THE BROOKINGS INSTITUTION

BROOKINGS CAFETERIA PODCAST

HOW DIGITAL PRIVACY LAW ASYMMETRIES CAN HURT CRIMINAL DEFENDANTS

Washington, D.C.

Friday, June 5, 2020

PARTICIPANTS:

Host:

FRED DEWS
Managing Editor, Podcasts and Digital Projects
The Brookings Institution

Guests:

JOHN VILLASENOR
Professor of Electrical Engineering, University of California, Los Angeles
Nonresident Senior Fellow, Governance Studies, Center for Technology Innovation
The Brookings Institution

REBECCA WEXLER
Assistant Professor, Berkeley Law School
Nonresident Senior Fellow, Governance Studies, Center for Technology Innovation
The Brookings Institution

ALEX ENGLER
David M. Rubenstein Fellow, Governance Studies
The Brookings Institution

* * * * *

P R O C E E D I N G S

DEWS: Welcome to the Brookings Cafeteria, the podcast about ideas and the experts who have them. I'm Fred Dews. Imagine, if you will, a defendant in a criminal trial is accused of, say, threatening someone over a social media app. The prosecution can subpoena digital records from the social media company to build its case against the defendant.

However, evidence that would prove the defendant's innocence is also held by that company, and yet defense investigators are unable to obtain it due to the way data privacy laws are currently written. In this scenario, a privacy asymmetry exists between prosecution and defense that could keep an innocent person in jail.

Rebecca Wexler, a law professor at the University of California Berkeley School of Law, has identified and studied this privacy asymmetry and has suggested how legislators can fix data privacy laws to address it. On this episode of the Brookings Cafeteria, Wexler is interviewed about her research by John Villasenor, a Brookings nonresident senior fellow. Together, Wexler and Villasenor wrote a piece on the TechTank blog at Brookings.edu titled How well-intentioned privacy laws can contribute to wrongful convictions. Wexler also has a forthcoming article in the UCLA Law Review on this topic.

Also in this episode, in a new Coffee Break segment, meet Alex Engler, a David M. Rubenstein Fellow in Governance Studies who examines the implications of artificial intelligence and emerging data technologies on society and governance.

You can follow the Brookings Podcast Network on Twitter, @policypodcasts, to get information about and links to all of our shows, including Dollar and Sense, the Brookings trade podcast; The Current; and our Events podcast. And, now, on with the interview. Here's John Villasenor with Rebecca Wexler.

VILLASENOR: So, thank you very much, Fred. And, I'd like to welcome Rebecca Wexler who is a nonresident fellow in Governance Studies at the Center for Technology Innovation at Brookings. And, she's also an assistant professor at Berkeley Law School where she teaches, researches, and writes on issues concerning data, technology, and criminal justice.

Her work focuses on how the rapid deployment of artificial intelligence and other data-driven criminal justice technologies affect the relative power of law enforcement, to prosecutors, and criminal justice attorneys. And, prior to joining the faculty at Berkeley, she held several federal court clerkships and also worked as a Yale Public Interest Fellow at The Legal Aid Society's Criminal Defense Practice. So, I'd like to thank you very much for coming on the podcast to talk about this important topic today.

WEXLER: Thanks so much, John. Thanks for the introduction. And, thank you, Fred, for having us here.

VILLASENOR: So, the first question I have is, the intersection between criminal defense and digital privacy is an area that, prior to your pioneering work, hadn't gotten nearly the intention that it deserves. At a very high level, can you explain the concern that you have focused on?

WEXLER: Sure. Yeah. And, so, you're right. When we think about privacy in the criminal justice system, we usually think about law enforcement surveillance, law enforcement tracking. But, criminal defense investigators also have to engage in investigations, and so, that can raise some similar tensions between privacy, truth, and fairness in our criminal justice system.

So, the specific problem I've been most concerned about right now is a troubling pattern in data privacy laws. Data privacy laws are well-meaning. Legislators want to protect consumer

privacy as we have this data-driven economy, and companies are collecting information about our heartbeats, about our movements, our communications.

