The Measure Pod: #62 Debunking common cookie consent, GDPR and ePrivacy myths (with Rowenna Fielding @ Miss IG Geek)

Intro - [00:00:15]

Topic - [00:02:37]

Wind down - [00:35:57]

Outro - [00:37:31]

### Intro

[00:00:15] **Dara:** On today's episode, we're joined by self-confessed data protection nerd Rowenna Fielding who helps us to bust some myths, clarifying the difference between ePrivacy and GDPR, personal data versus PII, and first party versus third party.

[00:00:29] **Daniel:** And if you stick around towards the end, you'll see Rowenna do a real time live audit of our compliance on our own website on the Measurelab’s website. So you have to stick around and see how well or not so well we've done, but the verdict is in the episode. Hope you enjoy.

[00:00:43] **Dara:** Enjoy.

[00:00:44] **Dara:** Hello and welcome back to The Measure Pod, a podcast for people in the analytics and data world to talk about all things analytics related. I'm Dara, I'm CEO at Measurelab.

[00:00:55] **Daniel:** And I'm Dan, I'm a consultant and trainer at Measurelab.

[00:00:57] **Dara:** We're very happy to be joined on the show today by Rowenna Fielding, who is a self-confessed professional data protection nerd. So Rowenna firstly, hello and welcome to The Measure Pod. Thanks for agreeing to come on and chat with Dan and I.

[00:01:12] **Rowenna:** Hello, thank you for inviting me. I do love to talk about data protection.

[00:01:16] **Dara:** Brilliant, well our ears are going to be open for this and we're really, really looking forward to the conversation. But we always kick off, instead of me doing a really bad job of introducing you, we turn the tables. So this is your chance to introduce yourself to our listeners in as much or as little detail as you like really.

[00:01:33] **Rowenna:** Hello out there, I'm Rowenna Fielding. I work in data protection, which means I am a warrior on the front line of the fight to defend humanities rights and freedoms in an increasingly tech dystopia, which sounds much better when I say it at parties. I've been doing data protection and ePrivacy for more than 10 years. Before that I was a techie, I was in InfoSec (Information Security) and then before that I was a spotlight operator in the West End, as you do. So taken a bit of an odd career path to get to where I am now, but mainly what I do is I help organisations stitch together technology, law, and humanity in ways that hopefully makes stuff work the way they want it.

[00:02:14] **Dara:** That's such a brilliant description. I'm very jealous because we've talked before on here about how whenever we try and explain to people what we do, it comes across as either a little bit dry and boring, or they just look at us like they don't know what we're saying and they just think we're speaking another language. So you've done a brilliant job, I'm going to listen back to that and steal bits of that I think, when I'm next at a party and somebody says, what do you do for a living.

[00:02:36] **Rowenna:** Help yourself.

Topic

[00:02:37] **Daniel:** Rowenna, the reason I found you and I wanted you to come on the podcast was actually because I saw you do an amazing talk at brightonSEO a couple of months ago. And the title of that talk caught my eye. Not being in SEO myself, I tried to seek out all of the non-SEO talks, which sounds a bit odd to go to an SEO conference, but there's more to it than that. But your talk was on “cookie consent, GDPR and ePrivacy compliance”, and it caught my eye. The world that we are in right now, the world of analytics, especially Google Analytics is a bit under the spotlight, on the centre stage at the moment, it's almost a day-to-day conversation that we are having. So I just wanted to say thank you again for coming on, and I'm just wondering if I could maybe just throw some questions at you that I had off the back of the talk you did.

[00:03:15] **Rowenna:** Absolutely, hit me up.

[00:03:17] **Daniel:** Amazing, let's start really slow and easy, shall we? And one of the things that I really enjoyed in your presentation was the confusion and maybe clarity, or maybe you can help clear things up. What is the difference between ePrivacy and GDPR? Why is there two and why should we care?

[00:03:32] **Rowenna:** Okay, you can't see this listeners, but I'm rolling up my sleeves. Okay, so GDPR is a data protection law. So it governs what happens to personal data, that's information relating to living individuals. ePrivacy is a law that governs the use of electronic communications equipment over public communications networks. So while they're related to each other and they work together, they're not actually looking at the same thing. That's the basic summary of what the differences are between them, one's about people, the other's about kit.

