ALIA: A warning to our listeners. In this episode there are multiple references to violence and domestic abuse, so parts of it may be difficult to hear.

ROB DOUGLAS: Amy was this beautiful young, very innocent woman who was just at the age of 20, like most 20 year olds, her life was just getting started. Here we are 20 years later, she'd be 40 years old. She'd probably be a mother. She was pursuing a college education.-She was working part time, she was just on the dawn of her life, her adult life. She had all those dreams, the music she loved, having a car, everything else. And although I've seen pictures, my first introduction to Amy was her grave site**.**

ALIA: Amy Boyer might have been the first person murdered by the internet.

BOB:  And this fall marked the 20th Anniversary of Amy Boyer' death.

ROB: This was probably a good year or so later after her murder, there were still items on top of her grave that her brother had left, that other people in town would bring by and place there. And uh, I'm actually getting a little choked up here, but um, you know, it, 20 years later I'm 60, she'd be 40 and she never had that, and her mother never had that, and her mother has never gotten over this. And I don't think anybody who knows the case has gotten over it.

**[THEME SONG]**

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. Privacy has been in the news a lot lately. Facebook, Google, Cambridge Analytica, facial recognition, image tagging, surveillance capitalism -- these are all terms you've seen floating around the Internet. And if you're like me, you probably think privacy is important, but feel like you can't do much about it. But privacy isn't some esoteric idea, a first-world problem, a luxury, an annoyance. For some people, the threat to privacy means they literally have no place to hide and that can be a matter of life or death. Bob and I are always asking the question, 'who killed our privacy?', but this time we're investigating how a lack of privacy can kill us.

*SINZI: So I think what's happening now is it's getting really personal.*
*ERICA: I think it is incredibly exhausting*
*TREVOR: we now recognize that our data can be weaponized*
*ROB: it's actually obscene what you can learn about somebody on the internet.*
*MENNY: You can change the way people think. You can change the way people, feel. And you can change the way people view the world.*
BOB: Amy's death was cruel and gruesome. But it also captured the public's imagination because of how she was killed. Data was a willing accomplice to the crime.

ROB: On a Friday afternoon in October of 1999, a beautiful fall day, Amy left work with two of her coworkers. They walked down an alley discussing their plans for the weekend. Amy got in her car, Liam came driving up very quickly, put his car door to her car door and opened fire, firing 11 shots, 10 into Amy and the 11th into himself, killing himself alongside of Amy.

ALIA: Rob Douglas is a private investigator who served as a consultant and expert witness in the federal suit involving Amy's death. Investigating her murder still haunts him.

ROB: Amy Boyer was a 20 year young woman living in Nashua, New Hampshire. She was, uh, a college student. She was working in a dental office part time and unbeknownst to Amy, for more than a year, a former high school classmate of hers by the name of Liam Youens was stalking her. And he was documenting the fact that he was stalking her on a website, literally named for Amy Boyer to the degree that if anybody had googled Amy's name at that time, or done a web search for Amy's name at that time, they would've found this website where he in great detail was, page after page, photographs, the whole thing, documenting how he wanted to kill her, why he wanted to kill her, um, his devotion to the Columbine killers and other stalkers and killers. And in, in essence, a look into the mind of a very demented and evil young man. And in order to stalk her he needed some information, he wasn't sure where Amy was living. He wasn't sure where she was working. He was trying to figure out a place that he could kill her. And so he started searching online, and to quote Liam Youens, and he wrote this on his website, "it's actually obscene what you can learn about somebody on the internet."

ALIA: Amy Boyer's killer paid a data broker to find out where she worked. And that broker tricked her mom into coughing up the address by calling Amy's home and posing as a health insurance company with a refund for Amy that needed to be processed through her employer.

