Intro:

We are honoured to have law and policy expert Elizabeth M. Renieris, an expert on data governance and the human rights implications of new and emerging technologies, as our 2023 Bijou guest lecturer. The author of **Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse**, her passion for data protection was ignited at university when a classmate hacked into internal residential house directories, scraped the student ID photos of female residents from their pages and pitted the undergraduate women against each other on a website called Facemash. Her classmate was Mark Zuckerberg, who went on to control one of the most powerful companies in the world.

Bio:

The founder and CEO of **HACKYLAWYER**, Elizabeth has advised the World Bank, the UK Parliament, the European Commission and the US Congress, and a variety of start-ups, global corporations and international and non-governmental organizations alike on law and policy questions related to AI/machine learning, blockchain and digital identity, as well as other new and advanced technologies. A senior research associate at the University of Oxford's Institute for Ethics in AI, Elizabeth has also held fellowships with Stanford University's Digital Civil Society Lab and the Carr Center for Human Rights Policy at Harvard Kennedy School. She serves as the guest editor to *MIT Sloan Management Review*'s Responsible AI project and was named to the 2022 list of "100 Brilliant Women in AI Ethics" by Women in AI Ethics.

Key points

- Laws focused on data have never and will never effectively protect people.

- We seem to think that if we could just control our data, we could protect against technology related harms and abuses. But privacy is much broader than just having control over data.
- The early organization of human life into databases, the trauma of two sequential world wars and in particular, the Nazis racially motivated atrocities, has helped cement international consensus around human rights and shape the values and formed modern day notions of privacy.
- Privacy is a concept rooted in constitutional and human rights law.
- We live in an increasingly cyber physical world... a world in which it is increasingly impossible to separate online and offline environments.
- The human rights framework offers us the only truly human-centric technology neutral approach, and it is our best chance of moving beyond data.

Introduction from Bailiwick Data Protection Commissioner Emma Martins:

"Welcome to the 2023 Bijou Lecture.

It was in 2021 that we launched Project Bijou and our aim was simply to encourage a sharing of stories and experiences around data and how it impacts us and our lives – in turn to encourage better understanding of how we can all play a part, however big or small a part that is, in ensuring better outcomes.

Conversations around those impacts have become even more pressing I think lately and we are certainly seeing a lot more public discourse. This discourse is really critical.

There is a wealth of brilliant people working in this area, thank goodness, and it is so wonderful to be able to highlight the work they do, and celebrate the work they do. We couldn't quite believe it last year when Dr Susie Alegre agreed to present our inaugural Bijou Lecture but I think it points to the shared issues and the shared concerns and the shared desire to work together for a less dystopic future.

We are nothing if not ambitious and I am thrilled that we have again got a contributor of such high quality for this year's talk.

Those that know me will know that I am a bit of a book worm. There is so much information out there but I find books allow the author and of course the reader to really get beyond some of the noise and the sound bites – it gives the chance for some really thoughtful, reflective considerations of the issues.

And I came across a book recently, a newly published book, called '*Beyond Data: Reclaiming Human Rights at the Dawn of the Metaverse*'.

The author, Elizabeth Renieris is one of the leading experts in this field and I ordered her book as soon as it was published.

I read a lot and I try to learn from what I read. But occasionally you come across something that literally stops you in your tracks and that happened to me with this book.

Chapter 1 starts with -

'For more than 50 years we have been so busy protecting data that we have largely forgotten to protect people.'

As someone who has spent their entire professional life working in data protection, reading that really hit me.

We need of course to understand the legal framework that sits around data, but it is all too easy to allow that to take our focus away from what really matters. What happens to data is what happens to us. This is not about spreadsheets and databases, it's about us.

Renieris brings such a beautiful clarity to this point and I think it goes to the very heart of our lives today and tomorrow.

It is a huge privilege to welcome her to the Bijou Lecture for 2023."

[3m 30s] The Bijou Lecture 2023:

"Hello, I'm Elizabeth Renieris and it's an honour to be able to deliver this year's Bijou lecture. Before I properly introduce myself, I want to thank Commissioner Martins and the Office of the Data Protection Authority for inviting me to share some thoughts with you as we approach the 5-year anniversary of the GDPR's application and as we enter a new age of AI.