[00:04:07] **Daniel:** Yeah awesome, and I love that explanation as well is that one is people centric, and one is technology centric. And I think where a lot of the confusion, especially from, you know, the people in our circles at least comes, is that a lot of people think that the view of a cookie banner or cookie compliance or these loosely defined terms come off the back of GDPR, and it's GDPR that made this thing happen where you get these popups on every website, but it's not really, it's changed it, but it was an ePrivacy thing to begin with, right?

[00:04:33] **Rowenna:** Yes ePrivacy law has been around, well, the European directive has been around since 2002, but it was the GDPR in 2016 that upgraded the definition of ‘valid consent’ to informed, freely given specific, unambiguous, evidenced and revocable and the websites out there that had not been getting that standard of consent had to obviously retool and hurriedly try and catch up with that work in progress.

[00:05:01] **Dara:** And there's a couple of examples where consent isn't needed, is that right?

[00:05:06] **Rowenna:** Yeah that's right. So ePrivacy law, it doesn't actually say cookies in the law at all. It's a bit about confidentiality of communications and it basically says you're not allowed to look at data or put data on or off somebody else's piece of, you know, end point device, piece of equipment, unless it's absolutely necessary to do so in order for the communication itself to happen, or it's absolutely necessary to provide a feature, an information society service is the language. A feature of the site or app or whatever that the user has explicitly requested or interacted with. So if a cookie doesn't fall into one of those buckets, then consent is required.

[00:05:51] **Dara:** And presumably if anything is bundled in with that, then that would require consent. So if somebody thinks, oh, I'm going to be really sneaky here and I'm going to try and collect some extra data as part of something that's necessary for the site to function, then obviously that would require consent. So if that data's being used for any, or sorry if some data produced by that function is being used for any other purposes, then consent would be required.

[00:06:16] **Rowenna:** Ah, so that's where the confusion comes in. So consent is for the setting of the cookie, as in the writing of data to the device or the reading of the cookie data from the device. That's completely separate to consent to process personal data under the GDPR. But because it's the same word, it causes a lot of confusion. So a cookie could be a dual use cookie, it could be something that is say, you know, for like bot detection or whatever, but is also the data from that is also being used for analytics. While the cookie consent may be valid, that secondary use of the personal data that's coming out of it, that would not be legitimate because you're not being transparent about what it's for basically. So there's a whole kind of tapestry of ways in which these two laws interact. The rule of thumb is there is no one size that fits all.

[00:07:09] **Daniel:** So specifically thinking about things like Google Analytics and the kind of stuff that me, Dara, and maybe a lot of our audience deal with on a day to day basis, am I right then in saying that you need consent to set the Google Analytics or any other analytics cookie? That's not up for debate, that is a thing that needs to happen.

[00:07:26] **Rowenna:** Yes, you are absolutely right. I mean, Google Analytics is an interesting one because even if you get ePrivacy consent as in consent to read, write and read from the cookie, you can't get consent for the processing of personal data that results from the setting of that cookie mainly because of the nature of Google, because it's so opaque and isn't really very good at following data protection law. So while you might be okay from an ePrivacy point of view, there are a number of reasons why Google Analytics is just not okay from a data protection point of view. It's worthwhile pointing here that law and risk are not the same thing, you'll get away with it but if you are strict about compliance with law and strict about data ethics, then staying away from Google Analytics is the way forward.

[00:08:21] **Daniel:** And that's a really, really important word, and something that I think about quite often is that it's not always about scraping the, you know, through from a legal requirement perspective, but there's also an ethical sort of side of it too and saying, well, just because I can doesn't mean I should. And there's a kind of, do you have the humanity aspect of layering the humanity on top of saying, well, is this okay? Even if it's legally able to be done, you know, I think that's a really fascinating field as a subject as well, and is so not black and white.