But, what happens is that law enforcement lobbyists are exceptions to those privacy laws, so that police can continue accessing sensitive information. And, few, if anyone, lobby for defense investigators to have similar access to the same sensitive information. So, this causes a troubling, foreseeable, almost certainly unintentional pattern where data privacy laws end up giving law enforcement more or better access to evidence than they give to criminal defense investigators.

The good news here is that there's actually an easy fix, and John and I are co-authors of a short piece on this for the Brookings blog. And, the fix is, look, at the end of the data privacy law you can put a savings exception. It says something like nothing in this act is supposed to prohibit compliance with otherwise valid legal process, like warrants for law enforcement, subpoenas for investigators. And, if legislators do that, the key point is they're not creating a privacy vacuum.

Having that kind of symmetrical, neutral exception would just open up the privacy law onto the baseline procedural protections for privacy that are already built into the criminal justice subpoena and evidence rules. So, that's the problem I'm worried about, and the good news is there's an easy fix.

VILLASENOR: Great. Well, that sounds like a really important problem. One of the themes of your work is that, absent the kind of solutions that you mention, there is this enormous asymmetry between state power on the one hand and criminal defendants on the other, and that's obviously highly prejudicial to defendants who are trying to get access to exculpatory digital records. Could you explain a bit and maybe provide an example of a case where this actually mattered?

WEXLER: So, let me start with a case, actually. A friend of mine who's a defense counsel at The Legal Aid Society of New York City had a client who was actually jailed when a complaining witness showed police, on her cell phone, text messages and voicemails that this client had allegedly sent to her in violation of a protective order that had been issued in family court. The client insisted that he was innocent, that he hadn't actually sent those text messages and voicemails. And, Jerome Greco subpoenaed a technology company called SpoofCard which offers a consumer service that allows users to send messages or place phone calls that look like they're coming from somebody else's phone number. And, he was actually able to obtain records that proved that the complaining witness in this case had sent those messages to herself in order to falsely accuse his client.

So, when he showed those records to the prosecutor, the prosecutor dropped the case and the client was released from jail. But, the key point here is that if defense counsel had been unable to subpoena the technology company for those records -- and the records weren't the client's own records, they were records generated by the witnesses use of the service -- if a privacy law had stopped defense counsel from subpoenaing those records, that client would still be wrongfully incarcerated today. And, that's unfortunately what some privacy laws are doing.

So, a case where defense counsel was blocked from a similar subpoena for potential exculpatory evidence -- I can tell you about another case, came out of San Francisco. A friend of mine who's a defense counsel there had a client who was caught on surveillance camera shooting at an SUV, and his argument was self-defense.

A man inside the SUV 6 months earlier had driven by and actually shot at him and his friends in an attempted murder. That attempted murder was investigated by the police 6 months earlier, but they hadn't caught the perpetrator. And, the man over the next 6 months used

Instagram to send death threats and harassing messages to the client, leaving him in constant fear for his life.

So, defense counsel needed to subpoena Facebook for the contents of those messages in order to prove up the self-defense claim. And, when defense counsel tried to subpoena those messages, Facebook refused to hand them over, because of a data privacy law. So, the bigger picture here is that technological change is deepening the power and balance between the government and the queues, John, as you were saying, and exacerbating information asymmetries in these investigations.

The reason that matters so much is because in the U.S. we have an adversarial criminal justice system, and that means prosecutors are responsible for introducing evidence of guilt before the jury, and defense counsel is responsible for introducing evidence of innocence. In our criminal system, defense counsel's actually the only actor who has a duty to actively investigate innocence.

If prosecutors happen to have possession of some exculpatory evidence they know their prosecuting somebody who might not actually have done the crime, then the Constitution requires that they hand that information over. But, there is no Constitutional, legal, or even ethical duty on prosecutors to actually seek out evidence of innocence. And, that's why defense counsel's independent investigative power matters so much right now.

One thing that technological change is doing is it's putting more relevant evidence in the hands of third-party companies, and that means that some of the procedural protections that we've built up in the 20th century to require prosecutors to disclose evidence of innocence, statutory discovery laws no longer work. We're relying on defense independent investigations even more than we used to.

