[MUSIC PLAYING]

RISA GOLUBOFF: Hello and welcome to "Common Law," a podcast from the University of Virginia School of Law. I'm Risa Goluboff, dean of the Law School.

LESLIE KENDRICK: And I'm Leslie Kendrick, the vice dean.

[MUSIC PLAYING]

In today's episode, we're bringing together a lot of threads that have come up this season. Big data, robotics, social media. And we're going to talk about how they all relate to statecraft.

RISA GOLUBOFF: Exactly, so imagine if the military and intelligence agencies could master all of those technologies at once and gather all of that data and get them to work in tandem. What would they do with that power? What should they do with that power? And assuming that they already have that power, what are they doing with it?

LESLIE KENDRICK: What are they doing with it? Our next guest has been asking just those kinds of questions. Ashley Deeks is a UVA Law professor and senior fellow at the Center for National Security Law. She's also served as a legal expert in the State Department advising diplomats on international law and armed conflict. And recently, she's been publishing research on how algorithms that try to predict human behavior, which are already being used in law enforcement, could affect decisions on the battlefield.

Ashley, thanks so much for being here.

ASHLEY DEEKS: Great to be here.

LESLIE KENDRICK: I was just wondering if you could start us out with some concrete examples of how developing technologies are being used in the national security field, how they might be being used, or could be used in the future.

ASHLEY DEEKS: Sure. In the military space, for example, you can envision militaries wanting to turn to predictive algorithms to help them figure out how most effectively to conduct their military operations. Where to send forces. Where to deploy. Who to detain. In the intelligence space where intelligence agencies have a vast ability to collect information, they might be using it to help predict how enemy states are going to behave. To help try to identify where conflicts look like they're about to spring up in maybe a more neutral sense.

We're starting to see AI being used to create fake news, fake videos-- what are sometimes called deep fakes. So AI--

LESLIE KENDRICK: Deep fakes?

ASHLEY DEEKS: Deep fakes. If you can pit two AI systems against each other to try to develop very persuasive fake videos, fake voices of people-- so I think they did that to President Obama. They had him giving a speech that he never actually gave. You can imagine the direct and serious national security implications of releasing a video that shows a foreign leader declaring war on another state, for example.

And I'd say related to that, those are mostly national security examples looking outward. But I think there are other ways in which high tech tools are going to be relevant for national security, including facial recognition software. Perhaps on our border. Perhaps to detect terrorists inside our country. Those would just be some examples of areas in which we're starting to see high technology about to play or are already playing a seminal role in protecting our national security.

RISA GOLUBOFF: So before we delve into those examples and explore them further, and some others as well, can you give us a sense of how the law fits into all of that? I mean, it's either domestic legal regimes and international legal regimes, so what is the law doing or what do we hope the law is going to do? How does it interact?

ASHLEY DEEKS: So right now, I would say that the law is lagging behind in both the international space and in the domestic space. And I think you often see the technology gets out in front of law. That's not to say there are no legal rules that exist to regulate how states use these tools, but there are very few legal rules that regulate the specific tools themselves. So just to give you an example, international law has a big body of law called the Law of Armed Conflict, also known as International Humanitarian Law, and those rules regulate how states fight conflicts.

So just because a state might be using particular advanced technologies in its fight against a foreign government or non-state actor, those underlying bodies of law, IHL would still regulate it. But it might become more complicated to apply rules that were written in a pre-technological era for the types of high tech tools we're starting to see. So there's some baseline rules that exist, but their application in the AI type space is increasingly complicated.

LESLIE KENDRICK: You've written a paper predicting enemies that talks about the way that predictive algorithms might get used in the national security space, and you're talk about it by analogy to what's already happening in the criminal justice sphere. So could you tell us just a little bit about what's actually happening on the criminal justice side to help us understand what we might happen in national security.

ASHLEY DEEKS: Sure. What we are now seeing in the criminal justice space at the federal level, state level, and local level are criminal justice actors, including judges and parole boards, using predictive algorithms to help make decisions about how dangerous people are. It comes up in the bail context, for example, where you're trying to decide whether you should continue to retain somebody or allow them to pay money and be released. The concern, of course, is that they might do something. They might commit another offense if they are, in fact, a dangerous person.

