Episode 2. The Original Sin of technology – 'Mistakes Were Made'

VARNEY: So, the original framework was getting companies to disclose and then if they are going beyond the bounds of what they say they're doing, prosecute them for deception, that kind of worked for about a nanosecond.

SWIRE: and at various points we came close to a deal because there was pressure on the advertisers, but it didn't happen. So the advertisers didn't have to do it.

RICHARDS: So back in the day it was a big deal just to get a company to sign up and actually put a privacy policy on the website because it meant that they were submitting themselves to the Federal Trade Commission. If you didn't have a privacy policy and you didn't say what you were doing with the information, then there really weren't any rules.

CATHERINE CRUMP: And sort of anything went and politicians were so fearful of alienating tech companies because of their economic role, ~~um,~~ that, that even sort of regulation that everyone agreed was sensible couldn't pass.

ED MIERZWINSKI: the fact is there are a lot of companies on the Internet, virtual companies, digital companies, companies you may not even have a real relationship with, that are collecting and sharing information about you. Uh, and it's not always for the good.

SWIRE: So we've got a huge technological wave crashing through. And then as a society we have to say, what are we going to do about it?

[THEME MUSIC]

ALIA: I'm Alia Tavakolian

BOB: And I'm Bob Sullivan

ALIA: And this is No Place to Hide, a So, Bob miniseries about the state of privacy brought to you by Intel.

BOB: Imagine a world where technology watched everything that you did, every place that you moved, every thought that you had. Where you literally had no place to hide.

ALIA: Last week, we talked a lot about what privacy is -- it's much more than wanting to be left alone. It's about safety, and freedom and originality. Our information is at risk. Which means our lives, our humanity, is at risk. We left off with data brokers: Companies whose sole purpose is to gather and sell the most intimate details of your life - from your SSN to the make and model of the car you might be driving right now.

Or in Amy Boyer's case, where she worked, which is the info her stalker ultimately used against her.

BOB PU: Liam Youens paid a data broker to give him the information he needed to kill Amy. But before we can get into why these companies are even allowed to exist, we have to go back to the beginning.

ALIA: Thanks to Cambridge Analytica, a lot of people are talking about privacy right now. But this isn't the first time America has had a big tech scare. And it's not even the first time we've had a big *privacy* scare

Bob: Professor Dan Solove, privacy expert at George Washington, has collected the story of the death of privacy, magazine covers about it, which have been published going back decades. "Will privacy ever stop dying" is the name of his collection, it's really funny.

ALIA: Oh my god these are great, and it's like covers from all kinds of publications, right?

BOB: So here's 2015 from Science "The End of Privacy"

ALIA: 2015 NPR "The end of privacy, a special series"

BOB: NPR 2014, "The End of Privacy"

ALIA: The New York Times 2014 Sunday Revue OpEd "Hacking Our Humanity: Sony, Security, and the End of Privacy"

BOB: 2013 "Is Privacy Dead? The Future of Privacy in the Digital Age"

ALIA: 2013 This week in cult of Mac Magazine, "The End of Privacy"

BOB: UT Magazine "Privacy is Dead" blood splotches

ALIA: 2012 The NYT Sunday Revue "The End of Privacy?"

BOB: "Privacy is Dead: With All These New Age Forms of Creeping, is There Any Room for Privacy Anymore?"

ALIA: 2000 "The End of Privacy: How Total Surveillance is Becoming a Reality"

BOB: "The End of privacy: The attack on personal rights at home, online and in court"
BOB: 1995 "The death of privacy, the battle for personal privacy in the courts, the media, and society"

ALIA: 1993 The New York Times “Who Killed Privacy?”

BOB 1970 Newsweek. “Is Privacy Dead?”

BOB: Okay so this is funny but the point here is back in 1970 national magazines were proclaiming privacy is dead and people were worried about this. And if people were worried about this decades before the internet was a thing for most people, how did we get here? How did this happen? How did Facebook happen? How did Cambridge Analytica happen? How did data brokers happen?

ALIA: And...why didn't somebody do something? Well, it wasn't for lack of trying. But...as we hear so often...mistakes were made.

