Episode 3, Part 2: Societies Online (Annie Galvin and Alice Marwick)

**Annie Galvin (AG):** Hello, and welcome back to *Public Books 101*, a podcast that turns a scholarly eye to a world worth studying. I'm your host, Annie Galvin; I'm the associate editor at *Public Books*, which is a magazine of arts, ideas, and scholarship that's free and online. You can read the magazine at publicbooks.org.

If you're enjoying the podcast so far, we would really appreciate it if you would subscribe, and even rate and review it on Apple podcasts. You can follow us @Public Books on Twitter and Facebook, and we would love to hear your feedback there.

So, when today's guest, Alice Marwick, agreed to appear on this podcast, I had *so* many questions for her that it felt truly impossible to narrow them down to a reasonable number.

**Alice Marwick (AM):** My name is Alice Marwick. I'm an associate professor of communication and principle researcher at the Center for Information, Technology, and Public Life at the University of North Carolina at Chapel Hill.

AG: Alice has researched everything from personal branding on social media to misinformation and politics. I'm not sure how she does *this*, psychologically speaking, but she has spent hours upon hours excavating the darkest corners of the internet—and I'm talking about white-supremacist websites and really misogynist discourses on Reddit and 4Chan. And, I think Alice does this because she really gets that we cannot understand technology without thinking deeply about what humans are doing on that technology.

So, I'm really excited about this conversation, and I hope you'll learn as much from Alice Marwick as I did.

[brief music break]

AG So I'd like to start with a question that we're asking all of our listeners and so the question is, what does being on the internet in 2020 feel like to you? So that can be a phrase, a word, a metaphor, a description, anything that captures the experience of being online in 2020 for you.

AM Kind of fun, kind of dull. I got that from Natasha Schüll has this great book called, Addiction by Design, about video poker machines and the phrasing she uses is a little bit different, but it's this idea that you are using things like video poker machines to sort of zone out from your regular life, that it creates this kind of interstitial space where the concerns of regular life don't really touch you, but it's not like a fun space or an ecstatic space, it's just kind of a null space.

AG Yeah, I think that's a really good, good way to put it. And you know, we all sort of pick our poison, our platform or game of choice, but they all seem to have that kind of, that effect on us so that's great, thanks. And so I think it would also help to give our listeners just a little bit of context and background about the work that you do, and your work as a scholar has covered just a really impressively vast range of topics related to the internet

from social media and internet community to misinformation, privacy, radicalization, and you wrote about openness in Wikipedia for Public Books. It feels like you have kind of covered every, all of the hot topics around the internet, so, could you tell our listeners a little bit about some of your most recent projects relating to the internet?

AM Sure, so when I describe I work I say that I'm a scholar of social media and basically anything about social media that interests me I feel free to delve into. And so right now I would say that my research agenda has sort of two branches. The first branch is critical privacy studies and I'm working on my second book right now, which is called, The Private is Political: Network to Privacy on Social Media, where I'm looking at how the impact of network to privacy violations are felt most deeply by people who are marginalized in other areas of their life. So I'm trying to integrate this critical theory of power into our understanding of privacy, and then my other set of interests have to do with disinformation, misinformation and radicalization, which I came to in the run-up to the 2016 election when I was a fellow at Data and Society and started looking at media manipulation online, and that's obviously like, that's the kind of new hot, sexy thing and the privacy thing feels a little old school at this point, but what both of them have in common is that they are trying to look at impacts of new technologies in a way that recognizes that those impacts are differential and that if we need to, to understand technology, we had to incorporate theories of power that are drawn from feminist theory, critical race theory and queer theory because they help us understand how technology actually plays out in people's daily lives. Like I'm not interested in making huge generalizations about tech does A or tech does B or Facebook does this or that. I'm interested in looking at both the positives and the negatives and nuances and recognizing that nothing is all good or all bad, and that when you actually get into how people use technology, you often find that the stories are more complicated or more complex than they might appear at first glance.

