EPISODE 3: A dark future, a reasonable hope

BOB: Alia, I'm going to ask you a potentially embarrassing question.

ALIA: OK?

BOB: Embarrassing for me, that is.

ALIA: OK? I'm ready

BOB: Do you know what an unlisted number is?

ALIA: I know that an unlisted number is a result of someone who made a conscious choice not to list their number/identity.

BOB: Great! So you know what a phone book is, too

ALIA: BOB!

BOB: Sorry, sorry. That's not my point. My point is - ~~did you hear what you just said?~~ You PAID the phone company to keep your number unlisted. PAID them. For privacy. So if you were person worried about creeps, or you had nasty neighbors, or you just wanted to be left alone, well there was a monthly fee for that.

ALIA: monthly fee to be left alone - kinda reminds me of Jessica Tunon, right?

BOB: Yes Jessica Tunon , who we met in episode 1, ~~The woman who~~ has spent a decade trying to keep her personal information off the Internet to avoid contact with an ex -- trying to get "unlisted" by the Internet. Her privacy tax is punishing. She gave me a spreadsheet once to describe it (I read a bit...leading into her)

> TUNON: And um, having a home and purchasing it on your own, also the um tax office will post your home address online. And, and finding out about all these different things you can, um, protect yourself by paying a fee, so paying a fee with having a website, which I do have, so paying it for your hosting company. Um, if you want a VPN to feel more protected, there's a cost to that. Having a PO box to not have your home address, um, posted. So I also have, um, three registered trademarks, the U.S. PTO Office. So having that, um, po box listed instead of home address or paying a registered agent, um, which is an annual fee of about a hundred dollars a year. So. Having a PO box I think is like a $300 charge a year.

ALIA: So she's like paying for protection

BOB: Do you know what we would call paying for protection? Extortion.

ALIA: I'm Alia Tavakolian

BOB: 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. Over the past two episodes, we've learned that privacy is a serious issue, so serious it can mean life or death to some people. We've learned that corporations and congress have pretty much sat back and done next to nothing to address privacy. Today we're going to talk about what can be done now that we're here?

As we learned in episode 1, Jessica and other people like her are at war. And in episode two, we learned America's at war. But where are the bullets? Where is the damage? Well, we know this war has sown a lot of seeds of distrust in our democracy -- in democracy around the world. But that might be nothing compared to what's coming.

> BARZILAY: So the future of AI and privacy is to me very, very dark. Um, cause the question is, um, who are you? Um, are you the sum of your thoughts or the sum of your decisions or the, sum of your, um, emotions? What if you will discover that all of those things can be easily changed through technology.

BOB: We met Menni Barzilay in episode 1. He talked to us from Israel. His example of privacy problems are stark, and remarkable and, well we'll let you judge.

> BARZILAY: And again, we witness cases where companies and other entities prove that by using technologies together with sophisticated enough algorithms, you can change the way people think. You can change the way people, feel. And you can change the way people view the world. And now you have a system that is able to learn by itself. You give it data and you connect it to platforms, again, like Facebook, Google, and others that allow you, allow a third party like the system to show us information and check what does this information make us do? 38:12 what kind of a decision we're making when given this information. And when you connect those new types of algorithms, what you get is a system that will be able to develop um algorithms that will allow us to change the way you think and the way you feel with a very high level of, accuracy.

BOB: "Change the way you think and the way you feel with a high level of accuracy." My Goodness.

ALIA: That's really scary.

BOB: I'm not sure that was as scary as the Gorgon stare thing though.

ALIA: Oh God, the Gorgon stare, that was like the ultimate no place to hide moment

> VERDI: Sure. So, so there is, um, there is a technology called Gorgon Stare, uh, which is an aerial based camera system. It's typically used on blimps, which can stay up in the air for a really long time.

ALIA: This is John Verdi, he's the Vice President of Policy at the Future of Privacy Forum. And this stuff he's about to talk about with the Gorgon's Stare sounds like something out of the Marvel Cinematic Universe. It's insane.