Likewise, in sentencing, judges are often confronted with a question of how long a defendant should be sent to jail. It's possible that the person doesn't actually seem all that dangerous, doesn't seem like the person will reoffend, and the judge might have an option not to sentence to any kind of jail time. Or the person seems extremely dangerous and so the judge is trying to figure out perhaps a long sentence is appropriate.

So they're sorting through a question that they have imperfect information about. They have lots of information about how other actors have operated in the past. People who have committed similar offenses from similar backgrounds and so on. But they don't know about the particular person they're confronting. And so, increasingly, these systems-- the criminal justice systems are turning to predictive algorithms to help these actors better assess what the person in front of them is likely to do.

RISA GOLUBOFF: Just as an interjection, it sounds-- we think of our justice system-- I mean, I don't know that it actually works this way, but we like to think of our criminal justice system as an individualized process of justice. And this definitely makes it sound a lot less individualized. Your own future, your own dangerousness, your own punishment is going to depend upon data about other people. Not data about you. Right?

ASHLEY DEEKS: That's right. And that's been one of the criticisms. I should say that these systems are not without a broad range of criticisms. One of them has to do with the biases built into the data. So let's say that somebody with five arrests is likely to be a recidivist, but if the police in that area tend to over-arrest African-Americans, then the algorithm will produce a bias. So that's one critique that they faced.

And, Risa, the point you made is another critique for exactly what you said. They are basing a prediction about person X on the past behaviors a person Y, Z, P, Q, and R.

RISA GOLUBOFF: Right.

ASHLEY DEEKS: On the other hand, if it turned out that you could develop an algorithm that was more accurate and more consistent than humans, then that is something worth thinking about.

RISA GOLUBOFF: Right.

ASHLEY DEEKS: And, in fact, we all have our own algorithms inside us that we can articulate less well or more well, but that judge is not making a decision about somebody's dangerousness in a total vacuum.

RISA GOLUBOFF: Right. You're always using sound evidence that kind of-- right.

ASHLEY DEEKS: I guess I should say there's another area in which criminal justice is using predictive algorithms, and that's in what's often called predictive policing. So here you have police departments with limited resources trying to figure out where they should best deploy officers on a given shift. And, of course, the gold standard here is to stop crime before it happens.

So these policing algorithms indicate at a very granular level where it is most likely that a particular property crime would occur between 2:00 in the morning and 4:00 in the morning on a Wednesday. And these algorithms are developed-- you asked about sources of data. The algorithms here are being developed, including day of the week, geography of the neighborhood, what the neighborhood looks like-- is it a lot of boarded up houses? Are there churches and schools? Phases of the moon--

LESLIE KENDRICK: Really?

ASHLEY DEEKS: --are relevant to this. Full moon, harder to hide your offense. No moon, it's quite dark out.

Home football games, people get presumably rowdier, drunker. So all of those kinds of data factor into the policing algorithms.

LESLIE KENDRICK: So this sounds like it's getting very close to the national security analogy and how that would come up. So walk us through that a little bit.

ASHLEY DEEKS: Sure. So what got me thinking about the potential connection was that militaries basically have to answer similar questions when they're fighting armed conflicts. In some conflicts, militaries detain tens of thousands of people. And the laws of armed conflict require them to revisit, periodically, whether they need to continue to keep somebody in detention. So the militaries need to predict how dangerous somebody is.

And likewise, if you're a military commander and you have troops in Fallujah, you want to send those troops to where you think they can best do their job, whether it's preventing an attack or protecting civilians. So they're asking themselves questions similar to the ones that our police are asking us in the criminal justice law enforcement setting. And, of course, the parallels are not perfect. There are important differences. But it's struck me that it was worth exploring ways in which the things we've done and the lessons that we've learned in the criminal justice setting might be something that our militaries are starting to pay attention to with their vast realms of data, including data about detainees and past conflicts.

LESLIE KENDRICK: And is this something that the world's militaries are doing now or that you think they're going to do, or do we even know the answer to that question?

