Privacy Lost & Found
Interview with B.J. Mendelson

For podcast release
Monday 26 March 2018

KENNEALLY: This time, there was no need for any hackers. Data on the personal interests of as many as 50 million Americans flowed freely and legally from Facebook's open online platform to a psychology professor at Cambridge University who said he was conducting academic research. Then, the information allegedly landed at a data mining firm in London, where it was used to shape advertising and messaging in the 2016 US presidential campaign.

Welcome to Copyright Clearance Center's podcast series. I'm Christopher Kenneally for Beyond the Book. This week, Facebook founder and CEO Mark Zuckerberg faced calls from elected officials in the US and the UK to answer probing questions about his social media company's data gathering and data sharing practices.

The heat under Zuckerberg has cooled off Facebook share prices sharply and raised tough questions about the dilemma at the heart of social media. A handful of private businesses hold a vast treasure trove of information about billions of people around the world. Data hoarding is good business for Facebook, Google, and Twitter, as well for a host of opportunistic data brokers and data dealers. Their financial gain is often your privacy lost, says BJ Mendelson, author of the 2012 hit *Social Media is Bullshit*, a debunking of the mythical powers of the Twittersphere. His new book, *Privacy*, makes the case that your personal life is up for sale. Indeed, Mendelson declares that privacy as we once knew it was sold down the digital river a long while ago. BJ Mendelson joins me now from his home in upstate New York. Welcome to Beyond the Book, BJ.

MENDELSON: Thank you so much for having me. It's a pleasure.

KENNEALLY: It is a pleasure, and the timing is perfect for this discussion with you, BJ Mendelson, because the headlines this week are really about the very problem you identify in the book *Privacy*, which is the way that Facebook and other social media businesses collect and harvest and monetize personal data. The story about

Cambridge Analytica and the way it obtained this data through Facebook – it doesn't surprise you at all.

MENDELSON: No, there was a lot of eye-rolling when this story broke and a little bit of me hitting my head against the wall, because this kind of thing I've been writing about for almost a decade now. It's pretty common practice both with Facebook advertising and with other tech companies that follow Facebook's business model. So none of this is new. It's just unfortunate that we're finally now – maybe because it did or did not sway the presidential election – actually paying attention to what's going on.

KENNEALLY: Tell us about what we should be paying attention to, BJ. Because this is something, as you say, that has been going on for a fairly long time. It's common practice in Facebook. In fact, as many have observed in the media, this is a feature of Facebook, not a bug.

MENDELSON: That's right.

KENNEALLY: Over 10 years ago, Mark Zuckerberg made a critical decision to open up the Facebook platform to third-party developers, and it's that choice that has led to all of this.

MENDELSON: I think that it goes back a little further. You have to remember that the business model for most internet companies going back to 1994 is the harvesting and collection of people's data. So Facebook, when he did make that decision, wasn't doing anything unprecedented. It was just following what came before.

The other thing is that when this stuff happens, there's a sense in the Valley that you can just do it and no one cares. Because to them – you're talking about a lot of kids with billions of dollars being dangled in front of them. They're going to do whatever it takes to get that billions of dollars. So it doesn't stop and come into the thought process of what are the ramifications of what I'm doing? What are the implications of opening up my platform to all these developers? It's true for all of the platforms – not just Facebook, but Twitter also went through this, and Snapchat as well.

KENNEALLY: But they would tell you that at least over a decade ago, they had a vision – a vision of openness, a vision of sharing, and they couldn't have anticipated the illicit uses of data.

MENDELSON: That's a flat-out lie, honestly. (laughter) The tech companies have done a wonderful job, fortunately for them, unfortunately for us, of painting themselves in this almost utopian kind of brush of being cuddly and friendly and promoting all these wonderful things. But the bottom line has always been since 1994, your data equals a whole lot of money, and they'll do whatever it takes to get as much of it as they can. So they've done a good job of copying Google, and Google copying Yahoo, and prior to that, some of the '90s dot-com bubble companies of putting on this friendly face, but all the while, it's a ruthless business operation. It always has been.

KENNEALLY: You look at some of the myths of the social media environment, of the digital environment – not just limited to social media. It's largely about that, but not exclusively. One of the myths that you look at is the notion of anonymized data – anonymous data. You would say, I guess, that that's an oxymoron.

MENDELSON: Yeah, there's no such thing. (laughter) What I tell people is if you hook up to the internet, you can kiss your privacy goodbye. Anything you do after you're connected, regardless of the device, someone somewhere is able to capture and collect that data. So this mythology of we have this information that's been anonymized – it's never been true. It takes very little work to actually find out who you are from the data that's "been anonymized." So again, it's just about putting a smiley, cuddly face on something that is a really shady business practice.

KENNEALLY: The other thing that the businesses have done is to make it our responsibility, BJ. They tell us that we can opt out, we can make some choices – and maybe in a minute we'll talk about some of the things that listeners can do to protect themselves, to at least maintain whatever privacy they have left. Making it the consumers' responsibility, in your view, just isn't fair.