AG Yeah, I think that's so interesting how you are bringing these kind of, these areas from humanistic study together with technology studies, and we can definitely keep, I mean, this will come up over and over again in the conversation I think, but, you know, technology is, it's just kind of humans, especially social media, is just humans talking to each other and so if we don't think about the, you know, different intersectional experiences of being human, we're really missing everything in a way. ..., so our kind of larger question for this episode is what is the internet doing to society and in order to explore that, it seems crucial to understand how these platforms make money off of us, their users, and you know, I think a lot of hear about data a lot in the news these days, how these “free platforms” like Facebook, Google, Uber, all of our apps make money off the data they collect about users and sell to other corporations, but I think a lot of us, certainly myself included before getting into more of [unintelligible - 17:02]'s work, didn't totally understand how this happens, how if I buy a baby shower gift for a friend, you know, all of a sudden the internet feels like I'm expecting a child as well. So I'm wondering if you can kind of walk us through the journey of a piece of data. So if we focus on Facebook for a second. When I put a set of personal data into my profile, like

my age, hometown, profession, relationship status, where exactly does that data go, can you kind of walk me through the journey of that data from my fingers striking the keys to me starting to see these targeted ads online?

AM So Facebook is famously opaque about what its data practices actually are. So a lot of what I'm about to say is my best guess based on things that I've learned over the years about how a large social platform like Facebook works. And Facebook is probably the best at doing this. So say I, you know, say I'm scrolling through Instagram, which Facebook owns and I click on an ad for a fancy pair of slippers on Instagram, right, something, I get marketed stuff like that all the time, right, yoga leggings, direct to consumer slippers, all those kinds of things. I'm also a sucker for that kind of stuff and I buy a lot of it so they already know that, you know, you show me fancy slippers maybe I'm going to buy them. So I click through to the website and I complete the transaction. So I've now bought slippers. So, Instagram and Facebook, which is the same data backend, right, they share all the same information and the same profiles about their users, they now have another piece of information about me. They know the time of day that I clicked on the ad, they know how many times they showed me the ad before I clicked on it, they showed me, they know what I was doing before and after I clicked on the ad … So that piece is, that piece of information about me, which they already have my age, my closest friends, what my closest friends buy, they know where I live, they know how my tastes have changed over the years, they know how much money I'm spending through all of these ads, etc., so this new piece of information about these slippers gets added to that data profile. Now, Facebook has made a big push over the last five years to try to integrate what you do online with what you do offline … So what Facebook has done is invested really heavily in what is called onboarding, which is integrating your offline and online profiles. So if you go to J. Crew and you give them your e-mail address at checkout, which a lot of the time every store is going to ask you for your phone number or your e-mail address, that acts as a unique identifier that they can then match up with the data profile that they have on you on the internet. So they know how much money I'm spending in Sephora online, and they know how much money I'm spending at Sephora offline, so they can look at the, these slippers that I bought, they can look at other purchases that I've been making on other websites. They have a fairly comprehensive understanding of what my consumer behavior is at this point. So then they are able to do predictive modeling to decide what are the things that they can show me that I would be the most likely to click on. And they do that by classifying me as a consumer in some way, so they will, they have probably a consumer profile that is like, you know, upper middle class, 40 something, suburban mom, that, or something like that, right? Interested in fashion and entertainment and books. Put me in that bucket and then they are going to serve me ads that are similar to ads that other people who are like me have clicked on. Then they are also going to use the slippers ad and say, okay, well what other products are like these slippers. You know, maybe they have other kinds of shoes like Rothy's or whatever that they are going to show me. So they are putting me in a, they are using this enormous amount of information they have about me, and they are combining it with information they have not just about me, but

about everybody that I'm connected to and about, you know, a large demographic group of people who are similar to me to predict what I'm going to do when I'm online.

AG Right. Whoo, that is quite a journey, that, so it helped me understand better, yeah. Alice, when I was reading your work, one thing that I learned about from it that I didn't know about really before was these third party data brokers, who, and please correct me if I'm wrong, yeah, basically act as kind of third party mediators between, or a third party marketplace between the apps that are collecting the data and other corporations, who can use that data for their marketing purposes. Can you tell us what a data broker is and what it does?