BOB: So back at the beginning of the internet, people did already care about privacy, we knew there were issues. And there was a chance to get privacy protections right. However, they didn’t. Jules Polenetsky was there. And like so many historic tragedies, the birth of Internet tracking just seems kind of inevitable now. We'll let **him** tell you.

> JULES POLENETSKY: You know, the advertising model in the world on TV, on billboards, um, worked a certain way. Companies wanted you to learn about their brand. They wanted you to feel good about their brand. Coke should make you feel like you're having a great day. and that model worked. And to know whether it worked, uh, you would, you would survey people, you'd poll them, maybe you, maybe you were a Nielson family and we watched TV. Um, we had billboards across the country and we could actually ask you or track with your permission, um, whether or not the fact that you saw those coke ads made you feel fuzzier and you know, bought coke at the store. Um, when media started moving online, you had this real challenge.
>
> So basically what is targeting? Targeting is advertisers realizing that online they had a lot of data, data that initially they were collecting to measure their advertising, to know that it was delivered and to count how many times and to sequence it. But now they had in those log files, they had your cookie and all the different sites that you were using.
>
> JULES POLENETSKY: And so you could build a profile of somebody by saying, look, this person has been, this cookie has been to all of these different sports sites. They must be interested in sports. So I'll label them as sports and I'll sell them to a sports advertiser. And then targeting got more complicated when advertisers said, yeah, but could you add in my list of my customers so I can reach them online? Or here's this prospect list. Or here are people who look like my customers. And so it got more complicated and it got more complex and more personal and more targeted. And you might say creepier. Um, advertisers realized maybe you came to my site and you didn't buy, but you might've been interested or maybe you kind of got distracted. Why can’t I

> retarget you again, leveraging the fact that the ad tech companies are using the same cookie on many sites and could take advantage of the fact that this is a good ad, this is an expensive ad because you're more likely to respond.

BOB: The only way to make a real business out of the Internet -- and believe me, outside of porn, that was not given in the early days -- was to create ads that were even more valuable to advertisers than what they were used to. So, tracking was invented. Right away, users knew something was wrong with cookies, and have tried (unsuccessfully) to rebel against them ever since.

ALIA: So, Failure #1: Advertisers quickly realized that they could use the information they were already collecting to create profiles of you. These tracking techniques got more and more invasive and creepier and creepier.

BOB: So, the Federal Trade Commission worked with industry groups to create a way to force companies to publicly disclose what they were doing with the information they collected -- and make them liable if they strayed beyond these disclosures. And thus privacy policies were born.

> CHRISTINE: So the original framework was getting companies to disclose and then if they are going beyond the bounds of what they say they're doing, prosecute them for deception, that kind of worked for about a nanosecond.

BOB: Christine Varney is now an antitrust lawyer, but before that she was at the Federal Trade Commission when these privacy policies were created. And She kind of regrets how that turned out.

> CHRISTINE VARNEY: And then the companies became so concerned about their legal liability that they wrote these 23, 28, you know, 42 page privacy disclosures that nobody could understand. And I don't think the big companies in any way intended to deceive people by writing very complex privacy policies. I think they intended to be comprehensive in any, in all uses, uh, from the data or derived from the data. And that became an insurmountable barrier for, I think people understanding what it was they were disclosing and what was being observed about them and what was being done with that data and those observations online.

ALIA: Bob. Be honest with me. Do you read the privacy policies?

BOB: Of course I don't. No rational person would.

ALIA: Thank God, I really thought you were gonna be like "uh yeah Alia, anyone who cares about their privacy *would.*"

BOB: Yeah, I mean privacy policies feel like they are designed for you not to want to read them. I would show you the iPhone privacy policy, but my printer ran out paper when I tried.

ALIA: So Failure #2: Companies were more concerned with covering their legal bases-

BOB: Asses

ALIA: -rather than making sure consumers actually understood how their information was being used.

BOB: It does seem pretty bleak. Peter Swire is a professor at Georgia Tech now, but back during the Clinton administration, he was one of the first federal officials to have a job with privacy in the title. Which means it was his job to herd cats and get them to agree to stop the insanity of advertisers completely ignoring privacy. But he had no leverage. He couldn't stop this Greek tragedy from happening.