> Um, and this technology was developed for use in theaters of war. It was developed, I believe originally, um, for use in Iraq. Uh, and the multiple cameras that are attached to this data platform that is attached to a blimp, um, are used to algorithmically analyze pedestrians, cars, cyclists, scooters, um, any vehicles or individuals who are moving around on the ground. Um, it collects and retains that information pretty much indefinitely. And it can be used to more or less track individuals or individual vehicles consistently over time and in a war atmosphere, one can imagine the useful, uh, reasons for doing this. Right? You would want to track enemy troop movements.You would wanna identify suicide bombers. Um, you would want to try to do all sorts of things um, that would be helpful when you're in a wartime environment. I think the thing that's really troubling about this technology is that some police departments in the United States have either brought it back home for use in American cities and communities or they are proposing that they do so. And it's this kind of pervasive, precise, comprehensive surveillance of everybody's movements that I think should raise real alarm bells for individuals, particularly if they're in a community where the law enforcement agencies are proposing to use this technology.

ALIA: Bob. This was supposed to be a podcast about privacy. Now it's kind of about ...Big Brother?

BOB: A strange question at this point: What is privacy? I have a long list from all our guests. Privacy is: Safety. Freedom to think. Free will. Protects minorities. Ability to be creative. Freedom from being watched. It's a statute of limitations on mistakes. It's freedom from Big Brother. It's the cause of the American Revolution. And, as Menny points out, it's really the essence of who you are.
~~What it's not?~~ And it's not what 2018 Bob thought it was. it's not the right to NOT share. It's the right to control the context of sharing. It is in fact the right TO share, to have confessional boxes all around your life.

> ALIA: Speaking of the essence of who you are - let's check in on our data broker project. We're about to reveal to Keith Allen Reynolds all the dirt we dug up on him. It's not quite a Gorgon Stare, but it's close.

ALIA: Bob, as we've been working on this, I've of course been thinking a lot about how I can protect my own privacy. And maybe I've found it! Or, Joel Stein found it. This is from his interview with CBS back in August:

Joel is a Bloomberg reporter who set out to confuse any and everything meant to track you. And in order to do that, he actually fought gadgets with gadgets.

He bought a shirt covered in license plates to confuse license plate readers. He hired someone to erase all his web and social media history. He even bought a mask to wear on his face everywhere to foil facial recognition systems!

BOB: Those are … things you can do. I bet that mask would get hot though.

ALIA: Okay, well fine. What are some more *practical* things I could do?

BOB: Stop giving your phone number out at stores, or at least use a fake one / disposable one (you can get one from Google!).

ALIA: Oh yeah! Bob you taught me to do that and now I feel SO empowered by it.

BOB: And I'm so glad! Other things you could do: come up with a burner email address when you sign up for things. Limit the number of places you register. Using a password manager, or very good passwords. Patronize sites that use tokens instead of store your credit card.

Those things can work, but in truth, they just kind of eat around the ends of the problem. It's society -- all of us, the tech companies, governments, people -- we all have to come up with the answer. And, yes,people are trying. For example, the state of Vermont just required data brokers to register and essentially get a license. That should help clean up the industry a little. And, as you've probably heard after Facebook, and Equifax, and all those other hacks, there is finally a lot of push in Washington DC to create a federal law dealing with the issues.

ALIA: But it's an uphill battle.
Becky Richards is the chief privacy officer at the NSA, which to me sounds like the hardest job you could have in privacy.

> BR: When companies and organizations are starting to fill a space that has historically been in the, in that public sphere, I think that's a place where we really haven't figured out how do we do this in a democratic process. Do we want these companies setting up what looks and feels a lot like a judge and a jury, but they get to choose who it is? Or do we want to go back and think about, no, actually this really should go back into too, that

> governmental space. You know, we're, you know, we're a government by the people of the people, for the people and we want to make sure it's representative of those people.