AM A data broker is a company that buys and sells personal data. So, they aggregate data from like a huge variety of sources, so public records like mortgage records, driver's licenses, campaign contributions, in some states gun licenses, anything like that, along with any information that they can mine off of just scraping social media sites. Combined with these consumer profiles that are created on social media sites or by different companies, and then they slice and dice all this data in a million different ways and they sell lists of people to different actors. So, say you are starting a, say you are starting a magazine for a cigar smokers or something, it's probably a poor business decision in 2020, but say that's what you are doing, and you want a list of people you think might be interested in this. You can go to a data broker and you can buy a list for that. You can also buy a list of people who are older, who have less money, who are maybe in financially difficult straights. If you are, you know, if you are maybe doing a somewhat illegitimate or less legitimate business, like you want to send I don't know, lottery come-ons or commemorative plates or MLM's or some scammy thing, you can also buy lists of people that you think might be more likely to fall for those things. And then -

AG Ugh, great.

AM - so all this information is totally opaque, it's really hard for people to see what information the data brokers have on them. Sometimes they sell this information to the U.S. government, even though some of it is information that the government isn't legally allowed to acquire and because none of us know what is in those files, none of us know when decisions are being made based on this data.

AG Right.

AM Because this data gets used in a huge variety of different ways, from policing algorithms to, you know, these, these databases that determine whether you are a good credit risk or whether you might be a good employee or even whether you might, you should be accepted into college or not.

AG Yeah, yeah, and I definitely want to talk a little bit more about those issues in a bit, but I just wanted to follow up and ask are these data brokers, I mean, is this a new, like a new phenomenon that has grown up alongside the internet and the extremely, the extremely

fine tuned micro-targeting that can be done, or were these a feature of advertising prior to social media?

AM They start with sort of direct mail and junk mail solicitation in the 80's, maybe 70's and 80's and then they get bigger and bigger and bigger, and more concentrated the more you go on. So the modern ones like Acxiom are very much tied to the emergence of the internet. The ability to micro-target is so much more sophisticated than it was 30 years ago, right? Like you can decide that you want to buy a Facebook ad that is targeted to people who are within 25 and 30, who live in the Lower East Side and Murray Hill, who are into astrology and who have a cat. Like you can go on Facebook and you can fill out all those fields, and you can say, okay, my new age pet emporium on First and Houston, this is where, these are my potential customers, right?

AG Yeah.

AM So the ability to collect all that information about people and also the way to be incredibly agile and nimble with it, to be able to target really quickly and really precisely is new because of the internet.

AG Yeah, right, okay. Yeah, I mean, what you were just saying about how, I mean, what really kind of blew my mind about what you were saying is the way that our online behavior and offline purchases are starting to be more and more integrated. Because that, I mean, I think when we are online, we are sort of aware that, you know, someone is watching us, we're being tracked, but that just feels like, I don't know, it is just crazy that, you know, I purchase things online and offline, and I really had no idea that that was happening.

AM Yeah, I mean, a couple of years ago I realized that virtually all of my students, who at the time were young Millennials and who are now kind of like the older Gen Z, they all believe that their phones listen to them and that micro-targeted advertising was delivered to them based on the things that they said to their friends or their mom or whatever. And no matter how much Facebook says that is not true, and how often I hear from engineers that is not technically possible because of the amount of data that would have to be processed in real time in order for that to happen, the fact that people think that is real is because these data practices are so unbelievably intrusive that we don't even realize how much data is being collected. They don't need to listen to us. They know where we are.

AG Yeah, they don't need it.

AM They know where we are when we are walking around. They knew who we were interacting with, right? Like, if I'm chatting with someone on Instagram, Facebook knows that. If I'm tagging a friend in a, in a picture that I took yesterday, Facebook knows where and when the picture was taken. It knows who is in that conversation. Yes, there are still enough uncanny coincidences that I still somewhat think Facebook might be listening. It's really hard not to believe that sometimes, but it really is a factor of the amount of

information that is out there about us that is being collected without our consent, without our knowledge and without basically any governmental oversight whatever.

AG Right, yeah, I mean, that notion that they almost don't even need to listen to us is really freaky, you know, that there are, these practices are so sophisticated already. Wait, what was I going to - oh yeah, and I mean, I think another thing that I learned from your work about the data brokers, I think a lot of times when we are, what we're talking about when we are talking about data sharing and privacy is consent in a way and it gets so complicated when there is that third party because, you know, maybe we think, we think that we're just giving the information to Instagram, right, and so we think, well, what's the worst that can happen, you know, they'll sell me more minimalist, basic clothes that I probably don't need. But, you know, whatever it is kind of this closed loop of commerce, but that notice that the data could end up in so many places that we don't know about I think is really kind of insidious. Why don't we now get into, I want to get into some of your work about, that you mentioned earlier in the conversation about the way that privacy impacts, you know, different populations differently, and I know that your book is coming out soon about privacy and some of your recently published articles looked at how breaches in privacy affect different people, different people differently, so specifically women and lower income Americans. So let's start with gender. Can you explain what you mean when you say that privacy is gendered?