[00:08:47] **Rowenna:** Yeah, absolutely. I mean, the GDPR uses a lot of quite subjective language, like reasonable, appropriate, adequate, and where the ethics comes in is what the organisation sets as its boundary line not to cross. You know, what is reasonable, what is appropriate, what is adequate. And I find that these conversations usually start off with ethics and then when the ethics gets too inconvenient, it moves to law, and then when the law gets too inconvenient, it moves to risk.

[00:09:18] **Daniel:** Yeah, yeah. I've had those conversations for sure. We are not legal advisors, but we are getting asked in some cases, like what I'm deciphering it as is what are we allowed to get away with and what is it going to cost me if we get caught you know. And I think that's the risk side of it where it's the less risk averse or the more forward thinking. Just a side point on that Rowenna and something that you mentioned just a minute ago, and I think another thing just to kind of clarify or attempt to within the time that we have, and this is something I hear gets confused all the time. And the difference between PII, so Personal Identifiable Information and personal data because that's one of the biggest differences when the GDPR came into effect. And I think there's a lot of legacy, especially around things like Google Analytics that has terms and conditions referencing PII, but then we got the GDPR referencing personal data. And I'm just wondering if you can help us sort of understand that a bit better and clear that up a bit.

[00:10:02] **Rowenna:** Oh, you just keep lining up the soap boxes for me. So yeah, absolutely. So data protection law, all the way back to 1984, the UK's First Data Protection Act has always been about ‘personal data’. So that's a kind of term from EU and UK law, and it has a very wide definition, so it's any information, data, so on a computer or in a structured filing system relating to an individual who is identified in the data or can be identified via the data, so that's quite big. PII is more of an industry term from across the Atlantic. So there is no formal definition of PII in any kind of federal US law, but it's the common term and that relates to direct identifiers only.

[00:10:53] **Rowenna:** So for example, in the podcast recording if you say my name, Rowenna Fielding, that's my PII. But if you then refer to me as the oddly enthusiastic geeky data protection lady who came to talk to us on the podcast, that's not PII, but that is my personal data because it allows me to be uniquely singled out and recognised even though there are no intrinsic identifiers included. So PII is a subset of personal data.

[00:11:19] **Dara:** Sorry if this is a very basic question to ask you, because I'm sure you probably hear this all the time, but is there a blurry line then with personal data? Because how exactly do you define, at what point does it stop being uniquely related to you and become broad enough. So let's say in your example there, if we had another, and I'm using your words, oddly enthusiastic lady on the show talking about data protection, then that wouldn't necessarily be personal data to you anymore.

[00:11:44] **Rowenna:** That's right, you've absolutely nailed it there. So personal data isn't a static bucket that information goes into and never comes out of it's more of a dynamic attribute tag. So whether a particular set or piece of information is personal data will depend massively on the context around it, why it's being used, where it's being used, stuff like that. So IP addresses, for example, you write an IP address on a piece of paper and drop it in the street it could be anything like a geek would probably recognise it as an IP address, but it wouldn't point to anyone in particular. However, an IP address assigned as a static IP to your particular domestic internet connection when you are the only member of the household, that's personal data because it's a way of pinpointing and triangulating on you. So, yeah, and this is something that really upsets technical people, I found that personal data is not a binary and it's not static. That personal data tag is something that is attached and detached depending on the circumstances and the context, more the circumstances than the context than the actual data itself.

[00:12:51] **Daniel:** Yeah the context is key right? And is it right then that it's also about, so again, even if you had IP address, that could be fine, that could not be fine it's about the context. But actually, let's say we scrapped IP address, my brain works in Google Analytics terms, sorry Rowenna. But if we took things like city, device type, browser, time of day, and we combined those very independently, not personal data sets together. They become personal data because in a sense we are fingerprinting, right? We can identify someone from that so I think that's something that's come up recently in Google Analytics right. And it's that idea that just because you're not setting a cookie, if you track everything else, it still can become personal data in a sense, right?

[00:13:26] **Rowenna:** Yes, absolutely. That's kind of at the core of why a lot of Google's T&Cs and all that jazz just don't legally stand up, although no one's had the cash to really call them out on it so far. So it's not something that can be really easily and quickly and simply defined. You know, I get asked a lot of the time for, can you just give me a list of what is personal data and what isn't personal data. And I have to deploy the two most used words in any data protection persons lexicon, which is ‘it depends’.