VILLASENOR: So, on that note, I'd like to ask you about one specific statutory framework that you have cited as problematic in relation to these sorts of questions. And, that's the Stored Communications Act which was enacted in 1986. To put it mildly, the technological landscape has changed quite a bit since 1986.

And, with regard to the issue of impeding these sorts of criminal defense investigations, can you give a little bit of insight as to what's problematic about the Stored Communications Act?

WEXLER: Yeah, sure. So, the Stored Communications Act, it's a general federal privacy bill that protects your privacy and the contents of messages you transmit over the Internet. If that's the contents of your email, or if it's your Facebook, other social media posts, it protects that privacy when those are stored by the electronic communications service provider.

And, it does that by prohibiting or regulating when a service provider can disclose those contents. So, they can't just take your social media private message and send it off to the news. They're limited with what they can do. There are certain express exceptions that allow them to disclose that information to law enforcement but don't allow them -- or there's no express exception for them to disclose that information to criminal defense investigators. And, as a result, technology companies have argued that they are unable to comply with these defense subpoenas.

Now, based on the legislative history of this statute, it appears that Congress probably didn't even consider defense investigations when they were enacting it. There's no indication that anybody intended to protect privacy in your communications from defense investigations just because they were transmitted over this technological medium.

But, that's the position that technology companies have held, and that's actually the law

when I was talking about the case with the SUV and self-defense. That's the law that was at issue there. It's a huge problem for defense counsel around the country.

As you mentioned in the introduction, I spent a year practicing with The Legal Aid Society in New York, but I'm also in touch with defense counsel in other jurisdictions. And, they're telling me that the Stored Communications Act is inhibiting their investigations on a whole series of levels.

So, first of all, if they know that technology companies are going to deny their subpoena, they may be chilled from serving it in the first place. So, there's chilling effects. Next, defense attorneys have told me that compliance officers at these technology companies regularly engage in overbroad denials, and that means even though there is a plausible reading of the Stored Communications Act to say that they're prohibited from disclosing content, there's no reading of this act that would prohibit them from disclosing non-content.

Anything that's not in the body of your message so the To-From information, contact, IP address, timestamps, location information, any kind of metadata that's associated with a message, all of that can be disclosed pursuant to proper legal process. Now, we're not talking about just freewheeling, you know. There's no limits and no privacy protections here.

But, pursuant to proper legal process, defense counsel can get that information, and they regularly do. But, when they send subpoenas to tech companies that have a mixture of requests, some compliance officers just routinely deny them off the bat, rather than responding by disclosing what they can reveal and then not disclosing or sending some letter traffic back and forth to explain why they're withholding --

VILLASENOR: So, they don't make it easy to get this information, even when there's a perfectly valid, legal framework for getting it.

WEXLER: Absolutely right. And, this is happening at multiple levels. I'm glad you mentioned ease. Now, look what they're doing for law enforcement. They've put on online portals just for law enforcement, to make it easy for law enforcement to submit their requests when they go on investigations -- upload a warrant -- there's a whole special part of the Facebook website, Google website, for law enforcement.

Meanwhile, Facebook especially has made it very difficult for defense counsel to even serve them with process. They won't accept service of process unless a defense subpoena is domesticated in a California court, which means indigent defense counsel all around the country have to have somebody in California help them if they want to even file the subpoena.

Ratcheting up into what problems this law is creating for defense counsel is that even when courts actually rule that defendant's due process in Sixth Amendment rights entitle them to this evidence, notwithstanding that there's a statute in the way, technology companies have chosen to take contempt judgments instead of hand over potentially exculpatory evidence pursuant to those court orders.

VILLASENOR: Why is that? Is it because they'd rather fight the contempt battle than create the impression that they're not being as careful as they should be with data? Is that the issue?