AM So when I say that privacy is gendered what I mean is that there are certain privacy violations that are more likely to happen to people based on their gender and that the impacts are going to be different based on gender.

AG Right.

AM So I coined this term in a study that I did of Celebgate, which was when a big trove of celeb nudes that were mostly selfies that were taken on cell phones were leaked to Reddit, and I was really interested in the sort of ethical ramifications of this because the difference between the way that the people on Reddit saw this, which was a sense of like entitlement and oh, oh, if they didn't want us looking at them nude, they shouldn't have taken these photos of themselves, versus the women whose photos were leaked, who basically to a one said this is a sex crime, this is a violation of privacy, this is a, this is sexist, this is misogynist. I really interested in that disconnect. So what I did was I looked at all the comments on this subreddit called r/theFappening and I sort of looked at the way that they talked about these celebrities and these women. And what I found is something that really kind of backed up another theory of privacy that a bunch of people have been working on for the last couple of years, which is that in the United States we tend to think of privacy as an individual responsibility, that you are the person who is responsible for your own data and if the data leaks, it's your fault, right? So if your password gets hacked, it probably wasn't a strong enough password. If your phone gets hacked, you shouldn't have taken those pictures to begin with. You shouldn't have left your phone somewhere. You shouldn't have been using a sketchy app or something like that, right? But what all this stuff ignores is the fact that these privacy violations happen

over and over and over and that they are basically inevitable and that people are resigned to them, and that people use social media or they use network technologies in general not in a way that they know at some point there will be some kind of breach, right? No matter how careful you are. There is no way to get around it because these technologies intrinsically connect people together … So there was this real sense of entitlement from these men of looking at these women's bodies and what we find is that there is this whole sort of set of privacy violations and this goes into a literature that a lot of other people have written about that is technologically-abled sexual violence, where you have all of these things like location tracking apps for example that an abusive partner might make their partner put on their phone, or doxxing, leaking nudes especially is a huge one, putting someone's, cutting and pasting someone's head on pornographic imagery and sending it to like their boss, their friends, etc., there's this whole sort of set of privacy violations that are much, much, much more likely to happen to women. And when I stopped seeing these as like these isolated incidences of harassment and started linking them to privacy and safety, I started understanding to what extent this was a gendered issue, and a lot of this stuff goes for non-binary and queer folks as well. I certainly don't mean to or insinuate that this is only for cisgender women.

AG Right, right.

AM But it is anyone whose gender I think makes them vulnerable in a way. That gender becomes what security, security experts would call an attack vector, which is basically a vulnerability that can be exploited. So if you have someone you don't like for any reason and that person is a woman or a non-binary person, then you can use their gender as a way to attack them.

AG Right, yeah, and I mean, when you are talking about that notion of, you know, men online feeling entitled to be able to view women's bodies and also the kind of ideology of individual responsibility, it starts to sound like, you know, in person sexual violations as well, right, that these two kind of ideologies dovetail together and it is just interesting to see the way that it all kind of, it feeds into the same issues that we were dealing with long before the internet.

AM Yeah, so I was really inspired by this strand of British feminist sociology that has been using this term called Safety Work, which is the work that women do to keep themselves physically safe in space. So, you know, holding your keys in your hand with one out like you are going to like stab someone with it. Looking behind you, avoiding certain parts of town, not riding the bus by yourself at night, being on the phone when you are in the Uber with your friend, like all these different kinds of things, right? There's this whole spectrum, and a bunch of women in British sociology had written about this for years and this woman, Fiona Vera-Gray kind of excavated this idea of Safety Work and brought it into the contemporary by interviewing all these women about like what did they do to keep themselves safe in their daily movements around the world. And I found this really, really interesting that this is a form of labor that is unequally distributed that women bear the burden of, and again, trans and non-binary people as well, in keeping themselves safe.