> PETER SWIRE: we were working on a standards process and we were trying to see if the privacy people and the advertisers and the regulators could sit down in a room and come up with an agreed upon standard so that your browser would work automatically and say, track me or don't track me.
>
> PETER SWIRE: But the advertisers didn't have much reason to go along. So they sat in the meetings and they said, oh, we can live with this as long as you don't do that. And at various points we came close to a deal because there was pressure on the advertisers, but it didn't happen. So the advertisers didn't have to do it and they sure didn't want to do it because they wanted to be able to sell their stuff and do their targeted ads. And so without Congress stepping in, there was no way to make the advertisers do that.

ALIA: Failure #3: Congress didn't step in, so advertisers had no incentive to go along with any proposed regulations.

BOB: Alia let's step back and talk about what happened to the relationship between consumers and corporations at the beginning of the Internet time as I like to say.

ALIA: Oooh I feel a white board coming out

BOB: PIcture a white board, and picture a pendulum, okay?

ALIA: Kay

BOB: And on one side is companies and the other side is consumers. And they're constantly teetering and tottering back and forth. Econ 101 – buying is an information war. In healthy markets, this is only theoretical but there's perfect information on all sides. You know all the

different people who are selling apples, you know what good apples look like, and they have to compete with you by having better apples and better prices.

ALIA: No one is keeping any secrets about the apples

BOB: As long as everybody has the same information, markets function. That's what open markets are. However this rarely exists. In most cases, companies have a bit of an edge information wise over consumers. They know that they are about to run out of apples so they can charge more. They know they have too many apples, they have to charge less.

ALIA: They know that Thanksgiving is coming up and you might be making a lot of apple pies

BOB: Right. So for the most part the information war is tilted, this pendulum is swung, towards companies. At the beginning of internet time, that changed radically. All of a sudden consumers had so much more information than they ever had before. Instead of having to go cart by cart to every apple salesperson, in two seconds you could sort every apple cart in the country practically and find out who had the cheapest apples.

ALIA: Oh my god of course all the information was right there at your fingertips

BOB: Right so the pendulum swung wildly towards consumers. Airlines for example, not that long ago, before the internet, most people bought their tickets through travel agents. Which means they had to believe whatever the travel agent told them. Sometimes the travel agent got pay from the airline or whatnot. And you certainly have never got more than one or two options. Right now if you want to fly to Hawaii Alia, you probably have hundreds of options. And again you can sort by price. That's a phenomenal development for consumers. But it's really terrifying for corporations.

ALIA: And it's terrifying for corporations because the consumers are now informed?

BOB: And because now we have this race to the bottom that all these companies are terrified of. Because you have to compete, only the company that charges the lowest price gets the consumers.

ALIA: The consumers had control and they didn't?

BOB: Consumers have all the control

ALIA: Wow

BOB: So enter Big Data. Enter something like dynamic pricing.

ALIA: And what's dynamic pricing?

BOB: Well you probably may not even realize this, but if you're logged in at one computer and shop for something at an airline or at an online bookstore, you may get a different price if you log in as somebody else.

ALIA: Wait, how is that legal?

BOB: It's legal because no one's made it illegal yet.

ALIA: Oh my god

BOB: Something you should always try by the way when you're shopping for airline prices is use a brand new computer and don't log in as yourself and see what happens, half the time you'll get a lower price. The companies know that you've looked five different times in the last week for that flight to Hawaii, they know you really want to go, and they'll probably try to charge you more, because they know that.

ALIA: Ugh that feels so unfair!

BOB: It does, but that's legal at least now in most cases. But this is the kind of thing that Big Data does for companies. Companies who wanted their information advantage back, they started tracking consumers. So that they didn't have to fight this race to the bottom and with this extra information, now they have an enormous information advantage.

> ED MIERZSWINKI: you know, you go back to the basic economics 101 we all took in college, and the rules of economics 101 were that to have competition you had to have the opportunity for buyers and sellers to have equal information. And we don't have equal information.

ALIA: That's Ed Mierzswinki of the Public Interest Research Group, a national consumer advocacy organization.

> Uh, and when companies that we don't have relationships with are collecting information about us and using it to possibly manipulate us and give fewer choices, I think it's very clear, uh, that, uh, again, as a consumer advocate, even though we're working in a different system than we were working in 30, 40 years ago, whatever, we'll always have work, uh, and people deserve better than what they're getting out of this system.