ROB: I can tell you I've thought about it a lot over 20 years, it has been the driving motivation of my professional life.I never forget about Amy, and I think it's going to take the murder of a very prominent individual. I think it's going to take somebody finding out that the way a stalker was able to kill a high ranking government official or someone else of tremendous prominence was that they obtained information in the same way that Amy's information was obtained. And then let's expand this out if we can Bob, then it becomes how as a society do we claw some of that back? I don't think we'll ever get it all back. The web is forever, but how do we start protecting our children and how do we start protecting maybe our grandchildren that aren't even born yet? How do we regain the hill of privacy? And I think the starting point is we've got to remember the Amy Boyers of the world. We've got to remember that we have a duty to her memory. And a responsibility to future Amy's to some young woman or young man who's out there as we speak, who is being stalked, who's being bullied, who's being harassed, and they don't quite know how their stalker, their bullyer, their harasser, or maybe their eventual killer got information about them. How do we retake that ground and start protecting people for the future?

BOB: How *do* we retake that ground and start protecting people for the future? I feel like that's the whole thesis of this miniseries. Rob Douglas is convinced that nothing has really changed in the 20 years since Amy's murder. If anything, things have become much worse.
Tech has made stalking easier. Spyware is cheap and easy to use. GPS gadgets can be snuck onto cars. Cellphones are easy to track.

ALIA: Yeah. Bob and I have spent the past six months talking to every privacy expert we could get our hands on, and it turns out, a lot of people are working on this problem, in all corners of the world, many with a LOT of urgency--I'm imagining Bob, it's kind of like the Race to the Moon in the '60s.

BOB: Yeah, that's exactly how this feels. It's like we have to get to the moon before the end of the decade, we have to solve this problem before we get to the next decade.

ALIA: Yeah, you can feel it. And our experts have given us a lot to think about. We've heard how dark the future can be -- let your mind wander into the world of robots and AI, as our experts do, and I think you'll find our very humanity, our free will, our ability to be creative even, is at stake. But, we've also heard about the powerful ideas that can turn this ship around and, hopefully, maybe, unleash the power of technology for good.

BOB: This is SUCH a crucial time. There are these new technologies arriving every day that are even more invasive. Alia, imagine a fleet of drones from your local government flying over your neighborhood and what that would do to backyard parties for example.

ALIA: That sounds like a sci-fi novel.

BOB: It's real. It's happening right now. Uh, but on the other hand, folks are working on and frankly having big fights about new laws and new technologies that are supposed to rescue us from this dark future.

ALIA: But before we get to that, let's begin with a set of people who can't afford to wait for Congress to act, or a startup to magically solve this problem.

JESSICA TUNON: Also going online, and doing a search on your first and last name, finding information about your home address or where you've lived or people who live with you over the course of your life is also online. So I've recently decided to pay a company to help me with that too, after the-- it's been over 10 years, still having my home address posted online.

ALIA: This is Jessica Tunon. After a difficult breakup and a subsequent move, she's spent the past 10 years trying to erase her digital breadcrumbs. And it's not going well.

JESSICA: The government in itself will post your home address online and that is due to their own regulations. When you do a change of address, um, if you do a permanent change of address, that information's also provided to others.

BOB: Jessica gave us a blow-by-blow account of step after step she had taken to erase her presence from the web, and you know, it feels dozens, maybe even hundreds of steps later, she's really no further along than she was when she started. And it's just a painful list to listen to.

JESSICA: You would go to different websites and every website's different. So different search engines will have different information. So when you think you've cleared it from one search engine, it looks like there's on another. And even sometimes contacting the, um, company that posted it, that can take upwards of six weeks and sometimes they repost it, which they've done over the years. So there's no real opt-out laws either cause some companies like data brokers will post your information, some of them will take it down the same day, some again up to six weeks. Some of them you have to actually write the better business bureau to have them taken down. But then again, you know, they'll post it up again, because the government republished it somewhere else.

ALIA: She asked her former boyfriend to stop contacting her, even took out a civil protection order. She's now a Washington D.C. based advocate for laws that protect women online. Still, she can't seem to stop the Internet from stalking her.