WEXLER: Yeah, I think that's absolutely right. I think that technology companies -- I believe they're not thinking this through and that we could help them think of it in a different way. But, their intentions are rightfully to protect their users' privacy to the full extent possible in the law. And, since there is a plausible interpretation of this statute that prohibits them from complying, they're relying on that interpretation.

They're also worried about civil liability. I don't think they should be. Another part of the

Stored Communications Act immunizes them from civil liability if they comply in good faith with the court order. The problem with their position, though, is that it's extreme to think that any federal statute is going to impose an absolute bar on defense investigations of exculpatory evidence. And, if you look inside the procedural rules in the criminal justice system, this becomes obvious.

We have extremely narrow categories of information that we let categorically ward off information from truth-seeking in the courts. We call them evidentiary privileges. The attorney-client privilege may be the most famous. And, that actually doesn't tell you to withhold information from defense subpoenas and from law enforcement.

But, nowhere else in the criminal system do we provide an absolute bar against truth-seeking, just because information is transmitted over a particular technological medium regardless if it's a communication between people in a relationship we think is sensitive, like spouses or your clergy or therapist, regardless of whether the contents of the communication are actually particularly sensitive. And, that interpretation of the Stored Communications Act that technology companies are advancing, that it would be an absolute bar, even in the face of countervailing defense constitutional rights, is just extreme.

VILLASENOR: So, with that sobering lesson in mind, as you, of course, know, there's any number of new privacy bills that are regularly proposed in Congress in each congressional session. So, what should legislators be keeping in mind when they draft new digital privacy laws to avoid these sorts of unintended consequences with respect to new laws?

WEXLER: Yeah. Well, thanks for bringing that up. There is a real risk that we're going to make the same mistake again, and these new data privacy laws that we know have caused so many problems with the 1986 Stored Communications Act. And, the issue is, what I think

legislatures should consider, is when they're about to draft an exception for law enforcement investigations, you know, think about whether defense investigators might need a similar exception.

As I mentioned, we rely on defense investigators to investigate evidence. Defense investigators are investigating the same crimes. They're investigating the same facts, the same events, the same people, and so, it's reasonable to think they might need the same exceptions.

The good news for legislators is, again, that there's this simple, easy fix. And, we have existing privacy laws that model this fix. So, you can have a blanket neutral exception for compliance with otherwise valid legal process, whether it's served by law enforcement or served by defense investigators.

And, the crucial point here is that that type of exception doesn't eliminate privacy protections, it just maintains the status quo. So, the same privacy protections that are built into our subpoena power, that we already have decided are sufficient that are currently regulating a vast amount of extraordinarily sensitive information in the criminal system, whether it's your medical records, your location information, those privacy protections will still apply.

So, the good news for lawmakers is that this is a simple problem to get ahead of. All you have to do is write in a neutral exception, and you don’t even have to worry about adding more or eliminating existing privacy protections in the criminal investigation space.

VILLASENOR: It sounds like the good news is that there is a straightforward path that can avoid this problem with new legislation, but, of course, that depends on members of Congress being cognizant of that and not simply copying and pasting these sort of legacy statutes.

Because, again, I think members of Congress, when they draft privacy legislation, are

very well aware of the historical tradition or need to have some kind of provision for law enforcement, but they may not be aware of the corresponding need to not hamper defense investigators who are doing what they should be doing for their clients, which is to pursue evidence of innocence if that evidence is available.

And, so, it's an awareness question, I guess, in part, right? So, are you optimistic that there's going to be growing awareness on this issue on Capitol Hill?

WEXLER: Well, I'll tell you, I'm getting more optimistic the more I get a chance to work with you, John, because you've been really crucial in helping to raise the visibility of this issue in Brookings, I think. I'm so grateful for the opportunity to help raise awareness through Brookings.

I have had some excellent exchanges with folks who are involved in drafting current data privacy bills. And, so I am hopeful that once we reach the right audience there's going to be a lot of receptivity here.

VILLASENOR: It's just raising awareness, just educating the community about this often overlooked issue, basically.