ALIA: That different system Ed is talking about is data brokers.

BOB: Remember when the Equifax hack happened and of the many angry reactions consumers had, perhaps the most important was: Who or what is Equifax and why does it know so much about me? Well, the bad news is that there are hundreds, thousands of smaller companies like

Equifax, like Cambridge Analytica, and they know even more about you. Data Brokers. And unlike Equifax, they are not required to tell you what they know, or even that they exist. Not in America, anyway. (That's changing, we'll get to that.)

ALIA: WHY WOULD these companies exist?

BOB: Alia. Let me tell you a story about my house sale.

ALIA: Oh no

BOB: So when you sell a property, somebody looks to see if anyone is entitled to payment on a property. Say you've got an electrical bill or maybe some taxes aren't paid, or any other way that people can put a lean on the pile of money that you're gonna get at the end of that sale. So the first time that the title company sent papers around to me, to my agent, to the buyer's agent, to everybody else involved in the transaction, listed on that piece of paper was you know who I am and all the normal information. And then there was this listing that said that I owed money for child support

ALIA: But Bob, you've never had a kid, right?

BOB: Right I've never had a kid, it wasn't me. And on that very document it said I owed money for child support, which went to all these people that are now involved in the most important financial transaction of my life with-

ALIA: Oh my god

BOB: Who now all think I'm a deadbeat dad. On that very same piece of paper, it was clear that the middle initial of the person who owed the money was different than mine, the age was 20 years different from mine, their prior addresses were different from mine, internally in that piece of paper it was easy to see this wasn't me. But my name is Robert Sullivan, the world is full of Robert Sullivans, and every time I have ever been involved in any kind of search like this, something like this comes up. Might be on a sexual predator list, might be involved in a former manslaughter that happened when I lived in Missouri

ALIA: Oh my god

BOB: And in this case I'm trying to sell a house and now all these people think I'm a deadbeat dad

ALIA: How do you defend yourself?

BOB: Well the line you hear in privacy over and over is how do you one ring a bell?

ALIA: Yeah

BOB: So of course I called the title company and they say oh this happens all the time, don't worry fill out this additional form - I had to fill out an additional form to prove that it wasn't me

ALIA: So you had to do the work because of someone's mistake

BOB: And all the time it took to fill out that form, hanging out there is the notion that I might be a deadbeat dad to all these people and I keep saying send an email tell people it's not me. So eventually a note goes out that says, we're amending form 42AB. And that's it.

ALIA: And did you get any confirmation that they amended it?

BOB: Um no is the answer to that. Nothing went out that said we're sure that Mr. Sullivan is not a deadbeat dad. But here's why that happens. That happens because people who are deadbeat dads, or people who do not pay their electricity bills are sometimes clever enough to change their middle initial or change their birthday in the hopes of avoiding something like this. So this is another information war and people who are landlords or maybe prospective daters or house sales or title companies do these over broad search to collect as much information as they can, hoping that they can catch someone who might be trying to evade a record. But in the world of guilty before proven innocent, they throw people like me in front of the bus just to make sure one of those dead beat dads doesn't sneak through.

ALIA: It's just awful and it feels like you have very little power.

BOB: So we live in this world where when you're doing transactions, people think they're entitled to know anything about you or anything that might be about you, which I think is the key word. If there are some mistakes along the way, so be it. That's how data brokers work.

ALIA: Let's take a break here, and check in on our data broker experiment

KELLY: Hey everyone! Kelly the producer, here to bring you the next installment of our Data Broker Experiment. If you remember, we've enlisted the help of two students from Duke University...thanks, Carter and Jake… to help us find out just how much information these data brokers have on our gracious volunteer, Keith, Spokes founder and president. And whether any of this information is *actually* accurate.

In our last installment, armed with just his name and his LinkedIn page, Carter and Jake began their deep dive into all things Keith Reynolds. And they ran into a *bit* of a roadblock when they realized there was more than one of him in Dallas. But not to worry, The path became clear thanks to the timely discovery of a Dallas Morning News article, which revealed his age.

So now we're gonna check back in with them and see what else they've dug up on Keith. And honestly, I'm super excited to hear what they've found.