JESSICA: I thought, you know, mentioning that I would be moving to another state would make a difference. You know, I never went on Facebook. I never went on, um, Twitter really. I didn't do a lot of things, actually, online, um, due to privacy concerns in general. It just feels as though I'm not protected. Um, it feels like a lot of people are not protected, and why are we not protected by this? So I just feel like I'm constantly at a loss. Um, and who can I better speak to? What can I do? Or what, you know, kind of value I can give to others, letting them know what they can do? But all in all, it's just, just, it's a hardship having that, and also knowing that, um, again, this is my own personal thoughts on this, but the government is the one who is actually allowing it to happen.

BOB: Alia, I've been covering privacy for 25 years, and you know what?

ALIA: What?

BOB: I hate the word privacy. Because for people like Amy and Jessica, this isn't about privacy. It's not about some silly worry that a department store knows your phone number or a hacker knows your credit card number. It's about safety. It's about freedom. Imagine being on the run from an extremely dangerous person, going through the lengths to change your name even, just to feel safe, and then having it leaked online anyway.

ALIA: It’s so frustrating. Because, yeah, we live in a world where it's actually absolutely essential for some people to drop off the face of the Earth. I mean, it’s quite literally life or death. And so many people are forced to move and change their names to escape a violent former partner, and It can be nearly impossible.

ERICA OLSEN: There's very little that you can do anymore when you're trying to navigate this world. There's very little that you can do that wouldn’t possibly end up online.

ALIA: That’s Erica Olsen. She is the Director of Safety Net at the National Network to End Domestic Violence. She looks at how technology impacts the safety and the privacy of survivors.

ERICA: Um, so we have a relocation project. We work closely with the Greater Boston Legal Services, um, and an attorney there who is just a, a national expert in looking at, um, relocation and identity. And we've been working together for many years at specifically, um, on the challenges that survivors can face when they are trying to escape a partner and an abusive individual and they're trying to hide their identity and it can be extremely difficult. So, even if you're somebody who's attempting to stay offline, if you don't have a Facebook page, if you're not using any of that kind of social media, um, to connect with people, there's many times that you can't even, you can't even apply for a job without doing it online. Or if you try to register to vote. If you tried to get married, if you buy a home, uh, if you move to another state, but you have a job that requires, um, a license and that state requires that license to be publicly posted. All of that stuff now happens online. All of that stuff is now data and information about us that is being gathered and compiled and data brokers, uh, love to compile that and sell it very conveniently packaged to abusers. Um, so it's, sometimes it's just information that gets out in piecemeal, but comes up in a Google search.

ALIA: Sometimes, disclosure is innocent. A roster of parents at a school event ends up online. A tagged photo appears in social media. So you can imagine how taxing it would be to get all of this scrubbed. I mean, it really turns into a full time job. Bob, I think about what we talk about all the time, and that’s like, you know, this sort of problem I have with people tagging me on their social media without my consent, and how just sort of violated I feel. And I cannot imagine if I was a survivor trying to scrub my online presence, how tedious and almost impossible it would feel to have to get rid of all that stuff. Cause I don’t have control over everyone’s accounts.

BOB: To make it even worse, at least if they tag you, you know that it’s there. Let’s say someone puts up a photo of you and doesn’t tag you, so you never get an alert that it’s there. You might go on for years not knowing your photo is online, but your, your stalker might. So, this *is* all consuming. A victim who’s digitally on the run, so to speak, has to constantly hop out of the range of cameras at parties, plead with others not to use their names, and then hope they don’t miss anything.

ALIA: And that feels so unfair, right? Because you shouldn't have to disclose that you're a victim in order to protect yourself.

BOB: This is something that advocates call the disclosure problem. As in, victims constantly have to disclose they're a victim just to get people to stop violating their privacy.

ERICA: They have to constantly say, this is why it's important that my information doesn't go on your website. I have to opt out of this. And I'm just a really big believer that survivors shouldn't have to walk around disclosing to everyone. I've communicated with, with survivors over the years who have gone through that process. And, um, I think it is incredibly exhausting. It's just constantly challenging to try to stay on top of all the ways that our information is, is used and collected. And in this kind of, this digital world that we're now in, we take, uh, some of this information for granted.