ASHLEY DEEKS: We don't have a perfect answer to that question. I asked a number of colleagues in the military, and also academics who had previously spent time in the military, to talk through some of these questions with me. And most of them seemed to think it was an interesting question worth exploring. So I took that to mean there are not militaries that are affirmatively creating detention algorithms right now. But that it is not crazy to think that they might in the future.

We do know that the militaries are starting to use machine learning and AI tools to help them process all of these thousands and thousands of hours of video that they're collecting from drones. It's very, very tiresome and it takes a ton of man and woman power to examine these recordings to detect items of interest. Maybe it's somebody on the side of a street who looks like he's planting an IED, or a Hilux truck with some guns on the back moving to a particular location.

So I think it is quite likely that our military-- the US military, I would say-- the Chinese military, the Russian military, with their capacity to collect these big buckets of data and their ability to develop sophisticated machine learning tools, are certainly heading this way if they have not arrived there already.

RISA GOLUBOFF: And where does the US fit within this larger international scheme of, where are we on collecting data? Where are we on being able to deploy these kinds of predictive technologies?

ASHLEY DEEKS: Mhm. So I think we and the Chinese are right out in front. The Chinese have put forward a number of national plans and strategies indicating that they see AI as imperative. That they see sophisticated AI as the future of warfare. And they've devoted a lot of time and money and attention to it. They also have a lot of companies that are, if not controlled by the Chinese government, closely integrated with the Chinese government so that they can dictate the direction those companies go.

In the US, we have a lot of capacity-- very sophisticated computer scientists and engineers. But the US has a trickier path to navigate with the private sector than, I think, China does. And there's another important difference as well. And that goes to the ability to collect information about your own citizens. So--

RISA GOLUBOFF: China has a greater ability than the United States [LAUGHS]. We hope [LAUGHS].

ASHLEY DEEKS: China has a greater ability and fewer legal restrictions. So the civil liberties, protections that we have in this country, and our interest in having our government overseen and monitored as it collects information on us, is not as prevalent in China. So they are doing amazing things, for example, with facial recognition software because they have a billion people and surveillance cameras all over major cities. So they're collecting, you can imagine, many, many, many, many hours of footage and examples of faces that they can train their systems on.

RISA GOLUBOFF: So you get the sense from civil libertarians here that people think we already live in a totally surveillance society. But you're saying we don't really. We're not really there--

ASHLEY DEEKS: They should take a trip to Beijing--

RISA GOLUBOFF: Yeah.

ASHLEY DEEKS: --and compare. Yes. And on that point at, the US government is regulated by statute quite carefully on its intelligence collection-- generally, but particularly with regard to US citizens. But people are often much more comfortable giving their information to private companies.

Why? Well, at a macro level, it's because companies don't have the ability to throw us in jail. But on balance, we are giving companies like Twitter and Facebook and Amazon vast, vast amounts of data that will allow them basically to predict everything about us in coming years. So I think that's part of the struggle and discussion right now about whether Congress should be stepping in more as we are turning our attention to the vast amount of privacy we've effectively surrendered to these private companies.

RISA GOLUBOFF: Well, especially if you go full circle and you say, private companies then get to decide whether and how much they interact with and share with the government. So once you've given to the private companies, then it's not the individual's choice so much anymore whether that information is going to go to the next step to the government and be used for other purposes.

ASHLEY DEEKS: Right.

LESLIE KENDRICK: So we want to get to these questions about private companies. But I wonder if you could tell us a little bit more about the predictive algorithms in national security. So in thinking about these predictive algorithms, it seems like one issue in the criminal justice system, and another criticism, is that it's just not very transparent sometimes how these are being used. National security is sort of by definition, something that we as regular citizens don't have a lot of insight into. Is there a role for greater transparency in how countries, or at least how the US in particular, would use predictive algorithms in national security?

ASHLEY DEEKS: So in thinking about the concerns that are almost certainly going to arise among groups in the US who follow very carefully what the US military and intelligence agencies do, they will be concerned about algorithms for some of the same reasons we've seen concerns in the criminal justice setting. They'll worry about whether it builds in cultural biases. That is coupled with what is sometimes, I think, just sort of a yuck factor of allowing machines to make decisions that have life or death consequences, or at least liberty consequences, for anybody, including foreign nationals.