And I started thinking about, what if rather than thinking about privacy, the way that we try to protect our privacy as a set of things that are always lacking, we think about it as a kind of work that we are always doing. And so in my new book I've coined this term, privacy work to encompass all of what we used to call privacy protective attitudes and strategies and instead think about everything from having a password manager, to making sure you can't see through your curtains, to hiding your Social Security number to, you know, all of these different things as this sort of privacy work that because there is no systemic protection for privacy being violated, we all end up doing on our own time. And I found that both men and women engage in privacy work. I don't really see a big gender difference in terms of the types of privacy work that people do, but when people are very vulnerable, their circumstances make them vulnerable, their privacy work tends to be more elaborate, just because they have so much more at stake if it fails.

AG Yeah, definitely. So I want to shift to some of the work that you've done around, around poverty and lower income Americans and privacy, and you have a really interesting article and I assume you are writing about this in your book as well, about how data mining and privacy violations have particularly harmful effects on low income Americans, specifically in three realms: employment, so seeking jobs, college admissions, trying to get into college, and policing. And so why don't we focus on employment because we could talk forever about all three of them. If a low income American, who has social media, who has social media accounts is trying to get a job, how can the data that they enter on those social media profiles potentially be used against them?

AM So a lot of low wage jobs use many automated systems to hire … where people's information is compared, is, people's information is put into a database and they are looking for kind of red flags like should I hire this person or not? And so some of that is things like, do you have a low credit score, like I guess that somehow has an impact on your employability, I don't know what that actually, why that would make you a bad employee, but then one of the other things that they do is they mine social media data and so a lot of the times they will, there will be these products that employers can buy that will say go through your social media and say whether you are using curse words or whether you are talking about drug use, or whether you are talking about guns or something like that. And so you are taking all this information that typically an employer wouldn't have access to, you know, your private communications, your communications with your peers or your friends, and because it is on social media, a lot of the time it is accessible, and it is being looked through not by a human, but by an algorithm, and they will generate a score for you based on this information, like is this somebody that is worth taking a risk on employing, and the problem with that is that since you have no idea that that is why you were denied the job, you can't do anything about it, you can't correct this record, you can't say, oh, you got me mixed up with somebody with the same name, or that's a tweet that I made seven years ago, right, it has no bearing on my current life, so a lot of the times these systems will deny people jobs and people don't even know that that is why they didn't get the job.

AG Right, yeah. That's interesting, and maybe briefly could you touch on some of the ways that this is used in policing, just so, I think maybe people have heard a little bit about this, but what is something kind of startling that you found from your research about how, you know, voluntarily putting data into various online systems can end up affecting how policing is done?

AM So predictive policing is a policing technique where you are, it's almost like *Minority Report*, you are trying to figure out where the crime is going to happen before it takes place, because you want to be able to deploy your officers or whoever to parts of town where there is high crime rates. And we know that crime rate tracking like New York City's CompStat system, has had an enormous impact on the way that different communities are impacted by police and frankly by police violence, right? So predictive policing that uses big data is often using the same kind of information that drawn from social media, that are drawn from public records, to determine a threat score for individual houses, individual blocks or individual people. So the idea there is if a, you know, the cops get a call from, you know, One Main Street, and they look at their dashboard and it tells them that there is somebody at One Main Street that is potentially very dangerous, they might go in there with, you know, all guns blazing in a way that they wouldn't if they are going to like a white suburban neighborhood for example, where the threat scores are very low. But again the problem is that there is no way to correct this information, and in fact a lot of this information is incorrect … you know, it's bad enough when you don't get a job at Walmart because of something that an algorithm thinks you posted on social media, but it's much, much worse when you get into the consequences of deadly violence being used, right, like the stakes are incredibly high and unsurprisingly the threat scores are very tied to socioeconomic class and race. So, there is, there is a real call there by a lot of social justice groups and civil rights groups for more transparency on the part of police forces and localities and municipalities that are using these products because their decisions are being made about citizens and residents based on information that those people don't have access to.

AG Wow, yeah, that's, that's all really interesting, and I think, yeah, again, it's so important to think about the way that these issues impact people differentially, and I'm wondering if you wouldn't mind my asking about the current situation that we're living in … I think recently in the news we've started to hear a little bit about how obviously contact tracing is one of the methods that the experts are mentioning as being crucial to containing the further spread of the virus as more people return to public life, and I think it's not very hard to imagine how GPS tracking on smartphones could be mobilized to help with this, so, you know, maybe it's a good thing that, that, you know, this data on where we are and who we have been in contact with could be traceable, and so I'm just curious about whether you've been thinking about privacy in the context of the pandemic and some of the tools that people are starting to talk about and even build toward this end?