WEXLER: I think that's right. You know, what happens is, look, law enforcement has a lot of visibility and ability to rightfully gain lawmakers' attention, and the defense bar has much, much less. And, so, we know that there's just going to be some things that fall through the cracks, and this is one of them. Having media attention to this issue, having meetings being -- I'm available as a resource. John and I have this blog post on this issue. I'm also writing a Law Review article called Privacy Asymmetries forthcoming in the UCLA Law Review that addresses some of these issues.

So, raising awareness on all these fronts is key. And, let me just say, another reason why I'm actually optimistic about this is that, contrary to what you might at first think, it's not a law

enforcement versus defense issue, because law enforcement really doesn't have an interest in stopping defense counsel from doing their job.

Law enforcement prosecutors, their ultimate goal is to seek truth and justice and serve the public interest. And, so when they rely -- and they do rely -- on defense investigators to find out what the evidence of innocence might be that's out there, that's a good thing for everyone.

Law enforcement doesn't want to have to go out and investigate the defendant's case for them. That would be a problem, because it would drain their resources and they'd be sent here and there. But, they are not harmed in any way by having defense counsel do their job.

And, actually, there's a case in the California Supreme Court in which the San Diego prosecutor's office filed a brief, arguing that the Stored Communications Act shouldn't block defense counsel from accessing information from Facebook. So, that's another thing that makes me hopeful here.

VILLASENOR: That's interesting. So, do you know what motivated them to file that?

WEXLER: Well, one thing that might have motivated them is that there is the possibility of structural constitutional error if we don't get this right. And, so law enforcement does want to have their convictions stick. There's a case that the United States Supreme Court considered and actually recently denied cert on, but I think it'll probably come back before them, where the Stored Communications Act barred defense counsel from getting access to a prosecution witness's potentially impeaching social media communications.

And, in that case, it's one of the cases where Facebook and Twitter both chose to take a contempt judgment instead of comply with the court order to hand over this information. But, in that case, my guess is that ultimately that conviction's going to be overturned because of constitutional error, and law enforcement prosecution's going to have to redo it. So, there's a

safety cost to the public from not getting this right, and there's a cost to law enforcement from not having fair trials.

In the short-term, the bigger picture, of course, is that it serves law enforcement's legitimacy and the legitimacy of the criminal justice system to have, as much as we can, accurate and fair criminal proceedings.

VILLASENOR: Is it your sense that these privacy asymmetries are on the radar in terms of ending up before the courts? Are the courts sensitive and aware of these issues, or are they simply just -- if a big tech company says, no, that's an overly broad request, we're going to deny it, do the courts just sort of rubber-stamp that when that's challenged?

WEXLER: Totally. Well, so you're putting your finger on, I think, one of the real difficulties with defense investigations and protecting defense investigations in this new technological era, which is that it's actually really hard to know what happens in those investigations. Because, so many of the defense subpoenas, I mentioned before, are chilled, but otherwise they can die in letter traffic between defense counsel and the company.

Over 98 percent of criminal defendants in our system plead guilty before trial, and so, a defendant might plead guilty while the letter traffic's happening, before a technology company even bothers to move to quash that subpoena in court or defense counsel bothers to move to enforce the subpoena in court.

If they do get to that stage of enforcement, they're only getting to the trial court stage, and there the trial court's order is likely going to be an oral order from the bench, and it's not going to hit the record, so it's not going to go up on appeal. So, we're only seeing a tiny percentage of the cases where defendants are being denied relevant evidence actually bubble up into our databases like Westlaw-Lexis and have some visibility in the appellate system.

The fact that there have in the past few years, and there are right now, some pending, interesting cases all the way up in State Supreme Courts. And, again, I mention there was this petition that just got denied from the U.S. Supreme Court on this issue. That makes me think that this is, as far as we can tell, quite a large problem, and we'll be seeing more and more of it in the courts.

VILLASENOR: I'm sure you're more familiar than I am about these statistics, about the number of criminal prosecutions where there's plea bargains that never go to trial. I think it's in the 90 percent-ish range, at least, that don't go to trial, at least in some court systems.