KELLY: Next time, we will find out even more things about Keith, and bring in Keith Allen Reynolds himself to hear all about it

For all his problems with credit bureaus, Ed Mierzswinki from the Public Interest Research Group, seems even more concerned with these secretive companies that know so much about us -- even if we know nothing about them.

> ED: We, we know the credit bureaus, we know who they are, we know where they live, we know what they do. Uh, and we can regulate them. The law actually, for all its faults, it gives us rights against the credit bureaus. We can sue the credit bureaus and we can put them in their place.
>
> Now there are many, many, many credit bureaus who are, as I sometimes describe them, um, many big brothers. They're just all kinds of companies collecting information on the Internet today, and we don't know what they're doing. Nobody regulates them. Data brokers, uh, credit bureaus are a category of what are known as data brokers. Data brokers buy and sell information about people, not necessarily their customers, but people

ALIA: Okay, we already know that in the wrong person's hands, this information can be deadly. But are there examples of how our personal information can be used against us?

BOB: Yeah there's plenty of them. Here's an example from Alessandro Acquisti, the Carnegie Mellon professor who we met in episode 1. He ran a large but simple experiment -- he sent out thousands of fake resumes that were identical but for one thing. The fake personas he created had social media accounts; some of them were designed to appear obviously Muslim. Would these Muslim applicants suffer religious bias, just because of their social media presence?

> ALESSANDRO: in the case of the, uh, religious, uh, affiliation, uh, we did find differences, uh, particularly in, uh, in, uh, at the level of certain states, meaning at the nationwide level, the difference was not statistically significant. It was about 12% versus 10% or so call back rate for the Christian profile versus the Muslim profile. But when you start digging deeper, you realize that if you look at more conservative leaning states, you have a much larger delta, much larger difference in probability of callback, depending on religion. Essentially, we found out that the, the Christian candidate, uh, had six times higher probability than the Muslim candidate of being invited for a interview in the more conservative states. So this suggests that, um, uh, some employers are indeed using social media, uh, to in the, in the, in the or in the, in the process of, uh, screening candidates.

ALIA: Let’s let that sink in for a bit. In conservative leaning states, Christian candidates were six times more likely than the Muslim candidates to be called in for an interview. And this was just based off of their social media presences. Think about what could happen if these companies paid someone to get even more information about the candidates? This does not sit well with me--how do these people make money? Like who pays them?

BOB: Think of data brokers as the little fish in the ocean. They wouldn’t exist unless they were a part of an ecosystem that involves bigger fish, and bigger fish, and bigger fish. And the biggest fish of all in this system is companies like Facebook. Remember, Cambridge Analytica would not exist if it weren’t for Facebook. There was a time that people thought Facebook might actually be a leading voice about privacy issues. They went out and hired some really good people who were interested in privacy, people like Tim Sparapani who came from the ACLU. He served as Facebook’s first director of public policy. He says that programmers and executives at the time knew that Facebook could be used either as a force for good or as a force for mayhem. Sparapani felt that company was fighting the good fight until...well until Wall Street came calling.
.

> TIM SPARAPANI: And I think the third, uh, most, uh, relevant thing that happened that really changed the arc of the company and began to sort of, put pressure on, um, some of the protections we had put in place, really wise, the technical, legal and compliance protections we put in place. But the external and internal, both, um, transparent and, and opaque was the, the movement of this company from a startup to a publicly traded company. And I don't think it can be understated what enormous pressure that put on the company and how it forced the undoing of many of these protections as people began to see the, the raison d'etre of the company changed from being a thing which was designed to, it makes the world both more open and connected. That was its mission statement To Uh, uh, a thing which was both making the world both them are open and connected, but also making a lot of money and had to respond to the quarterly demands of Wall Street. And that pressure to begin to produce money and to show extraordinary economic growth.
> TIM SPARAPANI: Uh and value, uh, growth. Really pressed up against some of those protections which were designed to put in place long-term thinking, to put in place long term safeguards for the benefits of not only individual Facebook users, but groups of Facebook users around the world. I think you put all three of those things together and we begin to have a recipe for some of the, uh, consequential problems that have happened and that have played out in the, in the interim after my departure until now.

ALIA: Again, people volunteer information to Facebook. And, as Facebook is fond of saying in Congressional hearings, the company doesn't sell your data to third parties. They do share it, however. And critically, they match it up with other data to build an even more sophisticated profile of you. And they dance with the devil, er, data brokers.