By way of introduction, I'm a data protection and privacy lawyer with cross-border experience, having practiced in the US, the UK, and the Middle East. Through my consultancy 'Hacky Lawyer', I work with clients around the world on confronting the thorniest law and policy challenges posed by emerging technologies.

I'm also a part-time academic, currently a senior research associate at Oxford's Institute for Ethics and AI. I'm a senior fellow at the Center for International Governance Innovation, where my work focuses on the ethical and human rights implications of AI and machine learning, digital identity, and extended reality technologies.

Perhaps most relevant for today's purposes, I'm also the author of a new book titled 'Beyond Data, Reclaiming Human Rights at the Dawn of the Metaverse' from MIT Press, which will be the starting point for my discussion today. In my book, I argue that laws focused on data have never and will never effectively protect people. Instead, I advocate for an approach to technology governance based on a broader array of human rights and freedoms well beyond what data protection, particularly in its current iteration can offer.

Here are five key points I'd like to make:

1. **We are obsessed with control over data.**

When we think about privacy today, many of us will reflect on our perceived lack of it at the hands of digital technologies, specifically the ways we are tracked and surveilled online through the digital breadcrumbs we leave behind as personal data.

Companies like Facebook, Google, and Amazon, and concepts like surveillance, capitalism or targeted advertising may come to mind. We may recount the seemingly endless stream of high-profile data

breaches exposing consumer data, health data, or financial data. Or scandals like Cambridge Analytica. After all, we are said to live in a data-driven world powered by big data in which data is the new oil, and data is power.

For some, this means that privacy is dead. For others, it means we must own or control our data to reclaim our privacy.

Our laws are equally focused on controlling data, how it is collected, shared, stored, and otherwise processed. Laws that prescribe largely unread notices about how our data is used and often seek meaningless, perfunctory consent to process it. Laws that require companies to keep our data secure and confidential from third parties while imposing few limits on how they handle it or what they do with it themselves.

Landmark regulations like Europe's GDPR and copycat laws the world over set out data, subject rights. The theoretical rights of individuals to access correct, erase and transfer their personal data from parties who process it can prove difficult to exercise and practice while other jurisdictions, including the US contemplate similar comprehensive privacy legislation.

We seem to think that if we could just control our data, we could protect against technology related harms and abuses. But privacy is much broader than near control over data, which brings me to my second point.

2. Privacy is a much broader and older concept rooted in constitutional and human rights law.

One that I trace in my book to the UN General Assemblies adoption of the Universal Declaration of Human Rights in 1948, declaring the right to privacy to be a fundamental human right. In the World Wars, population censuses, national registration systems and conscription systems for military service became commonplace in much of the western world. This early organization of human life into databases, the trauma of two sequential world wars and in particular, the Nazis racially motivated atrocities helps cement international consensus around human rights and shape the values and formed modern day notions of privacy. As with national constitutions preceding it, international human rights law conceived of privacy as the limiting the boundaries of one's family home, and correspondence in relation to interferences by the state.

In other words, privacy was deemed necessary to maintain zones or spheres around the inner or private life of the individual, protect the individual's physical person, home and family life; create boundaries that are foundational to the exercise and enjoyment of other fundamental rights and freedoms, protect individuals from discrimination and harassment and ultimately defend the individual liberty and autonomy necessary for a fully functioning democracy.

Advances in computing and network technologies in the second half of the 20th century would challenge these traditional notions of privacy, which before electronic or digital communications still typically required a physical interference or intrusion.

The idea of data protection introduced in response - though derived from the human right to privacy - was much narrower and not intended to replace or supplant privacy altogether.

3. **Modern data protection laws are based on an outdated view of the world.**

The earliest data protection laws in relation to digital databases emerged in the 1970s, in the early days of personal computers, a time when data about people was collected by known entities, typically governments, and stored in clearly delineated databases, both analog and digital for clearly defined purposes.