So one of the points I make in the paper is that we should learn our lessons from the post-9/11 deep secrecy that we saw. For obvious reasons, our intelligence and military officials conducted a lot of operations that were not made public, and many of them came under significant criticism when they were finally revealed. I'm thinking about things like the rendition program, keeping secret sites at various locations around the world. And we lost a lot of credibility. We were unable, in some cases, to work well with allies because they felt as though they couldn't engage with us on certain military operations because it was inconsistent with their legal obligations.

So I think this is an opportunity for the US to try to get ahead of the game here. We know that these kinds of algorithms are coming down the pike. And I think the government could do a lot of good, could bring along allies who are thinking about these issues, who are maybe concerned about these issues, to basically explain why it is that algorithms can be imperative to protecting our security, what some of the challenges will be and working through-- I think they should be forthright about the challenges. How they're going to try to deal with some of the challenges that will arise.

So for example, there's a concern about automation bias, that you will just automatically believe the recommendation of an algorithm and not use your own judgment if that seems off. How will they--

RISA GOLUBOFF: What systems do you put in place to make sure-- right.

ASHLEY DEEKS: What kind of training-- exactly. I think without that, you end up with something I call a double black box you have the black box of algorithms, some of which are actually hard to unpack-- to know why they're producing the recommendations that they are-- inside the black box, Leslie, that you referred to, of our national security state, which is the standard mode for US national security.

RISA GOLUBOFF: Double black box sounds very scary.

ASHLEY DEEKS: Double black box.

[LAUGHTER]

LESLIE KENDRICK: Yeah. And along with the military articulating some of these standards and trying to be a leader in that, do you envision a kind of oversight by some other types of entities? Or how will this be policed?

ASHLEY DEEKS: So it will be policed first and foremost by Congress. Congress and the intelligence committees really serve as our proxy for making sure that we're comfortable with what the executive is doing. The courts have not generally been aggressive overseers in the national security space. They use a variety of doctrines to help avoid the decision on the merits. One of them is the Political Question Doctrine, which is a determination that a particular question has effectively been allocated to the two political branches to sort out. So it's very difficult to get questions about, should the military be using a particular algorithm to continue to detain somebody in Yemen, for example. To get that before a court, it's very tricky.

And, of course, there's also the public. There are leaks. That's another part of our secrecy ecosystem that brings things to light. People transmit information to reporters, especially if they're concerned about the programs. The reporters write articles and that triggers both public discussion and often congressional oversight.

RISA GOLUBOFF: And then, to what extent do you see a role, not just domestically, for how regulation is going to work, but what does the international framework look like in thinking about predictive algorithms and the future in national security, more generally?

ASHLEY DEEKS: That's the question we all want to know the answers to. I think realistically we are many, many years away from any kind of agreement on the use of AI generally. I will say there's been a particular heated discussion in the international space on lethal autonomous weapons systems, which are pejoratively known as killer robots. So this is--

RISA GOLUBOFF: Pejorative? What's pejorative there? I don't see a pejorative [LAUGHS].

ASHLEY DEEKS: Selective. Pejorative.

LESLIE KENDRICK: So we're going to talk about killer robots now. All right, tell us about the killer robots.

RISA GOLUBOFF: [LAUGHS]

LESLIE KENDRICK: Ashley's work just is what keeps me up at night. So you've told me about the drones. Tell me--

ASHLEY DEEKS: No--

LESLIE KENDRICK: --about the killer robots.

ASHLEY DEEKS: --killer robots should let you rest easy.

LESLIE KENDRICK: Oh, sh-- OK.

ASHLEY DEEKS: Because we'll have them.

LESLIE KENDRICK: Explain why [LAUGHS].

ASHLEY DEEKS: Well, so it's interesting that this is the focus of the international discussions. I think it's exactly for the reason you just evidenced. Which is, oh, my god. This can't happen.

LESLIE KENDRICK: Yeah [LAUGHS].