AM So the problem with these kinds of apps that are trying to, or these kind of companies or initiatives that are trying to build these systems is not necessarily the systems themselves,

although, generally we find that when people build systems the same biases that those people and the society that they live in hold, those get put into the systems.

AG Right.

AM The real problem is overreach and abuse because we have very weak data protection laws in this country. We have very weak laws around what information the government can and can't have access to and we're very bad about keeping information in silos … And in this situation, even if you have all this information about people's interactions that is in the system that is supposedly for public health, right, or that is some kind of anonymity to it, we've seen over and over and over and over again that when you have all of these data points, not only is it extremely easy to identify people based on these data points, there's also such a huge push for that same information to be used by the government and by police, right?

AG Yeah.

AM So I don't believe for one second that any of these apps would stay in the public health realm, even if the people who are designing them have the best interests of everyone at heart. Clearly, it does seem like contact tracing is something that is pretty necessary to contain the pandemic, but I just worry very, very much that once this information is tracked and once this information is digitally instantiated, it can now be moved around and combined with all kinds of other pieces of information to do many things that are probably more nefarious than we might want to imagine, right, like, think about the way that you could, you could combine that information with immigration databases or with ICE databases to try to do targeted deportation raids, right? It is very frightening, and so my worry here is that we're opening a door that may, we just, it is justified by saying, okay, well this is the pandemic, people's lives are at stake, we need to do this, but it is going to open the door to using this data for all kinds of other ways that we probably wouldn't think were socially responsible or acceptable.

AG Right, yeah, and going back to that issue of us giving our consent to this kind of thing, right, we might think, well yeah, I'm doing this in the, right, in the interest of public health, that's what I'm agreeing to, but we don't know what's going to, where that is going to lead. So I want to just ask about one last issue before we start wrapping up and that is your work on misinformation online. I know we're kind of jumping all over the place.

AM No, that's fine.

AG Because you've covered so much ground, but you, yeah, and so, you know, I think in the wake of the 2016 election, we all heard a lot about fake news, alternative facts, the spread of misinformation online, and there has obviously been a lot of kind of pundit chatter about that. And in 2017, you and Rebecca Lewis published this really fascinating report with Data and Society called Media Manipulation and Disinformation online, and we can definitely link to that, and I follow political news pretty closely, but your report really yielded some findings that still surprise me, and I'm wondering what in the course of your

doing your research for that report, what were some of the findings about misinformation online that surprised you the most?

AM So we were doing a very specific set of qualitative observations. We were spending a lot of time in these kind of far right or alt right spaces. So we were on 4chan every day, we were on Gab, we were looking in different discords and different, you know, white supremacist blogs like the *Daily Stormer*, like we were in the fringey parts of the internet.

AG Yeah, you were deep in there.

AM Yeah, yeah, and what we, what we found was that there are all of these narratives that are bubbling up in these really, really fringe spaces, and they are being strategically mainstreamed by the participants. And those participants are looking for vulnerabilities in social platforms and in media institutions in order to spread often watered down ideas, but, versions of their ideas, but ideas nonetheless that are completely coherent with a project of white supremacy, right, or a project of creating a white ethnonational estate, and, you know, I had been following a bunch of these fringe groups for years, like I find the men's rights movement like extremely interesting for I don't know why. And I've been following them for years, and I had kind of some, you know, I had some interesting, like I had some interest in some of these fringe groups, but what really stunned me was to the extent that they were successful in getting their ideas out into the mainstream in a way that really fundamentally changed modern political discourse around things like race in a way that I don't think I would have been able to predict, right, before the 2016 election. Like I didn't think that anti-Semitism was going to become as mainstream again as it, as we see that it is now, right, where you see anti-Semitic ideas being thrown around in a lot of different spaces online in a way that, you know, me in my naiveté, I thought, okay well that's a thing of the past, right, or at least those of, you know, those of us who struggle with anti-Semitism, not on a daily basis, right?

AG Yeah.