A world in which it was possible to map personal data flows at scale, and to separate the online and offline environments. These laws hinged on the idea that with sufficient notice and transparency individuals could meaningfully control the ways in which their data is accessed, used, shared, and processed for specific purposes.

This original paradigm is still the prevailing approach, codified in modern data protection, privacy laws, including the gold standard GDPR. But that world doesn't exist anymore. Instead, we live in an increasingly cyber physical world. In which data constitutes the built environment, flowing through the vast web of internet of things, devices, sensors, AI and machine learning systems, including deep learning and neural networks, and increasingly virtual, augmented, mixed and extended reality systems at an unprecedented scale and speed, a world in which it is increasingly impossible to separate online and offline environments.

Data supply chains have become so complex and convoluted that few companies have a handle on the data they collect, store or process. Or can effectively map their own data flows. The idea that any single individual could exert any kind of meaningful control over their data in this environment is pure fantasy, and yet our laws continue to propagate this view.

4. **Privacy has become the handmaiden of tech related harms and abuses.**

This gap between the world we live in today and the one presupposed by data protection laws leaves us vulnerable to a loss of privacy in its original sense. As well as deception, manipulation, discrimination, harassment, and more.

It also allows companies to refashion the rights of privacy in their own image as a technocratic exercise in the confidentiality and security of data. Until very recently, private actors have relied on largely ignored terms of service and privacy policies, as well as their asymmetrical bargaining power to exploit user data.

As these practices are challenged, they're increasingly embracing privacy preserving or privacy enhancing technologies. A wide array of technical means, tools and approaches to help mitigate data privacy and security risks, such as the risk of revealing sensitive attributes present in a data set.

Examples include homomorphic encryption, differential privacy, on-device machine learning, and synthetic data generation. But when privacy is reduced to the mere privacy, confidentiality, and security of data, there are virtually no limits to what companies can do or the activities they can undertake as long as they safeguard and secure any data they process along the way.

In practice this distorted mathematical or technocratic notion of privacy vis-a-vis data protection has incentivized dominant technology firms to bring more into their own ecosystems, deepened their

vertical integration, and use privacy as a shield against competition, making us more vulnerable to control, manipulation and exploitation by entities wielding unprecedented power.

Data-centric legal frameworks are often too easy to circumvent as demonstrated by the use of synthetic data for purposes that would otherwise be impermissible with the use of personal data. The more that our laws continue to concentrate on requiring companies to protect the privacy and security of data, the more we forget to protect the privacy and security of people. As companies continue to find ways to move beyond data, so too must our approach to governing digital tools and technologies.

5. **We need an approach rooted in a broader set of human rights.**

As data comes to permeate everything, we are at risk of asking too much and too little of data protection.

On the one hand, data protection has become a kind of panacea for harms brought by technology acting as a kind of broad sweeping, albeit ineffective tool for technology governance. Far more than it was ever designed to do. In fact, as everything quickly becomes fused with data, we increasingly equate data protection or data privacy for my American friends, with privacy more generally. This asks far too much of data protection and at the same time, we are demanding too little. Our data-centric approach to technology governance has enabled dominant corporations to effectively reduce the once potent notion of privacy to a technical exercise in ensuring the security and confidentiality of data.

Core data protection principles related to data such as data minimization and integrity have crowded out other core principles focused on lawfulness fairness and transparency towards people, and the ultimate accountability of entities. In this way, privacy and the derivative right to data protection have grown, divorced from the human rights framework from which they derive and in turn lost much of their efficacy and power.

In fact, there are more than 30 fundamental human rights and freedoms that apply to our human experience, whether at the hands of digital technologies or otherwise, as the real and virtual worlds continue to blur, eroding neat binaries like online and offline, and as everything becomes infused with data, there will be no such thing as digital or data rights only rights.

So long as technology governance is predicated on data or specific technologies, it will be wielded and shaped by those who control both, namely, powerful commercial interests Only when technology governance is predicated on human rights, which attached by virtue of our humanity, will it be framed by human interests.

In fact, the human rights framework offers us the only truly human-centric technology neutral approach, and it is our best chance of moving beyond data. As with my book, I hope this conversation can help us shift the focus of technology governance, away from data and back to what really matters, protecting people.