[00:13:59] **Daniel:** Love it, I use that all the time, I think we all do, that's amazing.

[00:14:02] **Dara:** Unfortunately I didn't see you speak at brightonSEO, but I have seen the slides and you talk about the confusion around first versus third party and people wrongly thinking that if it's first party, it naturally means it's okay.

[00:14:14] **Rowenna:** Yeah, so the whole first party, third party thing, that's industry terminology. There is nothing in ePrivacy law that differentiates first from third party. It's all about the function of the technology itself. Reading and writing from an endpoint device and the degree of necessity of that operation for actually making the communication happen. However, just to make things interesting, in data protection, it does make a difference because there is a disclosure to a third party and often personal data generated through the use of a third party cookie results in what's called a joint controller arrangement relationship between the site operator and whoever the third party is. So it doesn't make any difference for cookie consent. It does make a big difference for fairness, lawfulness and transparency of processing of personal data, which is what the GDPR is all about.

[00:15:08] **Daniel:** Clear as mud, right? No I do get it, I jest. But yeah, I mean this is the thing, and I think this is the biggest issue or the biggest confusion that I see, and it's the conflation of legal jargon and technological jargon, and the confusion between what Google Analytics, for example calls something, what my consent management platform calls something and what the law says. And I think there's an overlap with all those and for example, even just the term consent management platform, most of the time we're talking about just cookie consent, right? And we throw “cookie banner” up as kind like, I have consent to do anything ever, not just set the cookie on the device, which we are consenting to. And I think that's the biggest confusion that I'm very much aware of is that what are we getting consent from and what do you mean by cookie consent or consent in general? Like the idea of the tech side of it versus the personal side of it is very, very conflated.

[00:15:57] **Rowenna:** Yeah and call me suspicious minded, but I get the sense that a lot of that obfuscation has been encouraged because it is convenient to industry. Yeah there is a lot of confusion and also that you know, what the law says has to be thought about in order to be applied to what's happening in front of you. Neither law, GDPR or ePrivacy directive, neither of them are a simple one size fits all checklist for every possible scenario, they've always got to have some thinking behind them. And so if the person doing the thinking is thinking, how can I get away with something, then the result will not necessarily be of great legal quality. Whereas if the person doing the thinking is thinking, how can I, in good faith, do what the law is requiring me to do here. Then you get, you know, more granular and more clear explanations. Sadly, that approach does take more time, effort, and money so it's not terribly popular.

[00:17:00] **Dara:** Can I play devil's advocate and play the other side and of a conversation that I had a long time ago now, but I'd love to get your considered and professional response, and that is when it comes to analytics, let's say Google Analytics, but you know, insert your analytics provider here. The argument of well it is functional, it is mandatory, it is essential for our business to operate. Without analytics, we can't measure what's going on, we can't make improvements and our business will go under. So it would just be a matter of time of stagnation and sort of decline before the business goes under, and that's because we can't optimise and improve and track. So that's me playing devil's advocate by the way, that's what I've been asked, what would you say to that?

[00:17:37] **Rowenna:** So I understand where that argument is coming from. In purely legal terms, the essential qualification is directly related to the site or app being functional in the first place. And because you can run a website without analytics, I do and mine’s pretty fast. You can't say that the analytics are essential for the communication to happen in the first place. What ePrivacy law doesn't do is pay any attention to the business model. It doesn't matter what your business model is, this is all about whether or not the communication is sufficiently confidential to meet these requirements.

[00:18:17] **Dara:** Something interesting you said there, you don't have analytics on your website, did you mean Google Analytics or you don't have any analytics?

[00:18:24] **Rowenna:** So updating myself I don't have Google Analytics oh no, I'm using Matomo but at the very, at the strictest kind of privacy settings. So pretty much all I see is hit count. I mean I don't rely on analytics really in any way for what I do, so I don't need it, and it also squeaks me out.

