TECH REIMAGINED
AN ENDAVA PODCAST

Can a hyper-digitised society be ethical?

[00:00:11]
BRADLEY HOWARD, ENDAVA HOST (BH): Hello, I'm Bradley Howard, and I'm happy to welcome you back to the latest episode of Tech Reimagined. The topic of today's episode is ethics in a hyper digited world. Today we have John Buyers with us, and John's going to be explaining a bit more about ethics and law. To say he's an expert is an understatement. He literally wrote the book on artificial intelligence – and for listeners, I'm holding up Artificial Intelligence: The Practical Legal Issues written by John. So hello, John, it's great to have you here. Can you tell us a bit more about yourself and your background?

[00:00:43]
JOHN BUYERS (JB): Thanks, Bradley, and thanks very much for having me on the Tech Reimagined podcast. Well, yeah, I'm a partner at Osbourne Clark and I lead the commercial team at Osbourne Clark, and I'm also for my sins a technology transactional lawyer - an emerging brand, an AI lawyer, as you've intimated. I've spent a long time, my whole career, essentially, in the technology industry, working in house initially at some very large technology services providers where I learned all about traditional outsourcing and other technology transactions transitioned into private practice. At the same time, I've seen the outsourcing industry move into a much more tech enabled space, which is what piqued my interest in artificial intelligence… and, as you intimated, ended up in me writing the book that you just plugged.

[00:01:36]
BH: I hear there's a third edition coming out soon as well.

[00:01:38]
JB: There is, yes. Yeah, I got a headache as soon as I hear that. But there we go.

[00:01:43]
BH: Well good luck with that. So let's start today's episode talking about ethics. It's always interesting to combine ethics and next generation technology. Do you think that technology has influenced our ethics and morality in a positive or negative way in the last 20 years? There's nothing like starting an episode off with a nice, simple question!

[00:02:03]
JB: Yeah. Well, I do think that that is a fabulous question, and I think it needs to be unpacked a little bit. But my overall impression is that I think technology, as with the general pace of life, has had, I think, potentially a bit of a negative influence on our ethical position. I'm a lawyer and I tend to focus on legal rights and justice. I think particularly if you take a technology like artificial intelligence, you can see perhaps where that is chipping away at fundamental human rights and freedoms, and I think particularly needs to be addressed on an ethical basis. I'll give you an example. One area that has given me some cause for concern is the Chinese national social scoring program.

I don't know whether you've heard of that, but essentially what happens in China now is that they have a national social scoring program so that if you throw litter onto a train platform, you're not allowed to travel on the train or you're not allowed to travel first class. So the Chinese are using technology to set up essentially a monitoring program to incentivize their citizens to behave in what would be required to be the correct way. I think that is ethically a bit of a black hole. We can see moves within the European Union to counter that kind of approach, because the new A.I. Act

that's going through the European institutions at the moment has prohibited that kind of national social scoring scheme.

So that's going to be outlawed. I guess in a sense, that's the kind of at the high watermark or at the most extreme elements of the bad uses that technology could be potentially used for, and specifically artificial intelligence. The other area that is obviously creating alarm is facial recognition, and the worry there is that we are kind of sleepwalking into a situation where it'll be the norm, that our faces are recognized automatically by machines and we'll be tagged, and that data will follow us wherever we go. To a degree, it's already happening in relation to our, for example, our website viewing behaviors, you know, we have the cookies that go around and track our behaviors and you have to take practical steps to stop that. Facial recognition, I think takes it to another level.

[00:04:45]
BH: Another example is also automatic number plate recognition, where you're driving along and you can be tracked, whether you go into either a car park or a congestion zone or you've done something wrong and then the police can then spot where you are. I mean, all of that is using some artificial intelligence at some point.

[00:05:04]
JB: Yeah, I mean, that's a form of recognition technology. So it's the same type of technology. It's just been trained on number plates rather than human faces. It does have an insidious effect on our rights and freedoms. You know, I think rightly the debate has been focused on the use by state authorities of facial recognition solutions. There was a recent case against the South Wales police, where they were setting up facial recognition vans outside Cardiff Stadium in an attempt to pick up crooks. They were just kind of sweeping the football spectators to see whether or not they could pick up felons, and they were challenged by various human rights organizations. And it transpired actually that insofar as English law was concerned, they weren't actually breaking the law, which tends to indicate to me that we need to kind of have a bit more – certainly in this country, a bit more law around that to protect individual rights.

[00:06:02]
BH: Can I just take that example bit further forward? So let's say a fan has been banned from a sport stadium for whatever reason - and it happens with pitch invasions or stuff like that, racist chanting and what have you. What's your opinion on setting up a camera outside to recognize people that have previously been banned may have bought a ticket under someone else's name or whatever and try to gain entry to a stadium? Is that against the law? Which bit might be against the law?