ALIA: Domestic violence victims certainly didn't sign up to be the heroes in our fight for privacy, but many think solving this problem will go a long way towards solving the entire privacy problem. I mean think about it: if we make the world safe for people who need privacy to survive it'll ultimately be a better world for the rest of us, right?

BOB: Yeah, exactly. Privacy wouldn't have to be something we have to ask for. It would be recognized as a basic human right.

ERICA: I think that when we all start to become a little more aware that anyone around us could have a potential privacy concern, I think the more we really think about privacy and care about privacy and each other's privacy as the norm. I think that we'll be in a better place and we'll be protecting people cause I think, I think what we have to think about is when we are protecting everyone's information, when we are creating things from privacy from design, and then we are actively interacting with people's information in a way that is respectful to privacy and making sure that each person we're interacting with is in control of their own information so that we're asking for consent.

KELLY: Hey everyone, Kelly the producer here. So, you might have noticed, a certain someone… or *someones*... have come up more than once in Bob and Alia's discussion about the state of privacy. Data brokers. Those shadowy companies combing the Internet for our information and selling it for their own gain. But how do they work? And how much can they actually find on a person, and how accurate is it? We want to find out firsthand, but we also don't want to send ourselves into a state of pure hopelessness thanks to greedy companies with no regard for our personal information. So we thought we'd make a fun little experiment of it. And what's more fun than digging up dirt on your boss? So in an effort to learn more about how these data brokers work...and maybe gain a bit of leverage, we've volun-told Spoke Media's founder and president, Keith, to be our test subject in an experiment to see just what you can learn about a person through the Internet. We enlisted the help of two *surprising eager* students

from Duke University. And armed with as little information as possible on him, there gonna help us find out anything that these data brokers have on Keith, and how easy it is to procure it.

ALIA: Hi Carter and Jake, you've got Alia and Bob

CARTER AND JAKE: Hi

ALIA: Kelly and Bob feel free to chime in, but I wonder if you could both introduce yourselves, tell us where you're based right now, what it is you do at Duke, like what you're studying, and uh what you're doing for us.

JAKE: Alright, um, I'm Jake Statisky. I'm a junior studying public policy and minoring in computer science. I'm from Raleigh, North Carolina.

CARTER: Yeah I'm Carter Fornash. I'm also a junior, um yeah I'm at Duke studying public policy but I'm from the D.C. area originally. And um the project that we are doing, so we are essentially on a deep dive into data brokers to find out what information we can on Keith Reynolds of Dallas, Texas. And then submit takedown requests to see if we can get everything that we found scrubbed from the web essentially.

ALIA: So, quick question, what did you guys know about Keith Reynolds before you started this project?

CARTER: We knew his name and his LinkedIn page.

ALIA: Wow

CARTER: And everything he decided to put out publicly on his LinkedIn. And that's all.

JAKE: That's it

ALIA: Wow

BOB: So what's the first thing you did when you decided to accept this mission?

JAKE: Well actually the first thing we did was we decided to look on a couple of databases, we realized there was more than one Keith Reynolds in Dallas, and so we needed to find a little bit more identifying information. So Carter found an article from the Dallas Morning News um about him, and it revealed that he was 35. And that gave us, uh, something to work with from there.

ALIA: Wow I'm so intrigued I'm really excited to talk to you guys again and find out what you found. Uh, thanks you guys, thanks so much! We'll talk soon.

JAKE: Yes talk to you soon.

ALIA: Okay, bye.

KELLY: Next time, we'll hear what Carter and Jake dug up on Keith. And honestly, I can't wait!

ALIA: Bob, you know, I never really thought much about privacy until we became friends.

BOB: I'm sorry.

ALIA: *laughs* No, I'm glad for it. Because now I think about it more, and I think it's important that we think about it. But you know, okay so we're talking about companies packaging and selling our information, it's reminding me of the whole Cambridge Analytica election thing. And you know, when it happened, it was all a big deal and the media was really loud about it. But it was this big messy thing, and I'm wondering if you could sort of break it down and make it more concise for us?