AM So the sophistication by which these actors understood the way that modern media functions, you know, journalists who are super overburdened, they are doing like five different jobs, they are, or their job requires writing ten blog posts a day so they are getting most of their sources from Twitter, or they don't have the shoe leather to go out there and be interviewing people, they were falling for these like hoaxes and pranks and trolls nonstop that got the alt right really so much more, so much more media attention than they should have gotten. And I see it happen over and over, like just very recently with these reopen groups. This is a tiny fringe number of people compared to the number of people who are staying home and doing like nothing and doing, you know, wearing their masks and wiping down their groceries. That is what most people are doing. These reopen folks are a tiny, tiny set of people that in some cases are being directly funded by political actors, and yet the amount of column inches that has been devoted to these people versus the amount of column inches that are being devoted to the, you know, your average person who thinks these things are absolutely necessary and that we should

continue staying home, it's the ability to manipulate the media's love for political spectacle and the sort of contrarian idea or this idea that you have to see both sides of every issue, which is preposterous and at the same time, it's really effective. So it was very dispiriting to me to see that over and over again social media platforms and journalists were playing key roles in amplifying these narratives and that social platforms have been very inadequate in their response to their type of amplification.

AG Yeah, I mean, I think that is what struck me so much reading your report is that, you know, maybe I've never been on 4chan or QAnon [ph. sp.], I've never read the Daily Storm or certainly, but I could read, you know, I could be a consistent reader of The New York Times or the Washington Post and essentially be seeing these conspiracy theories being given, hold on, sorry, you know, being given real legitimacy, and just sort of skewing my sense of what is actually, you know, what is actually happening out in the world, so that was super interesting and I appreciated that, yeah.

AM The other thing I'd like to mention is that often when disinformation or misinformation is discussed in the abstract, people seem to see it as like, oh, this is incorrect information, this is inaccurate information. This is like information that is just wrong. But it's not just that. It's deeply ideologically skewed information and it is almost always racist, misogynist, anti-Semitic and xenophobic and without understanding that, that focus, we miss the forest for the trees and we're unable to solve the problem because if you can't understand that racist disinformation is playing off of a 400 year history of American racism, then you are not able to use the tools that you need to stamp it out, right? Or to combat it. And so I've been very frustrated because I'm always pushing this agenda that the, the way that this stuff gets into the mainstream is it uses these like wedge issues that are more acceptable to a lot of people. So for example, when the alt right is recruiting young men, they start with anti-feminism always. They are always like, you know -

AG It's the gateway.

AM Yeah, it's always like, oh, women are so uppity, you know, why won't a woman sleep with you, they all think they are so great, but women are enrolling in colleges in greater rates than men and men's suicide rates are higher and what about father's rights and yadda, yadda, and there's this whole spiel, right? And when the alt right is trying to make inroads into mainstream conservative communities, they start with anti-Muslim, anti-immigrant attitudes. And a lot of communities, anti-trans attitudes or anti-non-binary attitudes are where it starts. So you have these issues that are, you know, they are more acceptable, and that, and those, that's the way that these discourses start and then as you get more and more into them, then you start seeing the virulent racism or the virulent anti-Semitism, and it really, without acknowledging that and without acknowledging those connections to mainstream discourse, they are not solvable problems.

AG Right, yeah, and that feels like a genie that has been let out of the bottle that is just going to be really hard. I mean, I do want to conclude by talking a little bit about regulation and asking whether you have seen any, you know, positive steps in this direction or ideas for

how we can do that, but I mean, I think that at a certain point, you know, when we're talking about technology, we are sort of leaving the realm of technology and we're entering this more, almost philosophical or psychological or sociological realm, where we are sort of thinking about like what is wrong with people, it's not like the internet created these problems. They are longstanding human and social problems, so, I'm just kind of wondering, I mean, what do we, what do we with that, right, we can definitely start talking about regulating Facebook and trying to strengthen journalism again, but it just feels like some of these problems kind of exceed the internet, they exceed technology and that feels like kind of a harder nut to crack, or a harder thing to reckon with. How do you think about that in your work, sort of what is technology, what is human, and how do we, I don't know, how do we work to solve some of the problems that those two things together have created?