[00:06:32]
JB: Well, yeah. Currently, that would be against the law unless you've obtained that person's permission to use their facial data. I mean, that's pretty clear under the terms of the GDPR, which exists in the UK at the moment. That would be data that would be classed under the GDPR, as special category data. So relating to that biometric information, which requires direct consent, but also potentially a decision that be subject to automated decision making under Article 22 of the GDPR, which also requires direct consent. You can't just base a processing decision on your own legitimate interest in that situation. So yes, definitely unlawful in this country, quite apart from my personal feelings on the issue.

[00:07:18]
BH: Also as a lawyer who specializes in the technology industry, what's your view on terms and conditions on apps and websites? I'm not going to ask you so blatantly, do you actually read them, but to the average person, what's your view on having those terms and conditions?

[00:07:33] JB: Well, they're there really to protect the publishers of the apps, aren't they, they're there as liability limitation mechanisms and you are given the opportunity to read them. I mean, this is not a new argument, Bradley. This is more going back to the realms of contract interpretation and whether or not the terms that they introduce in their terms conditions are actually suitably incorporated in the contract. But you know, we are in a take it or leave it situation. If we don't accept those terms, then we can't use the app. So, that's the way modern contract law has evolved, and I'm not saying it's perfect, but if you have doubts, then unfortunately your choice is not to use the relevant app.

[00:08:18]
BH: So do you recommend that the average person does read those terms and conditions? I guess in your industry, you have to say yes.

[00:08:26]
JB: Well, it's not as if you're going to be able to influence it. Although I would say that consumer regulators are pretty focused on the inequality of bargaining strength between consumers and very large businesses, and they've stamped on some of the more excessive or egregious approaches taken in relation to these standard form contracts, such as, for example, allowing companies to unilaterally amend the terms without notification to the other side. I think Apple was censured recently on that basis that that is not a lawful way to proceed.

[00:09:03]
BH: Right, okay. Well, thank you for answering that. While we're on to personal opinions at the moment, what's your view on politicians using online paid advertising inside social networks? I'm thinking more from the AI perspective of, they get all the big data, and that AI of the social network in order to target viewers and social network users.

[00:09:20]
JB: Again, this is a really complex point, Bradley. But in principle, I'm not opposed to politicians advertising their wares, because politicians need to get elected. But where I do have a real issue is in relation to the manipulation of the truth. I think what we've learned from recent political experience is that the truth is a very precious commodity and where it's amplified on a social media network where millions of people can view it, it has the potential or the lack of truth has the potential to create substantial harm. I would certainly like to see - and it's a very, very difficult issue to regulate because what you don't want to do is to remove freedom of speech or opinion. But you do want to stop blatant lying, and I do think that there is a line that can be drawn in the sand between the two. We are seeing baby steps, I would say, in relation to this type of issue in the new act that's being discussed by the European Union at the moment in relation to, for example, things like deep fakes. So the European Union has a new – in that act there's new transparency provision, which says you can't use a deep fake, which could be a deep fake video or deep fake audio without actually declaring it as a deep fake. It will be unlawful to do that under the act. But I think more regulation is required.

[00:11:04]
BH: My last question around ethics and law is when we insure our cars, certainly in the UK, we have to declare where the car stays overnight, whether it's in the garage, on the street, in the drive, etc.. How do you feel from an ethics perspective about an insurance company checking, I don't know, using a drone, for example, that actually, the car is where you say that the car is going to be?

[00:11:30]
JB: Again, an interesting question, and I think there are questions of degree. So my view would be if the insurance company has declared what it's going to do to monitor your compliance with its policies. So if you've bought, for example, a telematics hub to sit under your car bonnet, which checks the way that you drive and that's a condition of your insurance policy, I'm absolutely comfortable with that, because that's completely open and disclosed. It becomes less justifiable where the insurance company starts flying drones around to see whether or not you've put your car in your garage. Again, the same considerations would apply to that insurance company, if, for example, the drone is picking up personal data, and it picks up your face. Then there is a breach potentially of the GDPR because they have their processing personal data, biometric data, and they haven't obtained the user's consent to do that. So they would be undertaking unlawful activity – and if they did that with me, that's the response they'd get. So they ought to be a bit worried about it.

[00:12:29]
BH: That's really interesting. Thank you so much, John. It's been such a pleasure having you on Tech Reimagined, to answer some of the big questions around ethics in such a hyper digitized world. To all of our listeners, I hope you enjoyed today's episode of Tech Reimagined and thank you for joining. Please show us some love. Hit that subscribe button if you like the episode, and don't forget to tell your friends and colleagues about the show. If you have any questions or you want to reach out for any feedback, then please drop us a line at endava.com – we use the @endava handle on pretty much all the social media platforms. We look forward to hearing from you soon. Until next time, thank you.