BOB: Yes. At its core, the Cambridge Analytica story was this: There was this company of political operatives who wanted to micro target in huge elections, and they ultimately influenced both the Leave campaign in the UK and the election of Donald Trump. Cambridge Analytica basically stole a bunch of data from Facebook through a third party, and it, it affected about 87 million users. And they used that data, and it's really small, seemingly small things like what they liked or what photos they posted, and they put that all into a big computer algorithm and they spat it out, and they were able to essentially attack both the Leave vote in the UK and the Donald Trump/Hillary Clinton election in the US. By microtargeting in this incredibly refined way, they were able to manipulate huge swaths of people, doing what advertising does, but doing it in a much more powerful way.

ALIA: And why would they want to do that? Why would they want to micro target us?

BOB: Ultimately, for money. But they did it in a way that was against Facebook's privacy policies. Facebook gave the data to an academic. The academic gave it to Cambridge Analytica. And after all this came out, Cambridge, and then thousands of other companies, were cut off by Facebook. But what this really shows is how, you know, a simple like on Facebook, or a simple photo that you post can end up in the hands of an international company that's attacking democracy. And so, the exhaust of a small data act can become an enormous privacy problem and an enormous social problem.

ALIA: So, in addition to life or death for domestic violence victims, privacy is about...the future of democracy? It's about people's ability to think for themselves? Bob, what is privacy?

BOB: You know, this is why I said earlier that I hate the word privacy. Because it's such a larger concept than that. It's about all those things, and it's about much more. But, let me try, if I could go into storytime.

ALIA: Oh Bob, you know I love storytime.

BOB: Okay, so Rusty and I went across the country this year, as we always do, in our car.

ALIA: And just to remind everybody who's listening, Rusty is Bob's trusty golden retriever.

BOB: He's the best reporter I know. And we went to, one of the stops was in Laramie, Wyoming. Which is a, you know, kind of remote outpost in the middle of the country, in the middle of nowhere. And, um, and I go to a bar. Unusual for me. And--

ALIA: *laughs* Sarcasm.

BOB: *laughs* And started chatting with a young couple who were in there. Another unusual thing for me to do. And surprisingly to me, they were from Maine. And they were, uh, creative types, she had a nose ring, he had lots of tattoos. They were not what I expected to find in Laramie, Wyoming. And, uh, I of course made assumptions that all bad journalists make, and I said, oh, it must be really hard to move from Maine to Wyoming. That's, cause they're two pretty different cultures. And much to my surprise, they said, no, the people in Wyoming, in Laramie, have been incredibly open and friendly with me. Our car broke down on the first day, they came to help us. They helped us move in. But the one thing that they did, and the wife stressed this to me, was while they were incredibly kind and nice, nobody really asked us too many questions.

ALIA: Oh my gosh. Like nobody was noseying around as to why they moved there?

BOB: Exactly.

ALIA: Wow.

BOB: Everybody goes to Wyoming for a reason, and it's acceptable in Wyoming to not ask.

ALIA: Ahh!

BOB: It's like the anti-busybody state. And they had moved from New England where, at least her family, was kind of nosey. You know, she lived near her grandparents, parents. Everybody went to the same high school. Everybody up in each other's business. And these two young people loved moving somewhere where they could just go be themselves.

ALIA: Ahh!

BOB: And for me, privacy is really about being left alone so that you can explore who you really are. So you can make mistakes and not have mom and dad and grandma looking at you all the time. And I thought-- now she didn't use the word "privacy" once and this was the best definition of privacy I'd ever heard. You can thrive, you can really become yourself, you can be creative, you can try new things, in a world where you don't feel like somebody's looking over your shoulder. And I think, this is the most wonderful idea, that being left alone to become who you really are, is a central tenet of what privacy really is.

ALIA: So I love this idea that we're trying to define privacy. Like, privacy is not one thing. It's so many things. And it's kind of important I think that we define what those things are.