It's sort of terrifying to think that in some cases defendants who are innocent but don't believe that they're going to be able to get access to the evidence proving their innocence make essentially a calculated decision to plead to some lower charge because they're terrified of getting found guilty wrongly if they don't plead guilty. Because, it's a hidden consequence to these asymmetries that we may never even see.

WEXLER: Totally right. And, you can imagine, in the case that we were talking about right at the beginning of this, with Jerome Greco's client who's incarcerated pre-trial because of this wrongful accusation about the harassing text messages and voicemails, he might have served a fair amount of time in jail just waiting for this issue to get resolved, have employment consequences, housing consequences, maybe family members he doesn't see, now COVID exposure. And, so, there is a real consequence of that.

It reminds me, when I was mentioning the fact that some of our 20th century procedural protections are becoming less effective in a technological age, we do have constitutional requirements for prosecutors to disclose evidence sufficiently in time for defendants to consider it when they're evaluating whether to take a plea. But, we don't have similar protections to enable

defense counsel to independently subpoena similar evidence on a similar timeline.

In that other constitutional protection, what we've been worried about is prosecutors selectively suppressing evidence of innocence. That feels unfair. The government somewhere has possession of that evidence and they still prosecute, right?

VILLASENOR: That is pretty unfair.

WEXLER: The good news is we figured that out as a society in the mid-20th century, and the Supreme Court recognized that there's a constitutional right to have that evidence disclosed. But, now, with third-party possession of evidence, with tech company possession of evidence, the same effect happens when legislators, even inadvertently, pass laws that selectively suppress evidence of innocence. A little more removed from the prosecution team -- and, again, I'm not suggesting any bad faith here -- but, the effect is the same, and I think we should start to think about that as similarly unfair.

VILLASENOR: Right. Because, either consciously or not, what the tech companies -- when they do that, are essentially deciding is that they'd rather take the hit of, say, a contempt finding than take the hit of PR that might make it possible to portray them as being less than fully protective of user privacy.

WEXLER: Yeah. The technology companies are making that tradeoff, and lawmakers are inadvertently passing these laws that enable that tradeoff. There are sometimes tradeoffs, and so we might in some circumstances decide we're going to accept a hit to accuracy and fairness or accuracy and truth-seeking, because we have some other value that matters more, like strong encryption for privacy and security on the Internet that we think if we enable law enforcement to access it's going to have so many other consequences outside of the criminal system that we're willing to stomach some cost to truth there or evidentiary privileges similarly.

But, here, there's no real reason to do that. It's going to be very rare where we're going to want to accept that tradeoff with an absolute bar on evidence in the truth-seeking process, in part because we can still balance this tradeoff with other values by having legal process requirements. So, when law enforcement has to get a warrant, they have to show probable cause particularity.

When defense counsel wants to get a subpoena, they have to show relevance, admissibility, sometimes necessity for that information. And, lawmakers, if they are worried about too much excessive invasion of privacy, they can jigger that balance with the procedural safeguards. They don't have to take the nuclear option of a total ban on access to evidence.

VILLASENOR: Of the many complex issues we have in the policy world, this actually sounds like one where there's a pretty reasonable win-win solution, right, which is simply to draft new legislation that has these symmetric provisions that provide defense investigators with the access that they need to do the work to try to prove their clients' innocence.

I guess my question is, -- I'm just playing devil's advocate for a moment -- what's the counterargument? In other words, if somebody were to oppose a symmetric provision in new legislation, on what grounds might they do it? Would they be concerned about fishing expeditions? Like, what might they say -- what's the argument against it? Why isn't this an absolute slam dunk and everybody should do it and there's nothing you need to talk about?

WEXLER: Yeah. Well, you know my view on it, but let me join you in the devil's advocate. I think some of the stronger arguments for why we should have some hesitation are that the only actual reason to limit defense subpoenas, in my view, is because of the administrative burden that it would cost technology companies if we allow defendants to subpoena evidence from them.

So, a technology company's position is, don't get the evidence from us, get it from our

end-users, and they like to present that view as privacy protective, because they say end-users will get notice and they'll be able to tell the court not to enforce this subpoena. That argument is not a solid argument, because when defendant's subpoena technology companies, the end-user retains standing to argue for their privacy in court.