ALIA: The challenge begins because companies like Facebook have become so large, and so powerful, that they are functioning like governments now. People can file a Freedom of Information Act request with the NSA. They can't do that with Facebook.

Talk like that has a lot of people calling for big tech companies to be broken up, that they are too powerful. That would be long term fight

BOB: I was covering Microsoft in Redmond during the last big tech antitrust trial. That got ugly, and it did take years.

ALIA: But Christine Varney, the former FTC commissioner turned antitrust lawyer from episode 2 thinks there *are* things Congress could do to act now.

> BOB: Okay. So, so outside of the breaking them up solution, which is hard to, to not see as a pretty blunt tool, uh, what kind of things could congress do or could states do that would actually, if not clean up the whole problem, at least move in the right direction.
>
> VARNEY: They could pass a very straight forward law that says you cannot collect any data other than the data provided for the purpose, uh, which, uh, is clearly intended, it's clearly intended use. So if I'm buying something on Amazon, you can't use that data for anything other than to fulfill my order. If I'm using Google email, you can't use my email address or anything in my email, uh, for anything other than delivering my email. I mean, just, I don't think we need to overcomplicate this. I think you pass a very straightforward law.

ALIA: That sounds pretty simple. Data can only be used for the reason it's collected. I use an EZ Pass gadget to pay a toll, the highway gets to take my money and that's it. They can't sell or store my location information

BOB: I like this idea too, but not everybody does. Imagine your child goes missing, and toll booth data could help find him. Now, don't you want that data to be used for additional purposes? Or, what about research? What if toll booth data could help smart cities make a plan that would cut traffic and emissions? What I'm getting at is, there would have to be exceptions.

ALIA: You're so right. Okay so I've heard that a federal law has actually been put on the table, and tech companies are the ones backing it.

BOB: Yes, the Business Roundtable. It's a group that includes Amazon, Dell, IBM..a lot of heavy hitters. They sent a letter to Sen. Mitch McConnell saying they support "a comprehensive

federal consumer data privacy law to strengthen consumer trust and establish a stable policy environment in which new services and technologies can flourish."

ALIA: We should note here that our sponsor, Intel, did not sign the letter.

BOB: It's a good thing they are calling attention to the need for better rules. But consumer advocates say this could also be a bit of a Trojan horse.

> ED: And the first thing the companies want is a privacy law, quote unquote, privacy law, that says everything you companies are doing, keep doing it. Don't ever change.

BOB: This is consumer advocate Ed M again

> They want to legalize everything they're doing without giving consumers any new rights. And those rights that we want, uh, we want the right to sue companies that harm our privacy. That's off the table for the companies. Uh, we want, but the most important thing, as somebody that's been doing this work at both the state and the national level, all the good ideas I've ever seen, come from the states. That's why industry wants to preempt the right of state governments to pass stronger laws. Because all the good ideas come from state governments. Industry doesn't want any new good ideas. They want to perpetuate their right to run roughshod over Americans, over our privacy. Uh, disrespect everything we do. And so preemption, uh, and the right to sue companies, ~~Congress is going to~~, if the industry has its way, Congress is going to pass a law that says, you can keep doing everything you're doing consumers don't have any right to sue you

BOB: So the federal law Ed is worried about would actually, essentially, invalidate that Vermont law I mentioned earlier that forces data brokers to register. So Ed... really wants this federal law to fail.

> ED: The best opportunity I see is that it collapses of its own weight. And we still have the states leading the way. The states are where the good ideas come from. Congress never acts to protect consumers unless there was a disaster, or unless the states show the way. 2008, the entire financial world collapsed. And it was because of overreaching by Wall Street, uh, who thought they were the masters of the universe, et Cetera, et cetera. It took us years to climb out of the mess that the banks brought on us

BOB: So Ed is comparing Cambridge Analytica in the privacy world to the collapse of the housing bubble in the financial world. The collapse of the housing bubble led to the creation of the Consumer Financial Protection Bureau. And we might need something as bad as that in the privacy world, to create a federal agency with real teeth, to actually enforce privacy laws.