BOB: Yeah, um, and so I arrive at this, what I think is a profound definition of privacy which, after I've said all these words to you, eventually I'm going to come down to something like "privacy means being left alone." And I now realize all I've done is quote William Brandice from a hundred or so years ago in the Supreme Court, and that like, my very sophomoric opinion about what privacy is is just that.

ALIA: Okay, Bob - I want to introduce you to somebody who makes me think that being left alone is just the start of privacy. Menny Barzilay runs the Interdisciplinary Cyber Research Center at the Tel-Aviv University. And he told me this story that i think you'll get a kick out of

MENNY BARZILAY: Okay, so a short, a short thought exercise. So I'm telling it as a guy, but everyone can translate it to whatever they want. So you go with your girlfriend to the beach and you take those pictures with her and, and you're wearing your bathing suits and, and, and, and you're drinking and you're eating and you have all of those pictures and you, you take those 20, 30, 40 pictures and you put them on Facebook, you shared them. Up until that point, everything is, is great. But then the next morning you go to work, you entered the office of one of your friends and then you see that he actually printed a picture of your girlfriend in a bikini and he put it on his wall. And you look at him and you say, what's that? Why do you have a picture of my girlfriend on your wall? And he says, well, you publish it on Facebook because you thought people will enjoy watching this picture. I actually really enjoyed watching this picture. So I printed it out and put it on the wall. And you asked him to take it down and throw it away. And he says, okay, I didn't mean to make you angry, and he does that. And then the next morning you get to work. And now he didn't print anything, but he has a shortcut on his desktop. And when you double click the shortcut, you get this picture on Facebook. And you look at him and you said, come on my friend, we had this conversation yesterday. Why do you have a picture? Why do you have a link to the picture of my girlfriend? And he now, he's really confused and he says, I didn't do anything with this picture. It's on Facebook. So you tell this person, do you know what? Don't look on any pictures of my girlfriend. I don't want you to do that anymore. And he says, okay, I didn't want, mean to make you angry. He deletes this link. And then you next, the next morning you get to work. And you know what you're already angry. Cause you know that example's come in, in threes. So you get to this guy's office and now he's looking on your picture on your Facebook. And now this, it makes no sense. It makes no sense cause you feel

that you did nothing wrong. And yet something went wrong. And apparently that when we, when we publish something on Facebook, we publish it with a, a set of rules. There's invisible set of rules on how we expect people to behave with the information that we shared. Cause privacy is all about context.

ALIA: Okay, my head is spinning from that.

BOB: Yeah! Um, such a great story.

ALIA: What do you think about it?

BOB: Privacy is not about being left alone. Privacy is all about context. The rules are fluid.

ALIA: We also talked to Alessandro Acquisti, a professor at Carnegie Mellon, and he's done some amazing research about privacy. He's probably the leading academic. And what he had to say about privacy really blew my mind.

BOB: The stranger on the train story?

ALIA: Yeah, the stranger on the train story.

ALESSANDRO ACQUISTI: The fact that sometimes, before the Internet already, people could disclose exceedingly sensitive information about ourselves to a stranger they had just met on a train.

ALIA: Alessandro and his colleagues believed that people generally don't like to share sensitive information about themselves with just anyone. But it turns out that no, people love to disclose while simultaneously wanting privacy. Now, as Alessandro says, this may sound like a contradiction, but -

ALESSANDRO: Through my own experiments and studies, and those are many others working in this field, I believe that I started learning that it is not a contradiction. People are complex, people are nuanced, and we should not see privacy as, uh, the blockage of, uh, personal information.

ALIA: People WANT to share secrets. They get pleasure out of it. I mean, of course! They even want to share secrets with strangers.

BOB: This is sort of how confessionals work.
ALIA: You know, this reminds me of this website that still exists, but I think I learned about it in like middle school or high school. And it's called PostSecret.com, and Bob, have you heard of this website?

BOB: Yes!