When we're in a law enforcement context, the Fourth Amendment applies, and the Fourth Amendment actually limits an end-user's standing to challenge government searches and seizures if the government gets their information from a technology company. But, that's not true in the defense space, because anybody who has a privacy interest in subpoenaed information can move the court to quash the subpoena, move the court to protect their privacy interest and deny the subpoena.

And, so if we allow defendants to subpoena technology companies, all it will mean is that the technology companies will also be in the loop. We need to give the end-users notice, and that is something for lawmakers to consider, is mandating notice unless there's an extreme situation where it'll be unsafe or dangerous to have notice.

But, in general, we should mandate notice to end-users, or, in fact, anybody whose communications are caught up in this. Our wiretap laws require notice to people who are caught up in a conversation, even if they weren't initially the target of the investigation. So, we could require notice to everybody whose communications are implicated by a subpoena, and then all those people will be able to move to the court to assert their privacy rights, and so will technology companies.

So, I think the privacy argument is actually deceptive. We could enhance privacy by allowing defense attorneys to put technology companies in the loop here. But, what it would do is impose a substantial administrative burden on technologies, to comply with a new category of

subpoenas.

I personally don't think that's a legitimate argument to undermine truth-seeking and accuracy in the courts when all the rest of us have to shoulder the burden of compliance of legal process -- banks, hospitals, you and I if we're served with a subpoena. We've got to take the trouble to comply. So, technology companies, I think, should shoulder their fair share as well.

VILLASENOR: Well, thank you very much. This is a fascinating topic. And, again, as you mentioned a few moments ago, you've got this Law Review article forthcoming in the UCLA Law Review, called Privacy Asymmetries, which I think is destined to be sort of the standard academic reference on this topic. Thank you very much for being on the podcast, and I certainly look forward to further discussion on this really important issue.

WEXLER: What a pleasure. I really appreciate the opportunity to call attention to this issue. Thank you. Thank you, both.

DEWS: And, now, time for a coffee break. Here's Alex Engler who talks about how he became a scholar, offers some book recommendations, and (inaudible).

ENGLER: My name is Alex Engler. I'm a David M. Rubenstein Fellow in Governance Studies where I study artificial intelligence policy. I also do data science for policy analysis at Georgetown University.

I grew up in an upper-middle-class household in suburban New Jersey. The town, Morristown, was actually named the best place to live in America by Money Magazine in 2005, which was shortly before I left for college. So, while I got an excellent education there, I can't say that my life experience imparted a particularly broad perspective on me. Thankfully, I was the least aware that my experience wasn't particularly representative.

In fact, Camden, which was one of the poorest and unfortunately most dangerous cities in

the United States, was only 15 minutes away. And, that staggering inequity did not seek me as a kid. So, I left home not necessarily grounded in the realities of injustice on a personal level but certainly with an awareness that I had a limited scope of experience, and that's informed me in my studies since.

Certainly, my dad's lifelong (inaudible) was the biggest factor and inspired me to go into public policy. He recently retired from a career fighting for labor rights and environmental protections, most of which he did in New Jersey, and then that culminated in an appointment to the U.S. Chemical Safety Board. He was definitely the heart of driving me to policy studies.

But, my mom was in (inaudible), too. She was the Chair of a psychology department in New Jersey and was a scientist by nature. And, that's where the more rigorous, empirical side of me comes from. That's what primed me for being receptive to getting a Data Science degree after I've had a policy degree. And, that overlapped being interested in broader social issues while still engaging with the empirical and technical concepts of data science.

It has been a really useful combination in preparing me to study artificial intelligence at the sort of societal and for the policy level. And, I've become quite passionate about that. That's now what I teach -- previously in Chicago and now at Georgetown.

In terms of the most pressing issues of the day, it's hard to beat climate change and also sustaining the absence of great power conflicts, useful to sometimes do it yourself and the fact that there's more important issues than the one that you study, which for me is technology policy.

