Sharenthood: How Parents, Teachers, and Other Trusted Adults Harm Youth Privacy & Opportunity – November 19, 2019

So we are webcasting today, which means that this is being streamed live and also will be available online afterwards. We're very excited to bring Leah Plunkett here today. And she is speaking about her new book, "Sharenthood-- Why We Should Think Before We Talk About Our Kids Online."

Indeed, it's a book for parents and other adults, but it also brings the perspective of a legal scholar with a deep understanding of privacy and equity issues, and a strong grounding in technology and academics. Leah is also an academic who has worked for, and with, youth.

She's a faculty associate here at Berkman Klein. She's also an associate dean and associate professor at University of New Hampshire School of Law. She is a longtime close collaborator of Youth and Media, and Leah was just telling me that she was an RA With Jonathan Zittrain in 2004, which is fabulous.

She graduated from Harvard Law School, where she was training director for the Harvard legal aid bureau, and she continued to work as a legal aid lawyer with the New Hampshire Legal Assistance. There, she founded the Youth Law Project. And she also brings a perspective as a parent to her work. And she's got her son and her family right here, so that's very exciting.

So we're very lucky to have Leah with us today. Let's give her a warm welcome.

[APPLAUSE]

Thanks so much, Liz. It is just such an honor and a delight to be back with so many longtime collaborators, and mentors, and experts, and old friends, and soon to be new friends as we all have a lively conversation. So I'm going to talk for about 20 minutes and throw out three major ideas and then we'll open it up for what I hope will be a dynamic discussion.

I wrote a book from the MIT Press Strong Ideas series, called "Sharenthood-- Why We Should Think Before We Talk About Our Kids Online." This book is the direct result both of my background as a legal aid lawyer and a consumer rights lawyer and also of my work with the Youth and Media team, where we looked together-- they are still looking-- very closely at the ways that youth, so roughly 12 to 18-year-olds, are engaging in our digital world, as well as a number of the adults around them.

And I began to be increasingly interested and concerned about what the adults around them were doing. And so I embarked on a conversation starter. The Strong Ideas series, which David Weinberger-- who's also part of the Bergman Klein community-- has been stewarding, is designed to throw out provocative ideas about technology and everyday life by academics and experts for folks to have general discussions about. And the ideas I'm about to throw out I first tested in a fellow's lunch back-- I don't even know how many years ago. So it's wonderful to come full circle.

So my ideas today are going to focus on parents, play, and predictions. Before I move into those, quick question, because I'm a law professor and I have a captive audience. So I'm going to put you on the spot and ask by a show of hands how many people have heard the term sharenting? I'm glad my son has, because I talk about it a lot.

So sharenting-- I did not invent it. I got asked that recently by a reporter. I can claim no credit for that. I can claim credit for using it slightly differently. But just so we're all on the same page, the way the term sharenting is typically used is to refer specifically to what parents do on social media. So it is confined to parents in social media.

I think that that's a very important part of sharenting, and I will talk about it. But my understanding of sharenting is both broader and deeper. I think to really capture the full extent of the ways that kids' private information is acted upon digitally by the grown ups around them, we need to understand sharenting as being carried out not just by parents, but also by grandparents, teachers-- we start to talk a little bit about school just now-- coaches, in-laws, other trusted adults. And it needs to be understood as all actions taken with respect to children's personal digital information. So not just social media, but also FitBits and smart home devices and other digital technologies.

So now that I've sort of made sharenting broader and deeper, I am going to come back for my first provocative conversation starter and talk about parents. And I'm going to say that parents, in particular, pose an underappreciated risk to kids' privacy and their current and future opportunities. And I include myself in the parent category. So a big part of this book was writing a conversation that I was so engaged in and inspired by professionally. But also one that I was increasingly having personally with my spouse, with my friends, with family members.

So I say as a parent, I think we are a well-intentioned group, at worst we are a little bit careless, just in the course of daily life. It is difficult to impossible when you are trying to figure out whether this app is safe to use to put your child's information in, while you're also answering a work email, making dinner, letting the dog out, and doing a million and one other things. So we're trying our best, but we as parents right now are not the best gatekeepers. And that's tricky, because the law in the United States gives parents super-charged constitutional-level protections around whether, when, with whom, how, and why to have and raise kids and, as part of raising kids, whether, when, with whom, how, and why, to share information about them on social media, through apps, through devices, through smart home affordances.

So the United States Supreme Court has made this very clear. I'm not talking about digital world right now, but just very broadly. The supercharged protection that parents enjoy has come up time and again in the court's jurisprudence. And the court will say things like, "The child is not the mere creature of the state. Those who nurture him and direct his destiny have the right, coupled with the high duty to prepare him for additional obligations." That's Pierce versus Society of Sisters from 1925.

So gendered in the use of "his," but that same deeply rooted idea that there is a high duty by parents to prepare children for their destinies, outside what the government might require as a bare minimum of child welfare and child education. So that deeply rooted idea that we as parents are entrusted with the high duty of being gatekeepers between our kids and the world, it enjoys a lot of support.

