a podcast for you to check out.

PENN: Alrighty, that sound signals the end of this week's show. Per usual, we are going to end with some quick breaks that I will throw at Omar and Ellen who must then do a personal breakdown of the topic in 5 words or less.

So I came up with these topics while I was falling asleep last night, and I was like, oh I need 2 quick breaks. Ellen, I will start with you. I am teaching currently on 3 different campuses, so I am

driving a lot around the island. To keep me company while I am driving, I've been listening to audiobooks because I also have set a reading challenge for myself to read one book a month. Your breakdown is audiobooks.

ELLEN: I love them. That's my breakdown.

PENN: That’s good. Some people think of them as cheating.

ELLEN: I guess they're cheating in the sense that you can be doing other things while also quote reading or listening, but I think they're fantastic. Audible is a great resource. There's some libraries out there that have audiobooks where you can borrow rather than buy, if you don't have the resources to buy audio books because they can get kind of pricey. There's a lot of social books that are made into audiobooks that you can listen to while you're driving or running or doing whatever it is that you do, folding your laundry. So I love them. There are still books.

OMAR: I think it's just awkward when you say, I read that. Well, you kind of listen to it, but honestly some books, it makes comprehension easier, because you can hear when there's a bunch of commas in the sentence that you can hear when the author changes tone and emphasizes certain things. Or are they being sarcastic or not? Because the person narrating will try to do that for the text. So sometimes it can actually enhance comprehension. And obviously you can “read” faster.

ELLEN: I think it's great for people who have learning disabilities, if you're a dyslexic, audiobook that shit up, you don't have to read with your eyeballs anything but you're still getting the message.

OMAR: It shouldn't replace books, though.

ELLEN: I agree with that. I agree with that It's not a replacement, but I think it's a good supplement to your busy life, and still wanting to get some knowledge.

PENN: It definitely made my drives a lot better, because sometimes I run out of podcasts to listen to, which means we need to release more episodes.

OMAR: Some people listen to audiobooks while they're reading them, like the actual hard copy book because that keeps our focus to read longer.

PENN: That's true. That's true. That's interesting. Just as an alternative to Audible, there's also a website called www.Libro.fm. It's an independent source for audio boats. So if you hate Amazon, you don't want to support corporate America, you can go to a libro.fm. And you can choose a local bookstore to support, so that the proceeds goes to support this local independent actual bookstore in some state, somewhere, you know, if there's a favorite bookstore that you have in your own state, they could become part of libro.fm.

ELLEN: Another one is if you go on www.archive.org . That's a place where you can borrow textbooks and regular books, just looking at the text of them for free, but they also have audiobooks that you can borrow for up to 15 days. And that' totally free. There's a lot of different resources out there for that.

PENN: Omar, Nintendo has announced the Nintendo Labo, which is a bunch of DIY cardboard toys that they made for the Nintendo switch. Have you heard of it?

OMAR: It's like the switch, you said?

PENN: So basically you buy the Nintendo switch and then you can also buy the set of cardboard toys that you can make to go along with the switch. So the ad is really cool where you can make a cardboard piano and then stick the switch in it and then play the cardboard piano and the switch will play the piano.

OMAR: Wow!

PENN: You can make a fishing reel and actually fish in the Nintendo's fishing games. And then you can make like a jetpack, and then you can fly and do like VR with the switch basically. So I don't know which part I wanted you to break down. And then one of the comments that I read was, this is the most Nintendo thing Nintendo has ever done. So break that down.

OMAR: I'm gonna say, what's it called again, what's the device called?

PENN: Nintendo labo.

OMAR: I think Nintendo labo and virtual reality need to link up. That's way more than 5 words.

PENN: But you can say VR is one word.

OMAR: VR and Labo, link up.

PENN: So they're definitely starting to do that. And that's super exciting.

OMAR: That's really cool because I think the problem now virtual reality gaming is gonna become much faster into our world, which I think is really really cool and I think what's gonna be cool about labo is that you won't have to start developing all these multiple types of devices for certain things. You don't have to buy the fishing rod, the steering wheel, the gun, the other things. It can all be one item that you just can figure into whatever shape or thing you want, which is, I think, would make virtual reality much more you realistic. So you're not just holding these 2 controllers that have sensors on them. You can actually hold something that resembles the item that you're supposed to be using, which I think is pretty cool.

PENN: So thanks for listening to the Social Breakdown. We really appreciate it. If you're interested in privacy and surveillance or any of the topics we talked about today, you can check out our website to learn more at www.socialbreakdown.com.

OMAR: And be sure when you're on our website to do our survey, because if you do a survey, we now have stickers that we will send out with our logo on it.

PENN: Just go on our page and then click Survey for Swag. In addition to that, you can also find us on Facebook or Twitter and send in your questions at @socbreakdown. You can subscribe to our podcast wherever you get your podcasts. And be sure to tune in next week. Until then…

ELLEN: Stay social.

PENN: Thinks social.

OMAR: And go read books.

PENN: Or listen to them. Audiobooks.

OMAR: Or write them.