Even as data protection practitioners and professionals, we can center people and their protection before concerns about data. Particularly as we enter into a new age of AI, we can return to core principles, demand more than the mere confidentiality and security of data. And acknowledge the limits

of data protection where they exist. Recognizing that **just because something implicates data doesn't mean data protection is our only tool to govern it.**

Thank you and I look forward to your questions."

[15m 20s] Question and Answer:

Katherine Levy (KL): Elizabeth, thank you again for joining me. I wondered if we could just start by talking a little bit about the inspiration behind your work, '*Beyond Data, Reclaiming Human Rights at the Dawn of the Metaverse*'.

Elizabeth Renieris (ER): So I had several motivations for writing this book. A combination of personal and professional ones. On the personal front, I talk in the preface of my book about an experience that I had in university where a classmate effectively hacked into residential house directories and stole the university identity photos of female classmates and pit them against each other in this contest of attractiveness on a website called FaceMash.com. That's the origin of the Facebook story and that classmate was Mark Zuckerberg. It planted the seed in me where I felt a real violation of dignity and privacy and other things. And I think in part, inspired my journey to become a data protection lawyer.

On the professional front, as I went on to practice on three different continents, I grew increasingly disillusioned and frustrated with data protection as a means to address the types of harms that I felt at the hands of my classmate. And so there was this interesting tension on the type of justice I was seeking and the limitations of what I was coming up against in my practice. Then in academia, because I also, have spent quite a bit of time in academia, I felt there was a singular focus on data when it came to technology governance. Often the conversation was very divorced from one about people or one about human rights more expansively. So, it was really a combination of all those things that led me to, to this book. And that's really one of the things that really resonates with us is when you talk about that we need to go beyond data in order to protect people.

KL - Why do you think there is such a disconnect between data protection and protecting people?

ER - Yeah, it's a great question. I mean, personally I think it's bad branding, so I personally think the term data protection hasn't done us any favors. In the United States, we'll sometimes call that data privacy and of course it suggests that that's about protecting the privacy of data. In my book I walked through how the right to data protection is rooted in the human rights of privacy and was intended to protect people. Really, it was all about people at the start but it's certainly a misleading term that I think centers data. I think there's also been an intentional campaign on the part of private actors, the private sector, to really focus on data because it's easier for them to give the appearance of things being in control, right? It's easier to secure data, to protect the confidentiality of data while still doing anything they want with that data. And so rather than focusing, for example, on actual human rights or people, you know, they're able to sort of use computational mathematical techniques and say the job is done. The other important thing to note here is, I think that the chasm is because we are not our data. I think it's become so popular to equate ourselves with our data, our data selves but data is always going to be an imperfect representation for proxy for our lives. We're more than what can be reduced to data. And as I explained in my book, there's a process of, you know, turning these, these aspects of our lives into data points through a process of datafication but I outline the natural limits to that process. So as we're on

the frontier of things like neuro technologies, you know, there are limitations to what actually can be datafied in that sense and similarly with emotion recognition or other sort of high risk tech technology. I think it's this combination of getting distracted by, as increasingly everything becomes data, we sort of lose sight of what the, the right to data protection was, was meant to protect in the first place.

KL – I really love what you say about bad branding because in my life as a comms person working in data protection, it's just the worst term. But I haven't been able to come up with something unfortunately to replace that. But you go on to talk about shifting the conversation away from data centric framing towards a more expansive view, which is just what you've been talking about, rooted in human rights. Do you get a sense that we are starting to see that shift now?