And I would argue makes a lot of sense. If you think about the different potential gatekeepers for kids' well-being to paint with a broad brush, you have parents. You have the state. You can sort of subdivide those into categories. But as between parents and the state, I do think we want to tip toward parents as being the source of protecting their children and defining their destinies.

Now, that concept has been pushed through into our digital world. And, in general, when parents get to decide when it comes to whether when, with whom, how, and why to share our kid's digital data, we get to decide all of that. We're subject to the outer boundaries of criminal law and other what we might call freestanding laws-- so other laws on the books that don't have anything to do with privacy in particular. So let me give a few examples of legally permissible sharenting and examples of where we get to those outer boundaries of legal or criminal sharenting.

So perfectly permissible for me to take an ultrasound picture, put it on Facebook. Perfectly permissible for me to take my child's exact time, date, location, height and weight, circumstances of birth, full name, put it on Instagram with a picture. I can also make a YouTube video of the whole labor and delivery process and put that up and, if I monetize it correctly, potentially wind up with millions of followers and start building a business around it and enter the commercial sharenting space. I get to make those decisions as a parent. The law is not going to step in and regulate my ability to do that.

The law would step in if I were, heaven forbid, to make a video of myself doing something to or around my child that was criminal or illegal. So there have been some high profile examples of parents engaging in this type of behavior, filming it, putting it on YouTube, and then actually having viewers step in and alert child protective and child welfare services.

DaddyOFive. Has anyone heard of DaddyOFive? No? OK. So that was a couple of years ago. That was a YouTube channel that amassed a good half a million, 3/4 of a million followers. And it was a family prank channel. And their pranks crossed the line into what the judicial system found to constitute abuse and neglect of a couple of children in particular. Viewers alerted the authorities. The children were temporarily removed from the home. The YouTube channel came down.

But even outside of this commercial sharenting space, where you do cross that line into illegal and criminal acts, parents can push the envelope pretty far. So DaddyOFive-- I'm actually glad no one's really heard of them.

Who's heard of Jimmy Kimmel? Who's heard of his Halloween candy challenge? Right. So every year-- we just kind of finished this Halloween period-- Jimmy Kimmel, celebrated late night host, issues a challenge every year, where he says, parents, this will be really funny. Take your kids' Halloween candy. Hide it. Tell them you've eaten all of it, or thrown it away. Film their reactions when they understandably freak out, and then send them in. Put them on my website. And if you do a really good job, then I will select you and maybe even show it on this show. That's legal.

Now, keep in mind that if it was an older student doing that to a younger student in a K through 12 public school system, we would very likely be thinking about behavior that would meet the legal definition of bullying and actually require the school to take action against the student perpetrating that kind of, ostensibly, prank, but really behavior designed to intimidate, harass, cause emotional disturbance. But parents can do that.

So the other thing that parents are legally entrusted with doing is stepping in when other institutions or individuals want to share data about their kids, to the extent that there is a legal framework in place. Now, there are many spots right now in our digital world where there's not really a robust legal framework in place.

So if I'm with my kids on the playground, and I see another parent taking pictures of all the kids running around together, I can sort of, as a matter of norm or practice, go over and say, could you please not do that. We don't put pictures of our kids online.

But there's not some 800 number I can call where the sharenting squad is going to show up and take their phone. But to the extent that there are spaces where there is legal regulation of other people, or actors wanting to share private information about kids, its guiding principle is parental consent.

So a big example here and actually where my work with the youth and media team started is schools. Schools are subject to federal and state student privacy laws. The big federal ones really pre-date the digital era, but there are a lot of state ones. In fact, I think from 2013 to 2015, there were roughly-- it's either 500 or 300-- 300 bills considered around student data privacy. And a number of those were actually passed.

So when you're talking about sharenting within the school system-- a teacher wants to use an app, a school administrator wants to track attendance data-- the legal framework in place, to paint with a broad brush, is that parental consent is needed if it's personally identifiable information from an education record, unless an exception applies.

And interestingly, because we parents can be somewhat lousy gatekeepers, because we just don't have the time or the technical ability mixed with the legal ability to read all the terms and conditions and the privacy policies, if your child is in a school system where you have a really strong interdisciplinary team making those data privacy decisions, your child might actually be even more protected at school than at home.

And I do think that we as parents-- and we'll talk more about this sort of in our discussion-- there's room for all of us as parents to be better informed and take more responsibility. But it's also the reality that a big part of this is that parents as gatekeepers made a lot more sense in the brick and mortar era, where you could very clearly see the boundaries between home and outside. The boundaries between, this is our community space, this is our school, this is our playground and everyone else.