ALIA: Bob, what's our reasonable hope?

BOB: I'm glad you asked that. Not surprised, but I'm glad.

ALIA: I actually thought Trevor Hughes, from the Future of Privacy Forum, had some hopeful things to say. He said privacy is just…..going through a phase.

> HUGHES: look at some of the media and magazine covers today, they often say things like, your privacy is gone. You should get over it, or privacy is dead. Not so. Absolutely not so. Uh, my argument would be that privacy is doing what privacy has always done and that is change its form and shape, adjust to new technological mediation that has occurred, um, and adapt so as to protect this fundamental human truth on a going forward basis. What that also means though is that our laws and policies that we create to manage privacy must never be static. So we shouldn't hope for the single perfect solutions to managing privacy. And we shouldn't ever think that if we pass a law, it's one and done, um, that is never going to be the case year by year, decade by decade, generation by generation. We are going to have to go back and revisit these things to make sure that they're keeping up with what society expects in the current technological context and environment in which we find ourselves in to protect privacy.

BOB: Remember Sinzi Guitu, from Canada? She's in an interesting spot because Canadian privacy rules are kind of in between European laws and US. laws. Her perspective is important; she thinks people have a bad habit of seeing this issue in black and white. Innovation vs. privacy. Consumers vs. corporations. George Jetson Gadgets vs George Orwell surveillance. But it doesn't have to be that way.

> SINZI: Because put simply, privacy means don't share. You know, this is kind of the elementary understanding of privacy. Don't share, keep it all to yourself. You know, being left alone. And so the conflict is if you, if you're trying to be left alone, how can you engage in society and how can you be a meaningful member of society and how can you, how can we make use of your data, what you're doing, of what you're thinking and give you better healthcare, give you cool, important products, increase accessibility for you.
>
> SINZI: So I think that's how it was traditionally thought. But I think now that view has changed. And you know, many companies say we care about privacy, but it goes back to what you're saying. What do they mean by that? Facebook was in court in the states recently and their lawyer made an argument that when people sign up for Facebook and they post something, even if it's to a small group of friends, they're publishing, that is public. And intuitively the judge said, how can you have that? It's not so black and white. Like they're sharing it with a select group of people. They're not sharing it with the world. And the lawyer, and I'm not a US source, I don't know if what they're saying is really

correct, but they said this is, this is privacy. If you're publishing something, if something meets the definition of publishing, it's out there.

SINZI: 28:17 And this is what privacy is. It is all or nothing. You either keep it or you don't, which is a really, I think it's wrong, but it also archaic way of thinking about what privacy is. It's nuance. You can certainly have privacy in public.

ALIA: You can have privacy in public. Well, that's not what I expected anyone to say during this podcast.

BOB: ...this is a very nuanced thing...

HUGHES: Fundamentally. And one of the things that I hearken back to is that we are 250 years into the industrial revolution. And as societies around the world, we are still grappling with the consequences of the industrial revolution.

ALIA: That's Trevor Hughes again

HUGHES: Let's put an easy one on the table. The environmental movement exists because of the effluent of the, of the industrial revolution. So in many ways we are dealing with the societal and environmental consequences of the industrial revolution through our environmental efforts. And if we think of the rise of environmentalism since they, Rachel Carson wrote Silent Spring and other early environmentalists emerged in the US and elsewhere. Um, there are a vast and complex array of solution sets that have emerged, technologies, laws and standards, broad consumer and citizen awareness and understanding. If there is a blue plastic bin in your office or in a place that you are visiting a coffee shop or something, we have now been, um, uh normed in time understanding that that's usually the recycle bin.