ALIA: Okay, so you know that then it's a website where people submit their secrets via postcard in the mail. For strangers to see. Secrets like…"I like to walk upstairs when I'm not wearing underwear" OR "When I am really desperate I remind myself: I am a good person." OR "No one knows that I am not returning to my job after summer vacation"

BOB: So, Alessandro might say that PostSecrets.com is actually a good explanation of privacy. Privacy is not about hiding. Privacy is about sharing when you trust that your secret will stay a secret. Or remain within a tight group. Now, think about a time when you shared a secret with someone and they broke that confidence. They shared it outside the circle. Or worse, they did it to gain some advantage, like to cause trouble with a boyfriend or with family member.

ALIA: Oh my God, I'm thinking of something that happened in the 5th grade. So I was a real goody goody and I always studied really hard. But I once shared my test answers with a boy sitting behind me, and then this nosey girl was like, did you share your test answers? And I was like, yeah, but don't tell anyone. And then you know what she did, Bob? She marched up to our teacher and told her, and I got in trouble and I had to sit out of recess. And I was so mad!

BOB: *laughs* And you're still mad about it.

ALIA: I'm still mad!

BOB: Your privacy was violated.

ALIA: Yes! My 5th grade privacy was violated.

BOB: And it started when you shared. Um, why did she do this?

ALIA: Oh, she did it because I think she wanted to like, I think she wanted to tattle-tell.

BOB: And she probably gained some advantage. She felt like she was like saddling up to the teacher this way. Right?

ALIA: Definitely.

BOB: Yeah, yeah. So people share secrets all the time to like, break up lovers, or to gain favor with the grandfather for the will. Or, um, sometimes people violate privacy to sell a product.

ALIA: Sell a product?

BOB: Yeah.

ALIA: Like how?

BOB: Remember that Target story, where the firm figured out that a woman was pregnant and started sending mailers to her house, and that's how her father found out that she was pregnant?

ALIA: Oh my God, yes

BOB: Well this is the life we live right now. Author Shoshana Zuboff has called it surveillance capitalism. We go online and share secrets about ourselves to our circle of friends. Next thing you know, we're a product.

ALIA: Like I ordered a therapy book recently about something really specific, and now I'm getting targeted ads for like all these things related to this thing I'm dealing with.

BOB: That's awful!

ALIA: *sighs* It IS awful, and it feels like such a violation. But I mean, people are sharing these things, right? Like, I went and bought the book on Amazon. I mean, doesn't that mean that we don't care about our privacy?

BOB: I, I don't think so. So, this is where a lot of people will say, you know, if you cared about your privacy, you would have gone to a used bookstore and paid cash. Right? Screw that. That's unrealistic. But also, in truth, most people live what a lot of experts call the "privacy paradox."

LARRY PONEMON: So I think we have a bunch of people, we'll call it the privacy paradox, where good people will basically say that they care about their privacy, but there is evidence that suggests that they do not do anything to protect the personal information.

ALIA: That's Larry Ponemon. He has been doing consumer research for decades on privacy and what people call now the privacy paradox. Consumers say they care a lot about privacy, but will hardly lift a finger to actually protect it.

BOB: Larry breaks people into three groups: One, the privacy neutral -- that's the "I have nothing to hide, so I don't care group." Two, The privacy-centric, and those are people like me, who argue every time someone asks for your phone number, or won't use E-ZPass, and use disposable credit cards. So, those are the privacy-centric. And three, is the group in the middle, he calls them privacy sensitive. I think that's kind of a generous title for them. These folks *say* they care, but don't do anything about their privacy. This chunk, that middle chunk, makes up about two-thirds of American consumers. And that number has surprisingly stayed the same throughout the years.

ALIA: I would've thought that would have shifted way more dramatically than it has!

BOB: Sure, especially with all the news about privacy. But in truth, people who say they have nothing to hide and people who want everything to be hidden, there's only 1 or 2 more percentage points, according to his research. Even in the past decade.

ALIA: Wow.