And now, when you have products on your desk, the smartphone in your hand, that Gizmodo watch that you give to your child-- sorry, Sam, I know I haven't given you one-- on their wrist, a fertility tracking app, a fertility tracking bracelet, an Alexa, an Echo Dot, a smart fridge, a smart TV-- and I haven't even gotten into the stuff in schools. There's a lot of things that are in our homes, or even that we put on our kids' bodies, like a smart diaper-- and that's real, I did not make that up-- that are not actually keeping the information within the protected sphere of the home.

And these decisions can have real consequences for kids' current and future life opportunities. So in a very concrete example, when parents post on social media and others in the community can see that in real time, that matters. One of the things that has come out, as I've done a number of these book talks now in different settings, is the problems of parents on parent Facebook groups for a neighborhood, a school, or a community going off about issues at their own kids are involved in or that other people's kids are involved in and creating these digital trails that can actually really paint either their own or other people's kids in a pretty negative light.

After this book came out, I got a call from a dean at an undergraduate campus saying, I feel like our undergrads are doing a pretty good job with this. But we have a parent Facebook group that's out of control. I really wish we could get the parents to stop saying things in this group about, oh my child had a run in with the police. My child had a bad breakup. Could you write something that I could share with the parents? I said, that's a great question, sure.

And then as we'll talk about a little bit more when it comes to predictions, of course, we as parents really don't have any way of knowing where the data that we're sharing is going in terms of being used-- not just by the tech providers that we may think we're giving it to, but by third parties that they may be giving it to, by data brokers who may be aggregating it, analyzing it, and acting upon it now or in the future in ways we can't predict, control, or understand. So that's my first provocative point.

My second provocative point has to do with play. And I argue that childhood and adolescence, as protected life stages to play, are being threatened in today's digital era at the hands of adults. And that that threat further threatens kids' ability to grow up with their own sense of agency and autonomy and become the people that they themselves are meant to be.

And when I'm talking about play, I'm not just talking soccer field or playing pretend. I'm talking more broadly about spaces that are experimental, iterative, inclusive, and equitable-- protected. And the American legal system has a recent-- I'm not going to go back before the 19th century here-- but a recent tradition of treating minors as deserving of heightened protection in our justice system.

Minors typically can't enter into contracts, unless it's for necessities. Minors have child labor laws at the state and federal level that limit their ability to work. We have a juvenile justice system that is designed to be rehabilitative rather than punitive, so that if a child violates a law, that would be called a crim if an adult did the similar act. With a child we call it a delinquent act. We go to the court and say, is it true or not true that the child committed this act. And then we put a rehabilitative system in place. Although, as a former legal aid lawyer who represented kids, I will query how well we actually do that, but that is at least our commitment.

And key to this commitment is a recognition that children are still learning. They are going to make mischief, they are going to make mistakes. And ideally, they will grow up better for having made them. But there is limited or no way to learn from the experience of mischief or the experience of mistakes if there isn't any protection from an adult gaze, whether it is adults that know you or adults that don't know you, and an ability to have the fun but a little misguided, or downright terribly guided, things you do as a child forgotten. And somewhat counterintuitively, the more we surveil, track, monitor, record, even just share and post about what our kids are up to, the more difficult we are making it for our kids to grow up with agency, and autonomy, and space to develop their own sense of self.

Now, is there a direct line between giving a child a smart Teddy bear, or having a child' first words be to an AI assistant? How many of you heard 1A last week, that NPR show? They had a great segment. It was a professor, I think of media studies or linguistics, talking about kids whose first words are now to an Alexa, a Siri, or an Echo Dot and what that means in the domains of child development and attachment. I'm not going to step out of my legal zone, but just flagged that for folks who might want to listen to it.

Is there a direct line between that and saying that kids have a compromised ability, or an inability, to have the privacy to play and develop their own sense of self? I'm not going to say there's necessarily a direct line. My argument here is not a very precisely causal, but a more bigger picture conceptual. And as we increasingly and casually share intimate information about our kids digitally with other people or other institutions, we are moving away from protected spaces in childhood, both because other people may see things as they're happening.

There was a Microsoft research team study that came out this fall in October that found in a sample of teens, I think it was, that over 40% of them reported having issues with their parents posting about them on social media. So they were aware, sort of in real time, of a sense of exposure and even a violation.

Also because data about issues that kids have that's supposed to be kept private can get out and may be used against them, somehow now or down the road. And a big category here has to do with surveillance and tracking and monitoring. Parents do those things.

The Washington Post just had a great article about the Life360 app that a lot of parents are sending their kids to college with. That is really sort of a comprehensive surveillance app. And the post did a great job of interviewing parents about why they wanted the app and kids about how much they hated the app and the parental/child tensions that were arising when kids would disable the app or go out of bounds at the app, as, of course, they inevitably do.

We know that in addition to the devices you can use to track your baby's sleep, or have a digital video camera in their room, or a smart diaper on their tushy-- we know that schools are doing quite a lot of this.

There was a great article this summer from Education Weekly looking at the massive use of surveillance and tracking digitally that's being done in schools. And that, under my definition, is sharenting. Those are educators, those are trusted adults taking action with children's private digital data. And one thing really stuck out to me about that article. There is a product called Gaggle-- not Google but Gaggle, with an A-- that monitors digital content created by nearly 5 million US K through 12 students.