That said, in my expertise, artificial intelligence is doing some important stuff at the societal scale that we want to be cognizant of. It's consolidating a lot of influence in a smaller number of corporate actors. The number of AI systems in corporations is growing, and the scale of those systems is growing, so they're making more decisions.

And, when they make those decisions, they make them on an enormous scale. This includes healthcare, who's getting additional medical treatment. AI is making some of those choices. It includes employment decisions, who's getting hired, fired, and promoted. The top-rating, larger pieces of transportation, like autonomous cars and trucks, and affecting a lot of other critical infrastructure.

There's an emerging consensus on how ethics principles should govern these systems, deciding how the systems themselves and their operators should behave. But, there's no actual governance of oversight, and we're seeing that become an issue. So, if you think that, like I do, AI systems are going to have progressively more impact on corporate function, and governments as well, then there's an important question on how governments can provide oversight.

It's a challenging question, since our understanding of how AI levels really work, how to interpret and explain them. That's an emerging scientific field. And, it's also quite exciting, since it's an area policy that, collectively, we don't know that much about.

So, right now, the governance of artificial intelligence systems is certainly a big focus of my work. We're especially interested in the international governance of AI. The European Union is working on the first comprehensive AI legislation that would really determine limitations and guardrails for particularly high-risk applications of AI, like the ones I just mentioned in healthcare and in transportation and in employment. You might also think about finance and criminal justice as other highly (inaudible) circumstances.

So, while the EU is forging ahead, the U.S. is currently a little more reticent to do that. And, so, how this shakes out in terms of the international governance is quite important, since AI systems are baked into all types of products. If there's dramatically different standards in the EU and in Canada and in Japan and the UK and the U.S., it makes it very hard to do anything with

AI.

So, we are better off with a single set of standards that effectively makes AI safe and trustworthy that's enforceable across these countries, and that's a big, emerging conversation just this year that has, in fact, continued despite COVID-19.

There's also related issues, I think, if you're paying a lot of attention to artificial intelligence and large-scale data collection. You start to notice that this is a consolidation of economic power, and a small number of companies seem to be benefiting from this and have a huge informational advantage. And, it's not clear that this is resulting in the benefit of their consumers. And, there's certainly a substantial downside to their employees, and what governments decide to do about that is also a really serious issue.

When you talk to people about artificial intelligence, they tend to cite a couple issues that breakthrough in the popular culture. That's killer robots, autonomous cars, and sometimes the "algorithm" in social media feeds.

But, if you want to understand the issues that are much more likely to affect the vast majority of people, there's a trifecta of books that I want to recommend that are far more grounded in this reality. Those are Automating Inequality by Virginia Eubanks, Algorithms of Oppression by Safiya Noble, and Race After Technology by Ruha Benjamin.

Those are going to give you a much clearer sense of really the challenges that AI is actually posing in the immediate future that's far more grounded in reality -- examples of (inaudible) finance and loss of agency by employees, and loss of market power by consumers when faced with the implementation of technology at scale.

If you are really concerned about super-intelligent AI overlords, Gary Marcus has a great book called Rebooting AI that will convince you not to be so worried about that.

DEWS: The Brookings Cafeteria Podcast is the product of an amazing team of colleagues, starting with audio engineer Gaston Reboredo. Bill Finan and Robert Wicks of the Brookings Institution Press do the book interviews. Thanks, also, to my colleagues Adrianna Pita, Marie Wilkin, and Chris McKenna for their collaboration. Finally, my thanks to Camilo Ramirez and Emily Horne for their guidance and support.

The Brookings Cafeteria is brought to you by the Brookings Podcast Network which also produces Dollar and Sense, The Current, and our Events podcasts. Email your questions and comments to me at bcp@brookings.edu. If you have a question for a scholar, include an audio file and I'll play it and the answer on the air. Follow us on Twitter, @policypodcasts. You can listen to the Brookings Cafeteria in all the usual places. Visit us online at Brookings.edu.

Until next time, I'm Fred Dews.

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

Carleton J. Anderson, III

(Signature and Seal on File)

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2020