ASHLEY DEEKS: If we're in a world in which there are killer robots--

LESLIE KENDRICK: Oh, right.

ASHLEY DEEKS: --you and Elon Musk will never sleep again.

LESLIE KENDRICK: Right.

ASHLEY DEEKS: And I should just note that one of the reasons that I was interested in the "Predicting Enemies" piece was that I think we're quite some way from a world of killer robots. But it did strike me that there were lots of ways in which machine learning could be used in the military setting before we get to the killer robots debate. And in some ways, the killer robots debate has taken all of the oxygen out of the room for the other discussions.

RISA GOLUBOFF: You think it's a decoy?

[LAUGHTER]

ASHLEY DEEKS: Yeah. It's the stalking horse to the killer robots.

RISA GOLUBOFF: Oh, you go worry about the killer robots. And, meanwhile, we're going to be over here doing all this other stuff--

LESLIE Doing step one.

KENDRICK:

RISA GOLUBOFF: --secretly in the double black box.

ASHLEY DEEKS: Perfect

LESLIE KENDRICK: Perfect.

ASHLEY DEEKS: That should have been my abstract.

[LAUGHTER]

So the discussion is going on in a group called the Convention on Certain Conventional Weapons, which is an umbrella treaty under the UN auspices, although it's an independent body made up of a host of states, including the United States, China, Russia, and 180-some states, I think. It operates by consensus. And so they've, in the past, done things like regulate landmines, explosive remnants of war, blinding lasers. So things that are maybe not creating the level of panic that killer robots does. And you won't be surprised to hear that there has not been consensus about how to proceed on this.

LESLIE KENDRICK: Yeah. Because how different is a killer robot from a drone really? Super different because they're completely autonomous and there's no one telling them what to do, or what?

ASHLEY DEEKS: Yep. So that is what people are envisioning, I think, when they talk about killer robots. They're envisioning systems, often embodied in a robot, that are programmed to go out and identify certain targets and use force against those targets autonomously without--

LESLIE KENDRICK: So this is like the Terminator.

ASHLEY DEEKS: --without checking back in to a human controller who gives a thumbs up or a thumbs down to the use of force. That, I think, is what people are most concerned about.

RISA GOLUBOFF: Now, I'm up that night, too. Just so we're clear.

LESLIE KENDRICK: That's what the Terminator was, right? He was a killing machine that's like a machine that--

ASHLEY DEEKS: Correct.

LESLIE KENDRICK: --goes out and kills people.

ASHLEY DEEKS: Correct. But there are some systems currently in use that have the capacity to do a little bit of killer robot-ing. But they're being used in very constrained settings. So for example, South Korea, near the border with North Korea, has set up a number of systems that can autonomously detect targets and could fire on targets. But that second thing, that switch isn't switched on.

LESLIE KENDRICK: OK.

ASHLEY DEEKS: So it's currently-- there are still what we call humans in the loop.

LESLIE KENDRICK: It's just interesting, because it seems like part of the question is just, do you need a whole new set of rules, or could you have a kind of per se rule that certain types of weaponry, just per se, don't comply with the standards that we have? It seems like it's kind of one of these legal questions of, are we going to say we have standards that apply to everything, or do we need some special rule for this special type of thing?

ASHLEY DEEKS: Right.

LESLIE KENDRICK: Or are the existing categories elastic enough to contain it?

ASHLEY DEEKS: I'd say there may be three steep views on this. One is ban them. And they are supported by a bunch of NGOs who also believe that we should, quote, stop killer robots, unquote. In the middle bucket are states that are nervous about the prospect, that think there should be a form of regulation of what types of autonomy are and are not acceptable, but maybe wouldn't go so far as to ban them in all circumstances. So for example, maybe you would be comfortable if you had defensive systems on a ship that operated autonomously to shoot down incoming missiles. So fixed platforms, clear target. That might be OK.

And then in the third category, which is where I think the US is, and I think Russia is, probably, also as well, is that the laws of war exist and are sufficient to regulate these machines, these systems, already. There are a couple of provisions that would be really important. One is the idea of distinction, which is a core law of war principle that requires a state to distinguish between civilians on the one hand and military objectives on the other. There's also a principle of proportionality, which says that even once you've decided that you have a military objective in front of you, you can't targeted if it's going to cause excessive harm to civilians or civilian objects around it.