So all files, messages, class assignments on school devices or school accounts. And all of that data goes through machine learning to start with. It goes through algorithms. It automatically scans that information, looking-- and this is a direct quote-- to see if something bad is about to happen. If Gaggle thinks-- Gaggle's machines think-- that something bad is about to happen, they do escalate it for human review. And at that point the humans can decide whether something bad is about to happen or whether someone might be doing a research project on weapons in the Roman Empire.

But that is just one example of the ways, really behind the scenes, that information about our kids is being taken from a space that is supposed to be protected-- a school-- that's supposed to be a source of learning fed into a digital product that is designed to really make predictions about them. Are they about to do something bad?

And I'm not trying to downplay the importance of school safety at all, but just to surface that we're moving well away from sort of protected learning environments in schools when we think of protection as more than, is something bad about to happen.

And my last point has to do with how kids growing up today are already subject to, and at risk of far greater, data-driven predictions being made about them and their capacities for success and trajectories in major life domains, including education-- I just gave one example-- and employment.

So I'm going to read a hypothetical, because law professors love hypotheticals. And then I will stop talking and open it up to Liz and others. So here's my thought experiment from the book. So near-future hypothetical scenario-- not real as of when I checked yesterday, maybe real today. I mean, things do move that quickly.

So you're helping your 17-year-old finish her college applications. The applications require her SAT Score, SAT2 scores, AP scores, and her Tikebites personal capital scores. What the heck is Tikebites? Siri tells you that Tikebites serves as your child's passport from her past into her future. You ask Siri to stop reading the Tikebites soundbites and do some digging.

The response-- Tikebites is a commercial database that serves as a repository of childhood data and a clearing house into adulthood. Tikebites aggregates as much data about each child in the country as possible and then packages the data for purchase by different types of institutions and individuals. The most popular product is a set of scores that rates children's likelihood of future success in a range of areas, including education, athletics, and employment.

Tikebites will share these personal capital scores with any individual or institution that pays for them, isn't legally prohibited from having them, and demonstrates what is, in Tikebites's opinion, a legitimate need for them. You and your daughter don't need to do anything to have these scores sent. All colleges that receive applications from her will request and receive these scores at no cost to individual applicants. Tikebites does allow parents and youth age 18 or over to opt out of having Tikebites collect and share their information. But the Tikebites website warns you that opting out risks your child's future.

After all, the perky chat bot in the click here for help section tells you, an applicant without Tikebites scores is like a car without airbags. You could take it for a spin, but why risk it?

Right. So what do we think? Good, bad, ugly? And I'll turn it over to you and everyone else for a chat.

Well, I'm thinking that I'll follow up with a school question--

Please.

--since we left it with a school topic. So there's a lot of excitement about schools needing to kind of get with the current century and having technologies be part of that. And in order for kids to have an extended experience with technology, that means they get tracked, right? They create an account, and the account is set up by the teacher or maybe by the school-- probably the teacher.

And so how might we think about this data? And how might we say, if we're thinking from a legal perspective as a law student, or someone wanting to get into this area-- how might we think about what's in place now, what we might want to have in place in that context?

Wonderful question. And so when we're thinking about student data, in particular, we do have three big student data privacy laws at the federal level. The Family Educational Rights and Privacy Act, or FERPA; the Children's Online Privacy Protection Act, or COPPA; and the Protection of People Rights Act and Amendment, or PPRA, which is sort of the often forgotten cousin of the other two.

But to paint briefly with a broad brush, if you're thinking about a setup where a teacher or a school wants to create an account for a child that is transmitting personally identifiable information from an education record-- and that's a pretty broad category-- of information outside the school-- and transmitting it through a digital app or software provider is transmitting it outside the school-- they're either going to need parental consent, or more likely, they're going to use an exception to the parental consent request with a legitimate school official exception.

So a huge area of need for attorneys who work at the intersection of tech and education is for strong, meaningful, clear contracts to be in place between education institutions that are using these digital products and services and the product or service provider. Because the legitimate school official exception only works lawfully if the school is using that account to do something that would otherwise be done in-house. The third party provider is under the direct control of the school, hence the need for a negotiated, clear contract. And the third party provider is not using that data for anything other than the contracted-for purpose.

COPPA would kick in if that device that the account was created for was then being given to a child under 13, who was going to be using a commercial app or software that either was targeted at kids under 13 or knew that it was getting information from kids under 13. That's again an area where you need both folks on the education space and on the tech companies space, not to mention the regulator space, because we have a bunch of state laws and regulations in place to make sure there are clear negotiated contracts.

Protection of People Rights Act and Amendment would start to kick in around certain types of products or services that are really functioning as surveys, that are getting very sensitive information, like relating to religion or similar beliefs, or certain types of apps that are collecting information that may be used later for marketing or advertising.