AM Technology is human, it's made of humans, it is made by humans, and humans use it to interact. It is social. It is used by people within social contexts. You can't extract technology from society. They are so inextricably intertwined that one doesn't exist without the other, yeah, I don't know if I 100% buy that, but you know what I mean, like there is this inextricable link between technology and society. So if you are saying, okay, well, there's a bunch of racism online, how do we fix that, let's use technology to fix it, you can't, because, you know, we have had a lot of very smart and very driven people for many years trying to eradicate racism and it is still here, it is still present with us on a daily basis. So, the, the question is, how do we acknowledge that existence and then do the work within technology that we need to do … A so, Europe has been sort of a leader in passing what I think they hoped were comprehensive data protective laws under the GDPR. Unfortunately, you know, I think those laws have a lot of great intentions. The way that they have been operationalized has not always been the best, but often when you are talking about the overreach by social media companies, you see lawsuits taking place in the EU or in countries like Ireland rather than in the United States because there isn't a regulatory board in the United States that is willing to actually take Facebook to account for some of these things. So for example, we don't have laws about data brokers. We don't have any laws. They are not, they are basically unregulated. We don't have laws about information from different, different aspects of life being integrated. What we do have is a sort of patchwork where there are certain types of personal data that are highly regulated, like educational records with FERPA or health records with HIPAA, but we don't have any kind of principles that would apply to all of those types of data. So for example, we have something in place called the video, I think it's called the Video Privacy Protection Act (VPPA), that was passed in the 1980's under Reagan during the Bork hearings for the Supreme Court, because Bork was badly embarrassed by somebody going and finding out a list of everything that he rented from a video store and that becoming part of the trial. So they then passed a law saying you can't, you can't get somebody's video records, like those are protected information. But at the same time, your, you can subpoena a cell phone company and get access to every single number somebody has texted without even telling them that that has been done. So there is no principle underlying it, it's just the sort of patchwork of different laws. And we do need

comprehensive data protection laws, but again I worry that we're not in a regulatory climate where those laws, any laws that would be enacted would really be well thought through or would have the impact that is intended.

AG So, to wrap up, the last question that we're asking all of our guests is what is the next big question that you think we need to be asking as we study the internet and sort of what it is doing to us as societies?

AM I have no idea. … Like there are so many interesting things about the way that the internet functions. I'm someone that always is going to want to ask like five or six questions rather than one. And that's why I'm glad there is such a strong set of people working on different aspects of critical technology studies and critical internet studies coming at it from, you know, computer science, from information science, from the humanities, from medial studies, from communication, sociology, anthropology, because we need, because this is such a comprehensive part of modern human existence, we need all the tools we have in our arsenal, every discipline, every method in order to investigate it fully.

AG Yeah, that's really well said, and I think it is, it is exciting how studies of the internet have become so interdisciplinary and so that's really great.

[brief music break]

AG: And that's our show! A huge thank you to Alice Marwick for sharing her thinking about data, privacy, and the human side of technology. You can find links to her work at publicbooks.org/podcast, including an essay Alice wrote for *Public Books* about Wikipedia and the politics of openness. You can follow this show, and *Public Books*, @PublicBooks on Twitter to learn more about the work we do. We'd be so grateful if you would subscribe to the show in Apple Podcasts, Spotify, Stitcher, or Pocket Casts. And if you like the show, please tell a friend, or even a few friends!

Next time on *Public Books 101*, I talk to two really exciting scholars doing cutting-edge work around culture on the internet: Lauren Michele Jackson and Richard Jean So. We're going to think about what happens in a space—the internet—where anyone can say (almost) anything they want, at any time. What's new about internet culture? How democratic is it, really, given that long-standing dynamics like cultural appropriation continue to flourish online? So I hope you'll join me for the next episode of *Public Books 101: The Internet*, as we ask: What is the internet doing to culture?

This podcast is a production of *Public Books*, in partnership with the Columbia University Library's Digital Scholarship Division. Thank you to Michelle Wilson at the library for partnering with us on this project. This episode was produced by me, Annie Galvin, with production assistance from Jess Engebretson and Kelley Deane McKinney. It was edited by Jess Engebretson. Our theme music was composed by Jack Hamilton. Special thanks to the editorial staff of *Public Books* for their support for this project, and

to the Mellon Foundation and the American Council of Learned Societies, where I am a public fellow. Thank you for listening, and I hope to see you next time.