And there's a third provision that's important that-- it's called Article 36-- weapons reviews. It requires states to conduct weapons reviews, legal reviews of weapons, to make sure that if they were deployed, they wouldn't violate those first two principles. So the US says, you can't deploy, lawfully, a system that you're not confident can comply with distinction and proportionality. So that's the restriction. We don't need more law of armed conflict on that. Those are really important principles. And those would govern.

So we might develop some non-binding norms about human control, the importance of keeping a meaningful human control, and we might spell out a little bit what that means. But in general, in terms of new legal rules, we don't need them. And I would note, it's pretty unlikely that you would achieve consensus on a binding new treaty on this.

LESLIE KENDRICK: So it sounds like there are a lot of challenges in regulating algorithms and AI internationally. What are our prospects domestically?

ASHLEY DEEKS: So I think it is quite unlikely that we will see regulation of military and intelligence use of the kinds of tools we've been talking about for the same reason that we don't often see heavy regulation of how the military engages in its operations on the ground. Congress has had a very hard time in general dealing with technology and regulating technology. And it's interesting. If you look historically, there have been cases in which corporations have been extremely powerful, and Congress has gotten on-board to regulate them. Whether we're talking about big oil, or we're talking about the auto industry, or the pharmaceutical industry, we've seen these major powerful actors in Congress stepping in to say, you're not doing it quite the way that we think is most protective of the US citizenry or so on.

Today, in the past decade, we see other very powerful technology companies emerge. And we see Congress basically standing to the side. We have not seen any kind of regulation of facial recognition software, whether being used by private actors or being used by law enforcement. We are watching Congress starting to try to get its arms around privacy questions. One of the biggest challenges with these social media companies is how much data they have on us and what they're doing with it. Often not telling us what they are doing with it are using very, very fine print to do so. And Congress is just now, I think, trying to wrestle with how to do it.

And these questions are hard I don't mean to totally undersell Congress on this because you do need to have some basic understanding of how the technologies work. And that doesn't tend to be Congress's forte. You do need to have a vision for what you want the final outcome to look like. And at this point, Congress has a potential, I wouldn't say model, but place to look in what the Europeans have done with the GDPR, the General Data Protection Regulations.

So I think it's going to be a very slow process of regulation domestically. And what they will be regulating is the private sector rather than the government actors using this big data for national security purposes.

LESLIE KENDRICK: And you've written an article, "Facebook Unbound," that's largely about how big and expansive these private companies have become and all of the different ways that they use data, and that, on the one hand, it's very hard to regulate-- on the other hand, there might be some urgency involved here. Do you think?

ASHLEY DEEKS: I'm not sure urgency has ever gotten Congress to regulate faster.

[LAUGHTER]

LESLIE KENDRICK: Well, what's your view? What's your view?

ASHLEY DEEKS: Well, one of the things that I was puzzling over a little bit is why Congress is having such a difficult time. And it struck me that there were some parallels between why Congress finds regulating Facebook hard, and why Congress finds regulating in the national security space hard-- which includes the sort of lack of technical sophistication or comfort with technology. A worry about stifling innovation.

I think that's really in play here. Where we are confronting a potential adversary, China, that is not pulling any punches on developing AI. So I think some of those same challenges are making it hard to regulate. On the other hand, we are seeing changes being made by these companies without explicit direction from Congress. Some of this flows from congressional hearings and the threat thereof.

LESLIE KENDRICK: Right.

ASHLEY DEEKS: Knowing you're going to have to provide some sort of explanation for what you're doing. Public pressure, too, has led to some changes within the companies. And we're now seeing Facebook has proposed basically a Facebook court. A Facebook Supreme Court that would help it adjudicate what should stay up and what should come down. Because I think on the one hand, they're confronting criticisms that they're acting to totally control people's speech. It's all within this non-democratic actor to decide what constitutes a threat of violence, what doesn't. And on the other hand, they're being criticized for leaving up things that are very pernicious.