And with the explosion of activity on the state level, where I mentioned earlier we had 300 bills considered on student data privacy among the states from 2013 to 2018, and that five year period really being a time of very intense activity in student data privacy, we started the Student Privacy Initiative right around 2013 to help lead that conversation. 25 states actually passed 59 new laws during that time. And we continue to see growth in state youth privacy laws that don't just apply to kids in their capacity as students.

A big one being the California Consumer Privacy Act, which will go into effect in January, that would also bear on this space. So for law students or lawyers thinking about spaces to get into, helping to figure out how to negotiate and draft those contracts on either the school's side, or the vendor side, as well as entering into a space of state and federal regulation and law enforcement activity, there's a lot going on.

That's a great answer. Another thing that I've been thinking about that we've been talking about a bit here is in the spirit of hypotheticals-- one around Bitmoji, which is a little app that allows you to create avatars that you text. And so it's embedded into texting, and it looks like it's just texting back and forth and it's making a funny face for you that looks like you, or like an alien, or whatever you want to look like. But it's actually owned by Snapchat. And so it is allowed to collect all your keystrokes, and your contacts, and your location, and your accelerometer data. And so it knows an awful-- could know, we don't know what's actually collecting-- but it could know an awful lot about you.

So this is something that kids and tweens are very excited about using. You can't tell that it's part of the sort of social network ecosystem, because it looks like it's just in your text. You don't see it there. Looks like it's in a different spot. How should we think about this?

That is a perfect example of sharenting that happens in a stealthy way and stealthy by the provider. So as a parent-- and I will confess, actually, until we started talking about this, I hadn't realized the extent to which that actually was not just confined to my tech stream. So this is education for me as well.

But we should be-- you know, it surfaces a point that in some ways cannot be overstated, which is that it is next to impossible, and I will say potentially impossible, for any parent, even a privacy nerd parent, even a lawyer parent, even the most vigilant parent, to have the time and the expertise to combine all of the domains that would be required.

So let's sort of broaden out now and say this isn't something that's sort of being talked about and in the news. To try to figure that out for yourself, you would have to figure out where the privacy policies are for Bitmoji, where the terms of use are. That can be hard to just find as a matter of access. And then once you've seen them, good luck understanding them. And I say this, again, as a privacy nerd.

And even if you do pass the whole way through them, there is inevitably some sort of get-out-of-jail-free language for the company where it's saying, we're not going to share this, except to improve your user experience. We're not going to share this, except with our affiliates. We're not going to share this, except for research into development of new products.

And so as soon as you start to see language like that, it's like, well, OK, I've just spent hours or days of my life finding the language, reading the language, attempting to understand it. And it's crystal clear to me that you're reserving the ability to use this data now and in the future in ways that I can't see and I can't really control or predict. So I think that's an example that really encapsulates the weakness of this parents-as-gatekeeper model that we are using right now for youth privacy.

Yeah, I gave you a hard one.

No, it's a good one.

But it's a really interesting both sort of technological and legal question. It's also a parenting question. Like, what do you actually do as a parent and someone who-- you must get asked, what should a parent do all day, every day. What should a parent do when faced with a very, very complicated situation like this? The child probably just wants to send Bitmoji to their friends. Why can't I do that, mom?

Well, and as my son has heard me say, when it comes to in-private information that's leaving the house, I think parents can err on the side of caution. And I don't mean become a Luddite. I don't mean break your phone and turn off the wireless. But I do think there are a couple of parenting hacks, if you will, that we can all keep in mind.

One is, I would stay away from any device or service that purports to act as a surveillance or monitoring device. I think that we just don't know enough about the sort of cybersecurity issues around those in terms of their vulnerability to third parties getting them. I am particularly sensitive to the idea that any company is going to know, no matter what they promised me, where my child is and potentially what they're doing.

And particularly as a former juvenile justice lawyer, where I watched kids get pulled into court-- no kidding, once it was my client had shoved someone else's books on the playground. And the books had gone flying, and it was assault. I once actually stepped-- as lawyers in the room all appreciate, I was very careful. I didn't quite step in between, because I didn't want to have to tell my executive director that I'd been arrested for obstructing justice. But I stood right next to a 16-year-old female client who had slammed the door of a conference room.

We'd been in a very difficult IEP-- Individualized Education Program-- meeting for her special education needs. And she had documented-- I got a Dartmouth psychiatrist to document-- the depth of trauma history and emotional disturbance she was experiencing. And she had done a great job. There were, like, 12 grown ups and her at a table talking about really intense stuff.

She got up, and she got frustrated, and she slammed the door. Didn't break anything. She just slammed a door. School resource officer, the local police officer embedded in the school, showed up and first told her she had to go home. I said, why does she have to go home? We're fine now. I'm here. Her mom's here. Special education team is here. This is exactly what we're supposed to do. And he said, well, I've seen her before, and she's going to blow a fuse later in the day. And I'm thinking, yeah, because of you.