ER - Yes and no. I think it's, it's a little too soon to tell. As I talk about in my book, you know, we have 30 plus fundamental human rights and freedoms. Typically, when we're talking about digital tools and technologies, digital rights, things like that, two rights are very prominent in that conversation: free expression and privacy. And I think, again, this comes from a focus on data where if things are data or things are information, then there's a natural impulse to view those two rights as the most important, but we're seeing, especially, you know, with AI proliferating, we're seeing the conversation certainly shift to rights around labor, around things that are more economic, social, and cultural in nature, although typically not framed in that way but more collective rights, concerns beyond just individual civil and political rights which, which are the rights that include privacy and free expression. I also think that technologies like AI are exposing the limits of data protection. So we're really seeing how things like data minimization or purpose limitation, what do they really mean with these systems, right? When they're built, you know, by design, they're built by scraping the entirety of the web. All this data that was obtained for other purposes, I mean, the starting point is inherently intention with core data protection principles. So we are at this really difficult point I think, in data protection where, you know, are we acknowledging the limits of these principles? Are we abandoning them entirely? Does that undermine what data protection is trying to do? Because I don't see any appetite to shut these things down. You know, of course we had, the DPA in Italy temporarily halting things like Chat GPT, but I don't see in the long term any desire to really halt technological progress or stop these technologies entirely. We are going to have to grapple with, “what does data protection look like in a world that's inherently sort of intention with those core principles. And then I guess the other thing I would say is there may be a shift occurring, but I'm also concerned that we might be repeating some of the same mistakes we have with data protection in the AI context. So technology specific laws, very focused on data, the algorithm, the model, rather than starting from the perspective of people and human rights. And so I question how much those laws will withstand the test of time.

KL – Absolutely. One of the challenges of a globalized economy is this idea of borderless data-driven, digital economy. Can the human rights framework that you discuss succeed without borders?

ER - Yeah. And this is one of the biggest challenges we have to all technological advancement. Increasingly, these technologies become sort of borderless in, in some respects, in other ways. We do see this increasing fragmentation, especially geopolitically, you know, between the US, the UK, China, EU, we see efforts around data localization, data sovereignty. There is a tension between the sort of technological aspects, the nature of the technology being more decentralized and sort of borderless, but governance mechanisms are actually leaning more towards this kind of fragmentation and localization. I

think if anything has a hope of succeeding across borders, it's governance predicated on the human rights framework because it's the closest thing we have to some kind of international consensus. It's not perfect. I talk about the limitations in my book. I talk about the fact that human rights are particularly precarious right now because of the geopolitical environment that we're in. Our institutions are very fragile. But at the same time, you know, I can't think of anything else that would be a better starting point for global governance. So I personally believe that it's our best hope, and I think that now is really the time to reinvigorate and lean into our existing human rights frameworks.

KL -So you wrote the book, I think you started, was it in 2020, sort of at the beginning of the pandemic? Right. And it feels very prescient. When you look at what's happening now with artificial intelligence and it's triggered an unprecedented level of public engagement. Do you think that we are entering a new sort of chapter in public consciousness?

ER - Yeah. Yeah. Well, I think so. Academic publishing is very slow and of course, I completed the manuscript long before tools like Chat GPT were available to people on the market. So I couldn't directly address those types of generative technologies, for example in my book, However, I'm feeling extremely vindicated by what's happening now in the sense that it completely to me reaffirms my thesis, which is that if we just focus on the technocratic protection of the security and confidentiality of data, we have no hope of governing AI tools built on the way that they are on data. I think that a more expansive human rights framework is our best hope here. And I do think, again, we're seeing some of the shift in the conversation, although it's not necessarily being framed in terms of human rights, unfortunately. I'm seeing a lot of calls for, you know, new governance frameworks, new laws, new agencies, new oversight bodies, sort of throwing out everything that we've built over the last, you know, 50 to 75 years. That could be very powerful so I'm worried about this kind of policy obsolescence, where we're continually reinventing the wheel rather than, you know, re-skilling existing authorities, upskilling. Again, the way that these technologies are built, right, they're not built from scratch. They take what exists and they continually refine and reiterate. I think that's really the way we should approach this from a governance standpoint, which is, you know, to work with what we have to fine tune it as we go. I think this is where data protection could be a lot more powerful. At the same time, there's always this competition for resources. Now we have new regulators coming online and we have to think about the sustainability of that.