[00:18:45] **Daniel:** There's something that I remember from your talk though, and something you touched on there, which was essential, if it's essential to running the website. So we've all seen cookie banners that have, like, you can opt out of functional or performance or essential cookies. So there's a bit you said about that and I'd love to, I'd love to read it to you verbatim which was, “these are industry terms, not legal definitions, the only exception to asking for consent when a cookie is when it comms critical, that's it”. This is another one of those kind of like tech, useful to the technology or useful to the consent platform way to get around it from a risk perspective maybe but this is not a legal definition, right? There's nothing different between functional, performance, and essential.

[00:19:20] **Rowenna:** That's right and I mean the law itself doesn't define what is and isn't essential. It just says if it's essential for the communication to happen at all, then consent is not needed. So there's a degree of technological understanding required of whoever is making that judgement. And obviously, you know whether that judgement's being made in good faith. Because we're back to law, ethics and risk again. The law basically says you have to get consent for analytics, in terms of risk and business risk and individual risk. There is a world of difference between using analytics that's operated by a global surveillance company. Versus, you know, un-premised local analytics that doesn't do any kind of cross device tracking or correlation or behavioural profiling or device fingerprinting or data harvesting from a billion third party sources. So, I mean, it's kind of harsh for the law to say that analytics require consent, and my understanding is that the current draft of the updated ePrivacy law that's supposed to be, was supposed to be coming out of Brussels in 2016 and has been delayed, was going to make an exception to the consent rules for analytics that are privacy friendly.

[00:20:39] **Daniel:** So Rowenna can I play the devil's advocate again, just very briefly, because the other aspect of your talk, which was amazing by the way, but also the other aspect of what we see in cookie banners, but we also hear in the industry is the term and be ready for this, ‘legitimate interest’.

[00:20:52] **Rowenna:** Oh God.

[00:20:54] **Daniel:** I thought you would like that, I remembered that from the presentation. So tell us what's wrong with legitimate interest?

[00:21:00] **Rowenna:** So the requirement to get consent before setting or reading from a cookie comes from ePrivacy law. ePrivacy law gives you two modes to operate in, essential, comms critical that is, or consent, end of story. Legitimate interest comes from the GDPR and it's only applicable to the processing of personal data. So if you are setting a cookie that is not comms critical, then you have to have consent, legitimate interests just don't apply to the setting of cookies. It can apply to the processing of personal data that happens as a result of setting a cookie, but only if that cookie was set legally and only if the test for meeting the legitimate interest criteria are met, which is that the interests are defined and attributed, so whose interests. That the interests being pursued are in fact legitimate and you know, not illegal or scammy or rude. That an assessment has been made which looks at the data flows and draws up a balance between the impact, the rights, and freedoms of the individual and the benefit to the interest being pursued.

[00:22:13] **Rowenna:** So legitimate interest comes way down the line after the consent thing has been satisfied. You cannot legally set a cookie on the basis of legitimate interests. However, industry has tried that because it's convenient for them and the regulators are starting to catch up and issue slapping for that, and not before time, I would say.

[00:22:32] **Daniel:** I like that. So to use legitimate interest, it has to be an interest that is legitimate.

[00:22:36] **Rowenna:** Yep and it has to come after consent for the cookie.

[00:22:40] **Daniel:** Yeah, exactly. I mean, again that's the thing that gets conflated isn't it? Is the sort of personal data processing versus the ePrivacy cookie compliance side of it. And you know, one does not imply the other, cookies are a method of collecting data of which you then need to apply the GDPR to if I'm writing my logic there.

[00:22:57] **Rowenna:** No, that's absolutely correct, yeah. And not just cookies but also tracking pixels and local storage objects.

[00:23:03] **Daniel:** There was a thing going around recently, not so recently now probably of using you know, the favicons, you know, the icon in the top of the browser, using unique ones of those as identifiers to track people across different devices, browsers as well, using cookies or local storage. And I'm like, wow, there's always going to be someone pushing their luck and trying to find a way around something that isn't there.

[00:23:20] **Rowenna:** It's an arms race because what industry wants is data and what people want is to be left the hell alone. So every time you know, you get a law or some guidance or whatever that says, leave people alone by following these rules. Industry looks for ways to wriggle through, around, under and over those rules in order to get data. And then people push back with privacy enhancing technologies and the law gets changed, and around and around we go basically yeah.