So in some ways, they've thrown up their hands and say, OK, let's try to come up with some more neutral arbiter to help us on this, because we realize that we're not doing a perfect job here.

RISA GOLUBOFF: Although, I have to say, it gives me a little bit of the heebie-jeebies to think of an alternative dispute system outside of the courts, which have their own issues, but at least have all kinds of built-in systems for trying to provide procedural justice and substantive justice. And to think Facebook courts. I don't know. That sounds-- it's not quite killer robots--

ASHLEY DEEKS: [LAUGHS]

RISA GOLUBOFF: --but Facebook Supreme Court? That also is going to keep me up at night.

ASHLEY DEEKS: Maybe we'll have them adjudicate some killer robots questions.

[LAUGHTER]

That'll really send you into a tailspin.

RISA GOLUBOFF: Yeah. Exactly.

ASHLEY DEEKS: I think it would not, obviously, foreclose a resort to Article III courts, but it would be an effort to bring a body of experts together who have a little bit of remove from the company. I think there's a question of how--

RISA GOLUBOFF: How much?

ASHLEY DEEKS: How much?

RISA GOLUBOFF: Right. How do you create those systems?

ASHLEY DEEKS: And Facebook being the ultimate arbiter.

RISA GOLUBOFF: Right.

ASHLEY DEEKS: But I think it just goes to show that the difficulty that we're seeing on both the domestic and international plane in reaching consensus about how to deal with these new technologies.

LESLIE KENDRICK: This has been kind of a recurring theme this season about the ability of the law to regulate new technologies depends on legal actors understanding new technologies. And Larry Lessig, many years ago in thinking about intellectual property, said, there's the difference between east coast code and west coast code. East coast code being law and west coast code being technology. And there are big questions, I think, in lots of different fields about the extent to which east coast code can keep up with west coast code.

Do you have any thoughts about ways that the legal system could get better? Whether we're talking about Congress. Whether we're talking about the courts. The ways that various types of legal actors could get better at keeping up with and understanding technologies so that these hard questions can be answered a little bit more easily.

ASHLEY DEEKS: So I have two thoughts. One is something I think Congress is already trying to grapple with and improve on, and that is bringing actors into the congressional space, into members' offices, onto committees, that do have particular technological backgrounds to try to get both the members and other people around them smarter on some of these challenges. And so there used to be an office in Congress that was sort of an office of science and technology. A little bit like the Congressional Research Service for science nerds.

LESLIE KENDRICK: Mhm.

ASHLEY DEEKS: And I think that office went away, but there's some interest in trying to bring it back. So it could write plain English reports, presumably for Congress to read on machine learning AI, particular challenges that Congress is facing. So that would be one thing.

The other thing is a pitch to law students to actually spend some time trying to get smart now on, what are predictive algorithms? What is machine learning? What is AI? There is a lot out there that's written in relatively accessible language. But it seems to me that in a lot of these cases, we're going to need a lawyer sitting in one seat and the computer scientist sitting in the seat next to her, trying to help craft code that is responsible, that's responsive, that's compliant with the law.

So I see a future in that left seat, right seat that's really important. And I guess, in some ways, that brings together the west coast code and the east coast code.

LESLIE KENDRICK: Mhm. Well thank you so much for being with us. Ashley Deeks.

ASHLEY DEEKS: Thank you for having me. I appreciate it. Good conversation. Thanks.

LESLIE KENDRICK: Fascinating.

[MUSIC PLAYING]

RISA GOLUBOFF: So on our last episode, when we were talking with Mike Livermore about big data and the use of big data in law for discovery and for dispute resolution and all kinds of what gets called law tech now, we were talking about how important it is for there to be philosophers in the room and real analytical reasoning taking place before you program computers to do machine learning in those spaces. And, boy, if we thought it was important there, then it seems way, way more important here, where we're talking about war and the most destructive capacities that human beings have today.

LESLIE KENDRICK: That's right it seems like the stakes are even higher here than they are in other areas. And I really liked Ashley's idea of the double black box, because it seems like an additional concern in the national security arenas, how a lot of these decisions are just not that visible. There's not a lot of external accountability, and so having the right people in the room seems all the more important.