BOB: Notice we are still talking about transactions. The information war in consumer markets. Buying shoes; buying homes, getting apartments. We now know that Facebook, data brokers, and microtargeting are regularly used by governments, too. This isn't just information war. It's a real war.

> TREVOR: I think what has changed because of Cambridge Analytica and because of election manipulation, because of some of the dark pattern behavioral manipulation that we see, um, fake news, uh, um, bots coming out of Russia and other places, we now recognize that our data can be weaponized in ways that may not affect us individually but absolutely have consequences, um, uh, to our societies in there for it sort of gets back around to us eventually in the form of harm.

ALIA: That's Trevor Hughes. He's in charge of the largest privacy organization in the world, the International Association of Privacy Professionals.

> TREVOR: I don't think we had the appropriate tools in place to manage it as it was emerging. And now that it's here, we are scrambling a bit to try to resolve those issues. I don't have a silver bullet or an easy answer or a quick solution for any of that. And that's what I struggle with at the family barbecue is that I don't have an immediate and quick answer

ALIA: It feels like we *finally* are realizing what now feels obvious: our data can and will be weaponized.

ALIA: So, mistakes were made. People knew targeting, tracking, data collection, could cause trouble. But advertisers wanted to make money. Software developers wanted to make money. Retailers wanted to make money. Consumers became...pawns. And democracy became...collateral damage in the information war which is now...a real war. But now, it seems, people are finally paying attention, the way people finally paid attention to the environment after the Exxon Valdez oil spill in the late 80's. Here's Christine Varney again.

> VARNEY: Yeah. I used to say we have to have our, we have to have an Exxon Valdez of privacy before people will start to pay attention to it.
> And then we would have these massive privacy breaches and yeah, people would pay attention for a day and then it would go away. So we don't know if we had our Exxon Valdez or we had so many that nobody, nobody cared anymore.

> VARNEY: It was for a long time, Bob, nobody was saying anything new about privacy. And we're finally at a point where I think people are saying, wait a second, this is serious. You know, there are massive abuses that can happen from these, you know, data, uh, practices that are allowed to proliferate across the internet. I think the wake up call for the United States may have been the Cambridge Analytica events that, in my view, completely swayed an election. So I do think people are beginning to understand

> that the lack of privacy has serious consequences, not only for us in our individual lives, but in our country and in the health of our democracy.

BOB: Cambridge Analytica...Is that the Exxon Valdez incident?

> VARNEY: It may be, you know, in retrospect that may be the one that, that kind of triggers, uh, the long overdue examination of, of how we cure this incredibly invasive, um, pervasive ability to collect everything that exists about an individual without their knowledge or consent and use it for any purpose

ALIA: Has data had its Pearl Harbor? Its environmental disaster? Depends on who you are. For Jessica Tunon, yes. She couldn't even run a business while on the run from her abuser, so you could say that's her Valdez. If you are a young person trying to get a job, and you can't because of a social media post, that's your Valdez. If you are Thomas Jefferson thinking about the democracy you've created, 2016 was your Valdez. If you haven't had your privacy Valdez moment, just wait. You will.

So, what I am wondering now is...can it be fixed?

BOB: Not without a lot of vision. And a lot of money.

Next time on No Place to Hide, we figure out how we can fight this information war, one step at a time.

If you like what you're hearing, head to Apple Podcasts and rate and review our show! We totally read those, and it helps people find us!

No Place to Hide is a Spoke Media production, brought to you by Intel.

It's hosted by me, Alia Tavakolian and Bob Sullivan.

It's produced by Kelly Kolff, with help from Reyes Mendoza, Tre Jones and our intern, Kendall Lake.

Our story editor is Carson McCain.

Today's episode was mixed by Alexander Mark.

Our head of post production is Will Short, who also composed our opening and closing themes

The songs you hear in this episode come from FirstCom.

Our executive producer is Keith Allen Reynolds, whose prior six addresses we now know but will not disclose.

Special thanks to the folks you heard today: Jules Polonetsky, Christine Varney, Peter Swire, Ed Mierzswinki, Alessandro Acquisti, Tim Sparapani, and Trevor Hughes.

Thanks for listening!