[00:23:51] **Daniel:** I can't understand the cognitive dissidents that the, you know, all marketing is run by humans and yet these are people that probably won't accept cookies because they know what's going on but they want their people on their website and they do optimisations to increase that pool of people that are optimising.

[00:24:05] **Rowenna:** Interestingly I've found that a lot of the people in digital marketing that I've spoken to are just fine with accepting cookies, mainly because they're from sufficiently privileged backgrounds that the adverse effects are not likely to be inflicted upon them, so they're not so likely to be discriminated against by having inferences attached to them which confer social disadvantage.

[00:24:33] **Dara:** That's really, really interesting. I hadn't even, it's almost embarrassing to say this, but I hadn't even considered that aspect of it before that's really eye opening.

[00:24:43] **Rowenna:** Yeah, that goes into data ethics and impacts and loads of fun stuff.

[00:24:48] **Daniel:** Rowenna, we're going to have to get you back on another episode to dig into that can of worms or open that can of worms as well. But I suppose this is been a very kind of like dash into, you know, the world that we are in and the world that we both inhabit. If I may there's one other aspect that I just wanted to talk to you about from your presentation from brightonSEO, and that is around, and this will lead into potentially something very fun, maybe fun for us at the end, but consent mechanisms, invalid consent mechanisms. I know you had examples which we can't show, obviously being an audio medium, but there was a couple of types of invalid consent where people are in a sense playing that risk game of trying to dupe people into consenting, even if it is technically valid consent, or at least technically speaking, whatever What are those things that people should avoid? What should people not do? And what are the kind of things that you see that makes you squint and get really angry?

[00:25:36] **Rowenna:** Well, the first one I would say is the kind of operating on the premise that it's easier to ask for forgiveness than permission when the requirement of law is that you get permission. So things like, yes, we're setting cookies click here to say, okay, thanks bye, with no option for no, do not set non-essential cookies, so that's not legally valid consent. We're setting cookies to improve the performance of our websites and with no other detail when actually there might be a whole load of ad tech retargeting, behavioural profiling, stuff going on under the hood so that's not informed, that's deceptive, so that's not valid consent.

[00:26:14] **Rowenna:** The use of what is often referred to as dark patterns, but is more sensitively referred to as deceptive design. Things like, you know, hiding the decline box in the same shade as the background, whereas the accept boxes, you know, huge and green. That's not technically unlawful but it does indicate bad faith and that's a red flag. Oh my goodness, there's so many, so many examples of this sort of thing. Making it harder to decline the cookies than it is to accept them. So if you can accept with one click, but you have to go through five clicks to decline, that's not valid consent because the standard of consent set by GDPR is that it shall be as easy to refuse or withdraw as to give.

[00:27:00] **Rowenna:** You mentioned earlier the categorisations of cookies. Those categorisations don't appear in law, but can be used to manipulate people into believing that they are essential and also just straight up misclassification of cookies as essential when they're really not. So yeah, there is a load of bad practice out there, and again, regulators are starting to crack down on it, but there's also a wider understanding among the public that an organisation which is trying to con you into revealing data about yourself is probably not an organisation you can trust to do business with.

[00:27:41] **Daniel:** I mean, if you had a brick-and-mortar store and someone walked in and you treated them the same way that you are on the website, you wouldn't, would you? It's not the kind of thing you would do to someone in real life, but when it's digital, it's almost like a different game, isn't it?

[00:27:51] **Rowenna:** Yeah the abstraction layer that digital gives us has resulted in people kind of happily doing things that they would be horrified to contemplate doing face to face, it's saying if you do X, Y will happen and you don't get a say in it.

[00:28:06] **Dara:** Because there's so many people doing bad things and there's a perception now that cookies are bad. And if you ask, you know, a person, regular person and ask them about cookies and you know, they might say to you, that's bad I just decline everything. So have you seen any examples of websites where it takes a basic bit of guesswork here so you don't know, obviously, how many people are consenting, but have you seen any good examples where people are presenting a good enough case where they're informing users of what they're going to do with the marketing cookies, meeting all the criteria, but also not scaring people away by thinking, I'm just going to click no, because there's nothing novel about this, there's nothing enticing me to dig into this and find out what they're doing with this information.