HUGHES: We are on the same kind of education and normalization curve, normative curve, um, in the digital economy. So if we look back to the industrial revolution and think of how it revolutionized not just the way goods and materials were manufactured, but also how it revolutionized society. It's not just environmentalism, it's public school education, a standard work week, the idea of holidays, the idea of women's suffrage emerged largely out of the industrial revolution, um, the idea of a childhood and child labor laws emerged out of the industrial revolution. Society was forever changed by the industrial revolution. It has taken us 250 years and we still have not fully resolved all of the societal issues that, that revolution created for us. We are probably 25 years um, you could argue into the digital revolution and we have just begun to tackle some of the big societal changes.

ALIA: If you look at it that way, we are just at the beginning of this discussion. LIke if this were the industrial revolution, we would be in the late 1700s in Great Britain.

BOB: Yes! Alia And you would be William Wordsworth, writing about alienation from nature. The French Revolution would be hanging in the air. Err...I shouldn't have used that word. Napoleon would still be ahead of us...I'd better stop this.

ALIA: I do really appreciate the perspective though. Every age is arrogant about its own time, thinking its so important compared to the past or the future. So perspective is good.

BOB: On the other hand, I don't think we can afford to slow walk any of this. The crisis is here; there is near and present danger. We'd better do something soon.

> SPARAPANI: There is a vast dangerous ecosystem of some four to 6,000 companies depending on how you count, that fit this need, this notion of what we call data brokerage that are, existing only to buy and sell data about people.
>
> SPARAPANI: And they create, uh, a commodity, uh, about each and every one of us that makes every bit of information about us something that can be bought and sold. And what's the price tag on all of our personal information. It takes that information and packages it, uh, in all sorts of ways to be sold instantaneously to anyone who wants to buy it. And it facilitates all sorts of, uh, ongoing privacy, um, interventions in our life and, and frankly, privacy invasions in our life, some of which are particularly damaging. Uh, if Congress where to stop and regulate data brokerage, we would do enormous good for the American public and advancing their privacy.
>
> SPARAPANI -- I think this is a dangerous moment. I think that Congress should step into the breach and should do something...

BOB: We're at a dangerous moment' I really agree with what Tim Sparapani said. Artificial intelligence is about to get very good at predicting who might attend a protest rally, and allow governments to arrest people before the rally even happens. Algorithm bias is here, dictating where people can live and go to school. Manipulation on a grand scale, on a nationwide scale, is here. Sinzi even talks about a threat to free will. If we don't act, people in the future -- not next century, next decade -- are going to look very poorly on us.

ALIA: We'll explore more about what AI, robots, and the Internet of Things might mean for privacy in the next installation of this miniseries. But as we wrap up this season, Bob, what's *your* reasonable hope?

BOB: My reasonable hope. And it comes from history too. My favorite author is Thomas Cahill, who has this wonderful series of books called Hinges of History. He picked various critical points in humanity – the European Renaissance, the rise of Greek culture, the 'Gift of the Jews' – and most important, how ordinary people made critical decisions at crucial times and in many cases, saved societies from self-destruction. My favorite, of course, is "How the Irish Saved

Civilization," which is about an anonymous band of monks in Western Ireland who fastidiously and painstakingly copied and saved Greek literature from destruction – while the rest of Europe and European libraries were being burned. I like to think Cahill, or someone like him, will write another Hinges of History volume about our time.I think there won't be one hero who sets us right in this tech mess we're in right now. I believe there will be many. We all have to do our part. And that begins by caring.

CREDITS

ALIA: This was the final episode of this arc of No Place to Hide. But don't worry, we aren't done yet! In the next installation we tackle what will happen to the future of privacy. Stay tuned for that in 2020.

While you're waiting, why don't you head to Apple Podcasts and review our show. Drop us some stars if you're really feeling it. It helps people find the show.

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 - the one, but not the only.

Special thanks to the folks you heard today: Jessica Tunon, Menny Barzilay, John Verdi, Christine Varney, Becky Richards, Ed Mierzswinki, Trevor Hughes, Sinziana Gutiu, and Tim Sparapani.

And lastly, Thanks Tori Ano for recording us in DC, and watching dog videos with us on our lunch break

Thanks for listening!