LARRY: It was at the RSA conference many years ago and someone was, you know, one of the researchers I suppose was standing on a street corner saying, you know, they will give you a Starbucks coupon for 15 worth $5 even $15 for the $5 El Cheapo payment. Right. And would you, they basically give me your social security number and it's like most people say, okay, I like Starbucks. You know, I'll take your $5, gift certificate. And here's my social security number.

BOB: When we talked to Larry, I called his privacy sensitive group the lazy group. And yeah I know that's a bit unfair.

ALIA: Yeah I'm really glad to hear that you think that's unfair, because I feel like I fall into this group a lot of the time. But it's not that I'm lazy, it's just sometimes it feels so futile to do anything about my privacy.

BOB: It is! It is really really hard, in fact it's down right impossible to take charge of your digital privacy in meaningful ways. And when the world is basically friendly to you, when it feels like you are getting free coupons or a slick app that helps you park or pay bills, well that's ok.
But, as we all know, the world isn't always friendly. Canadian privacy lawyer Sinziana Gutiu grew up in Romania. She's seen first hand what happens when governments know everything about what people are doing inside their homes.

SINZI GUTIU: Like there are stories of my parents' friends telling on other people and then just disappearing. They would have to huddle and listen to foreign radio, um, to get access to cool music. And, uh, so all of that, you can, you can see how, uh, it's like the 1984 the book. Um, those are examples of what it was, what it was like and what it could be again, and we want to learn from past experiences, right? I mean, this is why Europe has such a different view on privacy. So I think what's happening now is it's getting really personal. It would be the equivalent of, you know, every single member of your family and all of your friends being part of the Soviet regime and telling you stuff. And so I think it's, it's a lot more personal. It's a lot more intimate. And again, if we think about people going with their gut or with what are their best friends says, I think that's very dangerous to still have your own original thought and your, and your own critique. And think critically about what's happening around you.

ALIA: So, privacy is about...your ability to have original thoughts, to think critically. Wow.

BOB: Yeah, that was...that was just chilling when she said that. I was sitting across the room from her.

ALIA: Mm.

BOB: I mean, dangerous to have your own original thought. Feels very George Orwell. Very 1984, right?

ALIA: Oh my god yes.

But what if the thought police weren't a government? What if it were a corporation? Or one that's acting like a government? Or an unregulated entity vacuuming up everyone's data?

ALIA: Like Cambridge Analytica.

BOB: Like Cambridge Analytica. Or one of hundreds of other companies doing essentially what Cambridge Analytica did during the election, but they're doing it all the time. Every day vacuuming up everybody's data, all the time. They are called data brokers.

ALIA: Aha and so these are the same companies that made it possible for Amy Boyer's killer to find her.

BOB: Right.

ALIA: And the one thing that's come up again and again, Bob, as we interviewed people was this problem of data brokers. I mean who are they? How do they know so much about me? It seems like they have eyes everywhere. And who's keeping an eye on **them**?

BOB: That's a subject which requires an entire episode, Alia.

ALIA: Next time on No Place to Hide, we tackle what went wrong with privacy that led us to where we are today, because it definitely didn't happen overnight.

CHRISTINE 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.
BOB: We should also note that No Place to Hide is the name of a great book written by Robert O'Harrow, a Washington Post reporter, back in 2005. Hopefully we're picking up where he left off.

ALIA: If you or a loved one have experienced or are experiencing domestic violence, you can call the National Domestic Violence Hotline at 1-800-799-SAFE. That's 1-800-799-7233. You can look at our show notes for an extensive list of resources. 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 which we should mention has no editorial control over this podcast.

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.

Today's episode was mixed by Alexander Mark.

Our story editor is Carson McCain.

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 yes the same Keith Allen Reynolds who also graciously agreed to let us hack his life. Thanks, Keith.

Special thanks to the folks you heard today: Rob Douglas, Jessica Tunon, Erica Olsen, Menny Barzilay, Alessandro Acquisti, Larry Ponemon, and Sinziana Guitu.

Thanks for listening!