But I just said, again, thank you very much, officer, I have this. And he sort of huffed and puffed, and he let her stay with me. And then he said, but you know, if you weren't here, I would have arrested her. And I said, can I ask you for what? What would the charge have been? And he said, disorderly conduct, for slamming a door. And I looked at him and I just said, very vigilant. And he looked at me with this sort of, like, are you complimenting me or criticizing me?

And it was one of those-- like, I just smiled and let him sort of take it as he wanted to take it. And he left. But it was just the luck of the draw that I happened to be there that day, and that I had gotten a lot of training from Harvard Law School in how to sort of stand firm and have tough conversations. But in an era where, particularly for kids who have disabilities, or who come from lower socioeconomic status, or are minorities in the communities they're in, we are already vigilant about responding to normal things they do as kids and teenagers with this sort of outsized response-- slam a door, disorderly conduct. And so the last thing that I would recommend the parents do right now is to buy a commercial product that says, we will keep track of where your kids are and potentially what they're doing in some way, shape, or form. So if they're outside of the boundaries you've set for them, we'll let you know. Right?

Well, the last thing I want to do is to create any sort of digital trail, not just about where my child is, but that purports to tell me when my child might be out of bounds. Because I have no confidence that any commercial provider would keep that data just for me to use with them no matter what they say.

And so would I then be serving up digital data that could go to a data broker now or five years in the future, and from that data broker go to be aggregated into some sort of predictive software for hiring, where it's not just anymore that you're taking-- Cathy O'Neil talk does a great job of talking about them in Weapons of Math Destruction. The hiring industry that does sort of pseudo-personality tests that 60% to 70% of Americans applying for jobs now are taking these digital assessments designed to see what kind of fit they are-- well, I don't think we're that far from these kinds of assessments getting data that we as parents have put out there about our kids, thinking it's just to one company, thinking they're keeping it to themselves. And before we know it, maybe not all of it, maybe not every product, but enough of it gets aggregated into those kinds of gatekeeping predictive products, so that I've unwittingly served up, oh, this child was always out of bounds when they were 15 years old. Well, finger on the scale of not being a good candidate for the job.

So I would say, as a parenting hack, don't use surveillance and monitoring products. I would not put any pictures online of a child of any age in any state of undress. I think that invites an unwanted gaze, as we saw this summer from research that came out from some of the Berkman Klein and other communities-- sort of what the YouTube algorithm was doing, from pushing viewers from content that is innocuous or innocent, involving kids, so kind of the nice summer day at the beach, to content that is predatory. That's just one example of the way that an unwanted gaze, either by an individual trying to find that kind of content or an algorithm trying to captivate interest, can go.

And last, and maybe least, I think if you are going to give updates on social media-- maybe this makes me old-fashioned. I use a holiday card rule of thumb. So my grandma used to put out these long one- to two-page typewritten mimeograph newsletters from wherever she was in the world. My brothers are here, too. Our grandparents were-- my grandfather was in the Foreign Service.

And so she would have once a year these big updates. And they went to everybody. They went to, like, the second cousin three times removed. My cousin's here too. They went to former colleagues, former bosses. So it was really for public consumption.

And this is less about the keeping things safe from downstream unintended uses and more responding to the increasingly voiced concerns and emotions and reactions of youth themselves, to, like, I don't want people to know that I'm nervous about getting asked to the school dance. I don't want people to know that it really took me a long time to be potty trained.

Or go to YouTube and search for "girl gets her first period." They have those mother-daughter chats on YouTube. And kids don't like to see that stuff. So I would keep that stuff private.

So that leads very nicely into my very last question. And then I'm going to open it up. One thing I appreciated about your book is I could see your experience in legal aid and working with youth and surely dealing with the juvenile system, the child protection system, and the courts. And I wonder what you might say to people who are thinking about going into that space. What are ways in which they can be advocates? Or what are ways in which you would want to see policy change? Or what can be done in that space?

Thank you for that. Because without that, I run the risk of sounding very pessimistic. And I'm actually a fundamentally optimistic human. And I am optimistic about this because I think that, on a whole, digital life is a positive thing for people and institutions and for the world in terms of the ability to build connections, spark innovation, and really transform everything about how we live, work, play, and so much else.

And I think when it comes to kids in particular, there is truly a heightened sense of individual and societal responsibility we feel. So I am optimistic that now that we're increasingly having these conversations, all of us in this room, everybody who recently read and commented on the New York Times piece, "How Photos of Your Kids are Powering Facial Recognition Technology"-- I mean, there is increasingly robust public discussion about this.

So what I would challenge all of us, in our personal and professional capacities, is to be increasingly guided by values-based decision making that is conscious in our minds. So are we going to have the ability to peel beneath the layers of Bitmoji or whatever the next thing is every time? No. Do we have the ability to say within our families, we value protected spaces to play? So we are not going to bring in digital technologies into those kind of private spaces unless they serve a really compelling need.