MENDELSON: No. I compare it to putting a Band-Aid on a bullet wound. More often than not – just recently with the Cambridge Analytica thing, Facebook was blaming its users for downloading the app and utilizing it. That, to me, is just insane. Because if you look at the privacy settings they do give you, while you have some control, it doesn't cut off about 99% of the flood of information that's being collected about you. There are the things like keystrokes and microphone data and things of that nature that Facebook doesn't want you to know that it collects. You can't even begin to cover that up using the privacy settings. So to say that it's on the user or to say, well, they read the terms of service to me is the height of arrogance.

KENNEALLY: Let's get this one out of the way. Should I tape up the camera and the microphone on my laptop or on my phone?

MENDELSON: Yeah, absolutely. (laughter) I always tell people if you don't want to do tape, use a Post-it note. It's by far the easiest thing you could do right now to protect your data. Because if you have a camera that's connected to the internet, it's not that it will be accessed, but it can be accessed. So if you want to minimize that threat, then all you have to do is cover it up.

KENNEALLY: Well, anyone who's listening, BJ, might roll their eyes about this, but we should tell them that none other than James Comey, the FBI director, when he was still at the FBI made the very same recommendation.

MENDELSON: That's right. And for what it's worth, Zuckerberg also has tape over his laptop camera. So what does that tell you?

KENNEALLY: Yeah, really. But the problem with some of this is that we confine it to the digital age, and we look back prior to the arrival of the web and think that was a golden age of privacy. But your book makes the case that at least when it comes to corporations and their willingness to hand over data to the government, at least, this is nothing new.

MENDELSON: Yeah, this has been going back since World War I. The federal government's been spying on people almost since the beginning of the United States in one way, shape, or form. The example I like to give people is Abraham Lincoln listening in on the telegraph to pro-South propaganda or people that were trying to destabilize efforts by the Union to recruit troops and then having those people arrested. That's a thing that happened that we don't talk about. So I have stuff like that. And during World War I, you had the passage of the Espionage Act, which basically said, look, the federal government has the ability to look at all the information being collected, and now thanks to technology finally catching up, we're able to access that technology and everything that's happening on it in the interests of national security.

KENNEALLY: The argument then and the argument now is that if you've got nothing to hide, you've got nothing to worry about. But in this quaint notion of privacy, we all have something to hide.

MENDELSON: Yeah. I was talking with someone the other day about this, and I said to them, if we all have nothing to hide, why aren't we all naked?

KENNEALLY: Well, because (laughter) I would get arrested. But I think the other reason is because I don't necessarily want you to see all my flaws, etc. Right?

MENDELSON: Exactly. That's an extreme position on that. But another one that's been staked out by Glenn Greenwald is if you have nothing to hide, why don't you give me your password to your email account and let me go through it and look at everything you've ever sent? Universally, people refuse to do that, because there is ultimately something that maybe you don't want to hide, but there are certain contexts where that information could damage you in some way, shape, or form.

In the book, I always blush when I tell people this – I joke about my porn preferences. I'm very open about it, but that's not something you want your employer necessarily to know, regardless of whether or not you have something to hide. So we always do have something that we want to conceal in one way, shape, or form. The downside to using any internet-connected platform is that it opens up the door for those things to be revealed.

KENNEALLY: Of course, Glenn Greenwald, for folks who may not immediately recognize the name, is the *Guardian* journalist who broke the story with Edward Snowden regarding the gathering of data by the National Security Agency and other federal agencies. So it has gone from being conspiracy theory to reality for many of this. Who can we trust today? Is there any reason for thinking that things aren't quite entirely dark?

MENDELSON: It's interesting, because every time that I've talked with someone about the book, they always say that it's very dark and very – not depressing, but overwhelming. I don't really see it that way. I see it more as now that all of these cards are on the table, there's a lot to look forward to. Because now, you have states like Washington that has privacy written into the state constitution. The city of Seattle has a privacy czar that's looking into the collection of data and how to best do that in a way that protects people's personal life. So we're now at that moment where there's a lot to be optimistic about.

The only thing to be pessimistic about is whether or not the federal government acts on what's happening with things like Facebook and Cambridge Analytica. They have that FTC consent decree from 2011. If it's proven that Facebook violated it, which I don't quite think they did, they would be responsible for trillions of dollars' worth of fines. And then you have a lot of senators that are calling for Zuckerberg to testify. That's all great. But going back to at least the

Obama administration, we've more or less given the tech companies a pass when it comes to things like this, so I'm not too optimistic about that.

But I am optimistic about everything else. I said that I wrote about this stuff almost 10 years ago, but back then, people kind of looked at you like, what are you talking about? Facebook is wonderful. But now, finally people are starting to go, oh, all these things are happening. What do we do about it? So I'm pretty optimistic.

KENNEALLY: And it certainly seems at the moment, at least, that the real concern is bearing fruit at the local level. You mentioned Seattle and various states. So either at the city level or at the state level, if the federal government isn't prepared to do something about this, there are other avenues.