[00:28:46] **Rowenna:** No, not really. In all the cases I've seen where the functions of advertising, analytics, A/B testing cookies are explained, people kind of back away going, what the hell, no no no leave me alone. Some cookies, I mean, even when they're not classed as essential, which you know is dubious and borderline, things like bot detection, anti-fraud stuff, capture stuff, people are more inclined to accept those, but only as long as they can trust the party behind them. But the only high rate of cookie acceptance I've ever seen have been for sites which are not compliant with either ePrivacy law or GDPR, and they're using deceptive design to manufacture consent. Having said that, tracking cookies are still better than browser and device fingerprinting and server-side tracking, which is covert stealth tracking that is infinitely ruder than saying to somebody, do you mind if I stick a post-it on your back and follow you around the high street.

[00:29:53] **Daniel:** Yeah the server-side movement, you know, is hard because you can't tell anymore. You can't even validate it's almost like they're going to be secretive about it and they've just moved collection over to another place. I mean you can do it well, but I think there's always going to be bad actors and the thing is, you can't catch bad actors out when it's server-side right, that's the whole point, and you can't plug a browser extension in to stop them doing what they need to do on their server-side so.

[00:30:13] **Rowenna:** I mean, you say bad actors, but the harmful impacts of this kind of tracking, surveillance, categorisation and profiling don't require any malignant intent. The data harms that arise from them are just effects of being able to apply categories to large groups of people without their input or collaboration, and then treat them differently according to categories. That's always a dangerous, dangerous thing. You end up with situations like, for example, on Facebook. African Americans don't get shown ads for high value employment opportunities or housing or high value goods because a whole category of people has been labelled as not economically advantageous. So you don't have to be a bad actor to cause data harms with surveillance advertising, and I think that's a point that hasn't really sunk in for the industry, mainly because it causes a huge amount of cognitive dissonance.

[00:31:15] **Dara:** Is that like bias in machine learning algorithms? Would that be an example of what you're talking about there, where it's not necessarily somebody intentionally going out of their way to do harm, but they're using this data in some kind of algorithmic way to profile and that's then causing this harm to people.

[00:31:32] **Rowenna:** Yeah, I mean all data is inherently biased because data is created as the output of social and technological processes to serve a purpose. So it's not like we're scooping butterflies out of the natural environment and pinning them on sheets, we're creating something wholly artificial as a representation to meet a need. So no matter how much data you gather about a person, it will never ever be able to provide a complete picture of that person, their hopes, their wants, their dreams, their experiences, all that jazz. So all data is inherently biassed, the more you do stuff with the more data you have, the more bias effect there will be in the output. And machine learning essentially is teaching bias just in a particular direction and since surveillance advertising does rely on automation, not just machine learning, but all kinds of automation. We've come to a situation where it's faster, easier, and cheaper to apply bias than it is to think about how not to, and the effect of that on society. I mean, well just look around you, it's on fire.

[00:32:47] **Daniel:** So Rowenna, we had an idea and we don't know how well this is going to go for us, but if we could ask, while we have you on the podcast, would you be able to look at our website and give us your initial thoughts on how well or not so well that we are doing, it's measurelab.co.uk by the way. And you should, if you've not been there before, you should get served a banner, pops out on the left hand side and I will brace myself for your verdict.

[00:33:12] **Rowenna:** Okay you are using the same CMP as the ICO, that's pretty good. Things turned off by default, that's nice. The cookie consent, obviously you've got the categories of cookies and there, I don't see, okay, so there's no specific information about what the cookies are presented upfront. I would have to go to the privacy policy, which, oh dear me.

[00:33:42] **Dara:** It was going so well.