Or then we can start to broaden out that conversation and say to our regulators and our lawmakers, you're not doing enough to address the issues of downstream uses of children's digital data. California is about to be doing a heck of a lot more. But even California's law suffers from some big holes in terms of not applying to enough tech companies and I think still making it difficult potentially for parents and kids to find what a company has about them.

I think we ask all the way up to the federal government, when the federal government starts functioning again, for more comprehensive youth digital privacy law that would regulate at the level not of parents or even schools, but of tech companies themselves, in terms of limiting the uses, particularly around predictive decision making and other gatekeeping functions that they can make of data that they have collected either directly from, or about, minors.

And I think that has to have a robust enforcement mechanism, a private right of action. So you can turn the litigators loose. And so that's another one, Liz, for law students and lawyers looking for a career focus. There is always room for a ferocious, creative litigator in a space, even if there isn't some sort of new comprehensive federal youth data privacy law. And so I am excited, now that we're thinking increasingly about these sharenting questions, to see what the next generation of lawyers does with perhaps some existing causes of action constructively applied in new ways.

I don't really see a space, and I hope there's not a space, to have a lot of kids growing up and suing parents, unless it's been really egregious. But I definitely would look and hope for spaces to have some theories of kids growing up and suing tech companies or the gatekeepers that may have acted upon that digital data.

Great. Well, with that, let's open it up to questions. Does anyone have-- Rubin has a mic and Megan as a mic. We've got one over here by you, Megan.

Yeah, so I'm just wondering how stepping away from the parents plays into this, like issues where, say, a parent is following these recommendations that you did or, say, they don't want any information about their children, like pictures-- I'm specifically thinking of pictures on social media-- they don't want any of that online.

But I hear in conversations a lot-- and this might just be anecdotal-- that oftentimes aunts, uncles, grandparents are some of the worst perpetrators of sharenthood. And how does that play into that? Do you see any inroads for ways of parents to kind of enforce their subjective kind of values over their child's privacy on other parties?

I'm smiling because I've been getting that question increasingly. And so I feel the need to write something specifically about this before the holidays, so hopefully I'll get something up on my Psychology Today blog. I will also just put in a quick plug.

I've been talking to a Wall Street Journal reporter who wants to do a story on this and wants to talk to parents or grandparents or other family members who are willing to go on the record to talk about that. So if any of you are, or know people who are, my contact information's online. Please email me and tell me, because I get this question a lot now that I'm talking about the book. And so between my, admittedly, anecdata and also this Wall Street Journal reporter's question, there's clearly a lot there to unpack.

What I have been saying to people is that there is a bit of a, take a deep breath and have the conversation in a way that depersonalizes it and normalizes it. So whether it's, hey, did you see what the New York Times reported about how photos of toddlers from 2005 are informing what the Times called "bleeding-edge surveillance technology"? That's creepy and weird. I trust you. You're an amazing aunt, uncle, cousin, brother, whomever. But I really don't trust big tech. So can we just keep it among the family?

Or I heard this crazy law professor speak. She's going on and on about smart diapers and fertility tracking apps. But she might have not been completely crazy, and maybe we shouldn't do this. But I think we just have to take a deep breath, depersonalize it, and try to normalize it.

And you were talking about sort of parenting challenges. And I think those of us who are parents or caretakers of kids at all are really used to, and in fact seek out conversations, like, hey, your kid's coming over for the first time, any food allergies? Or, I want to show the kids a movie tonight, are you comfortable with something rated PG?

We're kind of used to those conversations. And I think we all need to, as uncomfortable as it is, make this the same kind of basic conversation you have, either on behalf of your own child or if you're watching someone else's child.

And actually, when I was working with the publicity folks around this book, one of the things we briefly talked about this summer is, as sort of a giveaway with the book, should we have a sticker that said, like, no sharenting or safe sharenting that you would put on your child? And we decided that unfortunately, in today's world, that would just make those kids targets for having their pictures taken and then being trolled and doxed and harassed. So I did not do that.

But I think we can all kind of try to verbally put the sticker on. And if you want to talk to the Wall Street Journal also, you can come see me afterwards.

Hey. Thanks so much for the talk.

It's great to see you.

Sorry I popped in a little late, so maybe you touched on this. But I'm curious to see if you saw any generational differences between younger mothers who have grown up with social media in a particular way, versus older mothers.

I think that the--

Or parents.

It's OK.

Excuse me.

It's OK. I'm a mother. I'm happy to talk about mothers. But to talk about parents, I do see some. And I see that for parents in my generation-- I'm 40. I'm the tail end of Gen X. I didn't have an email until college. I didn't have a cell phone until after college. I know a lot less than people younger than me when it comes to this. And so there is this way in which-- and it kind of gets back to something I shared earlier about a dean from an undergraduate college calling me and saying, my students are doing fine, it's the parents of the students that are getting them into trouble.

Kids are learning today a lot about digital citizenship and digital privacy-- the wonderful curricula that Youth and Media is developed, that Common Sense Media has developed, and other trusted partners. And so when it comes to the kids who will soon be parents, or who are kids of parents like my age, they may actually know more and be in a position to teach parents.