MENDELSON: Yeah, I think that's one of the big takeaways from my book, is I have no confidence in the federal government to do much of anything. That's not necessarily a Democrat or a Republican stance. It's just I'm a big American history buff, and throughout history, we've only made changes incrementally. And unless something big has happened, it just doesn't happen on the federal level. So for us, the states are – we're starting to see progress with – I mentioned Washington and New York City. They've passed a law where they're investigating the uses of algorithms and the data it collects to write new decisions against you. That kind of thing is wonderful. So it's happening. We just have to be a little bit more organized in asking for our state representatives to take that step forward.

KENNEALLY: We are speaking right now with BJ Mendelson, author of the new book *Privacy*. BJ, let's tell people about a couple of things they can do right now if they really do still have this idea that some of what they do is worth hiding. Where should they go? Apart from taping up the camera and the microphone, there are settings. There are some available free services online that can help.

MENDELSON: So I try not to advise people to use things like a VPN or the Tor browser, because I've found in advising that that it's a little too complicated for most people. So what I've done is two things. First, I recommend taking all of your passwords and putting it in a notebook offline that only you have access to. That sounds very old-school, but it's the only way to guarantee your passwords' safety, which would keep people out of your accounts.

You should also turn on two-factor authentication to all of your accounts, which is basically a fancy way of saying when you log into something like Twitter, you'll

get a text message with a confirmation code. So unless someone has that confirmation code, they can't get into your account.

The other thing is I highly recommend the services provided by the Electronic Frontier Foundation. You've got services like HTTPS Everywhere, the Privacy Badger, which are free tools they have on their site. Privacy Badger will stop a lot of the spyware from doing exactly what spyware does. HTTPS Everywhere will make sure that your connections are more secure when you're browsing. And if you want to take a little bit of a bigger step, there are tools like the Brave browser, which can be found at brave.com, which completely cuts off all advertising and spyware from your viewing experience. I found that that's pretty easy to use and install.

KENNEALLY: One of the things that probably annoys people most is that there are people out there making money off of my data. I think you suggest that we should all be paid for this use of data. We should be charging Mark Zuckerberg a licensing fee.

MENDELSON: Yeah, so that argument – it's funny. It's been around since about 2000, 2001, and it splits into two different groups. The first is the licensing fee, where Facebook would have to pay you – and not just Facebook, but any of the tech companies – would have to pay you a licensing fee. It probably won't be a lot of money, because the value of an individual user's data probably isn't worth all that much. It's more in the aggregate where it's worth a lot of money. But because they're making money off of you, you should have a say in that. I think that that's a basic economic fairness argument, that if someone is profiting off of you, why aren't you getting a cut of that?

The argument is that you should be paid for your time and attention using things like cryptocurrency, like the Basic Attention Token and some of the other things out there, where you would get paid as you give the data. That argument has really picked up a lot of steam in recent years because of the wave of automation that's happened, where essentially people are saying, look, when you give information to Facebook, you are, without maybe intending to do so, powering this next wave of automation, where jobs are going to be destroyed because of the data you're providing. That sounds extreme, but it's actually something that's happening right now. So in the interest of economic fairness, if those jobs are going to be replaced – if your job is going to be automated because of all this data you've provided, then you should be compensated in some way, shape, or form so you can learn skills to learn a new job.

KENNEALLY: Speaking about learning skills, there's a skill in understanding how your data is used – what you call data literacy. Should it be taught in high schools, do you think?

MENDELSON: Yes, absolutely. I don't even hesitate on that anymore. I don't know what it's like in other states, but in New York State, you do have to take a government and an economics course before you can get a Regents diploma, and I feel that those classes are perfect to spend a couple of hours talking about what happens with your data, whether or not you're compensated for it, what the long-term consequences are.

That's one thing we really haven't talked about, is part of the problem of privacy and data is that we don't stop and think about the consequences. We just think, OK, I'm going to log into Facebook and have some fun. We don't even think about the automation. We don't even think about the billions of dollars that's being made off of your information and your family's information. So I think it's important at a really young age to tell people these are things you should be aware of, and if you don't like what a company like Facebook does or what a company like Cambridge Analytica does with the information they've collected off of Facebook, these are the things you can do to stop it.

KENNEALLY: Well, if there is going to be a course on data literacy in a local high school, *Privacy*, the book by BJ Mendelson, may well be on that reading list. We've been chatting with the author, BJ Mendelson, here on Beyond the Book. BJ, thanks for joining us.

MENDELSON: Oh, thank you so much. It was a pleasure to be on.

KENNEALLY: Beyond the Book is produced by Copyright Clearance Center, a global leader in content management, discovery, and document delivery solutions. Through its relationships with those who use and create content, CCC and its subsidiaries RightsDirect and Ixxus drive market-based solutions that accelerate knowledge, power publishing, and advance copyright.

Beyond the Book co-producer and recording engineer is Jeremy Brieske of Burst Marketing. I'm Christopher Kenneally. Join us again soon on Beyond the Book.

END OF FILE