KL - What's interesting about data protection is that sort of horizontal type of regulation as well, because it impacts on every single sector. But one of the things we're trying to do, because we're well aware of the sort of limitations that we have as a small regulator and a small jurisdiction so with our project Bijou what we want to do is create this cultural shift around how people's data is treated in any context. And do you think that a cultural shift can do more than legislation to create checks and balances for advanced technologies?

ER - Yeah, absolutely. I mean, I think that will probably come before lots of regulations and I think the zeitgeist has been the biggest driver, I think since, you know, Cambridge Analytica, The Great Hack, subsequent sort of films and things in popular culture, I think really have shifted the conversation and, uh, certainly increased the demand for, you know, privacy and data protection. I think that's probably driven market outcomes more than the laws and regulations at times. That's great because that means it can sort of mutually reinforce what data protection authorities are trying to do.

KL - You talk about reclaiming our power by remembering a time before data and imagining a future beyond it, which is quite a powerful phrase. What does that look like to you and where would we be in five years' time if you could be in charge?

ER - It's such a difficult thing to imagine, I think particularly for people who have come of age, you know, in the era of the internet, in a world of data, you know, my peers and, and peer generations. I think in my mind it goes back to this, what was the genesis of all this? You know, what was the context for all this? The context was, again, heightened geopolitical tensions, you know, two great world wars. A sense of exasperation but also hopefulness around an international consensus and fundamental things that we felt were core to kind of international peace and stability. One of them being the notion of a private life. And so I think if we could, if we could try and project into the future of what does that mean, putting aside data, what would a private life look like? What are the things that we seek to protect in that way. Is it freedom of thought? You know, is it freedom of association? Is it these other rights and freedoms? We mentioned Susie Alegre was a speaker in the series last year. I mean, I think those types of rights and freedoms are overlooked in this conversation, but they're critical to the, the interior life and so, you know, the reason I have this subtitle in my book about the Metaverse, and that's very tongue in cheek, is because, you know, if we're in a space where everything is, you know, connected, if everything's online and, and we're online all the time, and there's a pervasive sort of data stream flowing across people and environments, you know, some people will say privacy is dead. I say privacy is, you know, completely revitalized in the sense of. Again, what is the interior self in that context? So, it's hard to say. I mean, we see how quickly things are moving. What will things look like in five years? I have no idea. I don't want to make those predictions, but I think the best way that I can think about it is, again, putting data aside, what do, as an individual, what do I think I'm protecting as my interior life and, and my private self?

KL - So very much the one thing that you'd like to perhaps people take away from your book is to look at this issue within a much wider context?

ER - A much wider context and thinking about it, as separate and apart from the technology, working backwards to get to the technology. I think that's our mistake. We start from the technology and then that already narrows sort of the constraints and limits our imaginations rather than starting from the perspective of the human experience and working backwards to now, how do we have to design and build our technology?

KL - Obviously it's such a big discussion and it has so many implications for humanity. Just to end on a slightly positive note, I mean, what inspires you? Who inspires you in this, in this space?

ER - Yeah, I've been thinking about this because it's very easy, I think to lose hope in this space and to feel overwhelmed. A lot has inspired me recently. So I think first and foremost the women, particularly in AI, machine learning who have been risking their lives and their reputations and their careers to speak out, warn us about these things long before it was in fashion to do so. I think it's really important to note that particularly with the more recent whistleblowers that have come online. I think the 150 plus workers in Nairobi who voted to unionize, who are core to the whole AI system providing services for companies like Facebook and TikTok. I think those types of collective labor movements are really interesting and inspiring right now. I think the data protection authorities, right? I think people who are showing up to do the work under very resource limited constraints, but being willing to adapt and

change, to constantly evolving technologies. And then young people who are resisting technology in different ways. And again, trying to sort of re-establish limits for themselves, I think is very inspiring.

KL - It's been an absolute pleasure to speak with you. Just before we go, is there anything that I haven't mentioned that you wouldn't mind, getting across?

ER - I think we've covered a lot of ground. I think it's just to stay hopeful. We're only human, right? We're not machines, so we can just do the best that we can. Thank you so much for having me. It's been a pleasure speaking with you. I'm really excited about this lecture series as well, so I hope lots of people tune in.