So I think in addition to seeing definitely some differences between parents who are younger than I am, so in their 20s and 30s, and somewhat more sophisticated, we also, no matter what age we are as a parent, have so much that we can be learning about digital citizenship, which includes digital privacy, from our kids.

I think we've got one over here. Is that a hand over here?

Yeah. While the mic is coming, I will say I gave this talk recently. And I had a more senior member of the audience say to me, this is very interesting. Can you talk about what the kids and teens are doing in terms of sharing pictures of themselves? And I said there's some wonderful scholars and experts who talk about that. I'm not talking about that today. I'm talking about you and all the other grown-ups of this room. So yes.

Hi. Thank you so much for your talk. I just wanted to ask. I feel like a lot of what we're talking about, we're seeing this divide between safety and privacy, which we see in a lot of other spaces. So coming from background doing work in child exploitation, there really is this feeling of, like, get everything offline, but also this feeling of, like, I want to know what my kid is doing, I want to know where my kid is, and this feeling of the way to keep them safe is to surveil, which then creates all those other privacy issues.

So where do you think that middle ground lies of parents feeling like things are spinning out of control and they want more control over their kid, but also wanting to make sure that we're respecting kids' privacy?

That's such an insightful question. And you see it in schools as well, that they're saying in order to promote safety, we have to do more and more surveillance, more and more monitoring. Which we can query whether that's even addressing the safety concern and certainly can be creating other downstream problems with privacy and potentially safety if the data that the school is collecting is breached.

I would come back to this idea of a values-based analysis. So even before you get to the question of, is this particular product a good idea, is this particular watch a good Idea, think about, at the level of values, safety and privacy, but also autonomy and agency. So how do we balance those to try to further our goals here?

And I think one piece that is often left out of the safety and privacy discussion is this agency and autonomy piece. So parents are not going to be around all the time. School personnel are not going to be around all the time. I'm going to share about my son while he's out of the room. But he recently-- oh, you're there, OK. All right. No talking back. But I'm going to share it.

You tried to get me to let you walk to school by yourself, by saying if I gave you a Gizmodo watch, I would know where you were. And I told you that I wasn't going to do that because I don't believe in surveillance and tracking. And also you said to me, and if I get into trouble, I can call you. And I said, buddy, you can always call mom or dad about anything. But actually, when you are old enough to walk to school, and you, heaven forbid, do get into trouble, you can't call me first.

You need to find a police officer, a crossing guard, a parent you know, a teacher. Scream, run, make noise, even use your karate. We talked about that. And come up with a solution space around agency and autonomy. Because even if I know where you are, and even if you can call me with the push of a button, I may be 10 minutes away. That 10 minutes maybe too long.

And so I would say values-based discussion before you get to the level of coming up with a tech solution and making sure that those values are promoting agency and autonomy for kids and also equity and making sure that, particularly, as we move from a home setting into a school setting or a law enforcement setting, we're not unintentionally engaging in inequitable solutions. Sorry, Sam.

There is someone over here, if you want to-- and I think this is the last one.

So I have two questions. The first one was about, I was wondering what your thoughts were on that kind of paradigm shift that we see in the expectation of of privacy. And as parents become more and more comfortable with sharing, sharing their private-- how do you reconcile that with kind of the technology with that?

So thinking that we may be all be getting more comfortable with this idea of having information about us out there, I think that one of the ways we reconcile it is thinking about-- even as we may in certain domains be accepting more and more transmission of data, whether it's about our kids or about ourselves-- also recognizing that once people of all ages peel back the layers, they actually become less comfortable. And so I certainly accept that, in general, we are seeing a paradigm of letting more information out. Cathy O'Neil's book cites, I think, 2/3 of American adults have Facebook accounts. And that's just one of the many data points.

I'm not going to say that your general characterization about the paradigm is off. I don't think it is. But I think as you peel back the layers, when you see the Cambridge Analytica scandal break, when you see, as a parent, another letter in the mail from the school district saying that Pearson got broken into over the summer-- real world example-- you do start to become less comfortable and ask questions and raise challenges.

And I think actually that our kids and teens are savvier about this often than we are. I mean, think about the finsta, the fake Instagram account, so popular among teens where they're very savvy about privacy. And the Youth and Media team does a wonderful job unpacking this, that they can curate and customize how they present in different spaces in a way that, actually, even as they are using digital services and products-- and so they are letting some data out-- they're doing it in a very sophisticated, very curated, very principled way. So I think there's room for that kind of thoughtfulness and more complex response.

So I think with that we have to end. I would encourage--

I'll hang out and answer your question.

Yeah, please do come up and ask the rest of your questions. And I would encourage everyone to get Leah's book, which you can get right outside. And maybe we can all give Leah a thank you for this wonderful talk.

[APPLAUSE]

Thank you. Thank you.

Thank you.

Thank you, Sam.