[00:33:45] **Rowenna:** Yeah, let's have a look. Yeah, so you still not actually itemising the cookies anywhere. So you're not really getting informed consent, although you are doing better at not getting informed consent than most organisations are. Just like with all of these, the only way that I can decline the cookie is to go in and manually delete it from my browser, which obviously is an effect of what cookies were designed for, but makes kind of valid consent sort of impossible. I'm not enough of a web dev geek to know whether or not it's possible for the server to send an instruction to the browser to delete a cookie, but that sort of thing probably should be considered. So you've got HubSpot running, mm-hmm. HubSpot is not essential by any means, so you would need cookies for that. You've got two third party cookies, one of which is Google Capture, oh, and a local storage object. And wowser, that would be 26 third party requests to 14 unique hosts, so there seems to be quite a lot of, with my data protection hat on, there's a lot of third-party tracking on your site, which I don't see explained terribly well in the privacy info. Yeah no, not at all.

[00:35:13] **Daniel:** A bit of work needed.

[00:35:14] **Rowenna:** Yeah.

[00:35:14] **Daniel:** That is really interesting and thank you so much for doing that and that's really enlightening. You've obviously put it into a tool there as you were reading from, if you could share the link with that to the side, what I'll do is I will unashamedly post the results of that in the show notes so people can see how badly or well we are doing. We're on a journey to get better at this kind of stuff and so we have to put our hands up and say if we're not doing something right at the moment, and we'll work on fixing it.

[00:35:35] **Dara:** Something else that I really liked and if it's available online somewhere, maybe you could share this also is your cookie handling decision guide which was in your slides. I thought that was great, I learned a lot from it. So I don't know if that's somewhere publicly accessible if you're happy to share it.

[00:35:51] **Rowenna:** I can't even remember if I put that up on my, buy me a coffee site, but if I didn't, I shall rectify that this evening.

Wind down

[00:35:57] **Dara:** Brilliant and we can include that as well in the show notes. So I've got two more questions for you. Some people think these are the easy ones, some people think they're the hard ones. The first one is, what do you do outside of work to wind down?

[00:36:09] **Rowenna:** I binge watch sci-fi and I binge read mostly sci-fi. I drink gin and I obsess over puffins, and I do embroidery.

[00:36:20] **Dara:** Amazing, I was going to say you sounded so similar until you said obsessing over puffins which is a new one. Brilliant, and why not.

[00:36:28] **Rowenna:** They're adorable.

[00:36:29] **Dara:** The second question, this is an easy one, if people want to find out more about you or they want your help, they want to engage with you and for your consulting services, what's the best way for people to get in touch with you?

[00:36:39] **Rowenna:** So I am terminally online, so the easiest and fastest place to find me is always going to be on Twitter @MissIG\_Geek, but I'm also on LinkedIn as Rowenna Fielding. I have a buymeacoffee site where I post both paywalled content and freebies. So that's, buymeacoffee.com/MissIGGeek and I have a website for my sort of consulting front end, which is missinfogeek.net. So yeah, I'm all over the interwebs.

[00:37:14] **Daniel:** Great, and we'll put links to all this on the show notes as well.

[00:37:16] **Dara:** So thank you again for joining us on The Measure Pod and I think we've signed you up through the process of this for coming back on and doing a data ethics episode.

[00:37:25] **Daniel:** And to our newsletters and all our marketing communication.

### Outro

[00:37:31] **Dara:** That's it for this week, to hear more from me and Dan on GA4 and other analytics related topics, all our previous episodes are available in our archive at [measurelab.co.uk/podcast](https://www.measurelab.co.uk/podcast/?utm_medium=podcast&utm_source=transcript&utm_campaign=62), or you can simply use whatever app you're using right now to listen to this, to go back and listen to previous episodes.

[00:37:49] **Daniel:** And if you want to suggest a topic for something me and Dara should be talking about, or if you want to suggest a guest who we should be talking to, there's a [Google Form](https://docs.google.com/forms/d/e/1FAIpQLSeMwfzg9TdNKeZYRxHci_y0D9up4EyAL5zNMYZNE9P_82fz3Q/viewform) in the show notes that you can fill out and leave us a note. Or alternatively, you can just email us at podcast@measurelab.co.uk to get in touch with us both directly.

[00:38:06] **Dara:** Our theme is from Confidential, you can find a link to their music in the show notes. So on behalf of Dan and I, thanks for listening, see you next time.