RISA GOLUBOFF: I agree. And that raises a tension that I think has existed forever between expertise and democracy or transparency. And certainly going back at least to the progressive era around the turn of the 20th century in the United States, when there was the rise of new disciplines, the rise of social science expertise, there was the proliferation of federal agencies based on that expertise and a huge populist pushback that, we don't want eggheads sitting in a back room making decisions. We the people want to be making those decisions.

LESLIE KENDRICK: That reminds me of an example that just came up recently where San Francisco became the first American city to ban the use of facial recognition technology by city actors, including the police department. And I had questions about that, and they basically track exactly what you're saying. Is that a decision made out of expertise, because there's certainly a lot of expertise about technology in San Francisco? Or maybe it's the epicenter of technological development and this is a populist reaction to that in some way. This is suspicion about the very technologies that are proliferating right around there. And I'm not sure exactly how to process it.

RISA GOLUBOFF: Yeah. It will be interesting to see what other cities and states do in response to similar changes in technology. Louis Brandeis, a famous jurist, described the states as laboratories of experimentation, laboratories of democracy. And that's true, I think, both of states and cities. And San Francisco's often been, whether you want to call it the cutting edge or an outlier--

LESLIE KENDRICK: Right.

RISA GOLUBOFF: San Francisco has often been very experimental in its policies. But it will be really interesting to see how and in what ways other states and cities, and ultimately the federal government, follow or don't follow those footsteps.

LESLIE KENDRICK: Yeah. And it seems similar to what Ashley said about the national security context, where they're trying to figure out how to apply old principles, long standing principles, to new technologies. And it reminds me of another early 90s sort of internet reference, so I'm clearly showing my Gen X creds here today. So along with the Larry Lessig east coast code, west coast code, there was a famous speech that Frank Easterbrook gave in an article that he wrote about cyber law and the law the horse, where he said, internet law. We're sort of treating that as-- it's a new thing. It's a different thing. The technology defines everything about the law in this area. And he says, that's kind of like the law the horse. That's kind of like if, in the 18th century, you had looked at a legal treatise and it had a whole page on horses and a whole page on cows and a whole page on butter churns. And that's not really the way that the law organizes itself. The law is organized in terms of principles. And those principles should be applied to new things rather than sort of dragged around by them.

RISA GOLUBOFF: I suppose what the technologists would say is, this thing is so new, and it's so different, that it's so different in kind that, even if you wouldn't have necessarily had a law of the horse, because a horse wasn't so different from a camel or an ox or--

LESLIE KENDRICK: Right.

RISA GOLUBOFF: --something else, that this new world order and the new technologies are so different that they really do require massive transformation in the law.

LESLIE KENDRICK: Yeah. I do think that that would be the pushback. And I think we're sort of still sorting all of that out. But it reminds me of what Ashley said about the killer robots, which I'm still freaked out about the killer robots. But is this a new technology that we can apply existing principles to, or is it sui generous? And I think it seems like, with a lot of these technologies, the first question is essentially that question. And that, I think, entails understanding what it is, which, that's always going to be new and different, and we have to have experts in the room to explain that.

But once you understand what it is, figure out, can this be contained and described by the existing principles, or is this something that really requires innovation in the law?

RISA GOLUBOFF: So I guess, for me, maybe the last question, a $50,000 question is, when you think about the killer robots, and you think about the law-- whatever that means to you. Does the combination of those two things make you more able to sleep at night or are less able to sleep at night?

LESLIE KENDRICK: Yeah. So killer robots on their own in a lawless society versus killer robots in the law, I definitely feel better about killer robots in the law. And I think talking with Ashley and realizing there are people who are experts in both the technology and international law and national security here are thinking about those things. That definitely makes me sleep better than if it was just the killer robots. But Ashley is often the person from whom I find out about the new thing like the killer robots [LAUGHS].

RISA GOLUBOFF: So she's responsible for a lot of your sleepless nights.

LESLIE KENDRICK: Yeah. She has to do with a lot of my nightmares. But I'm glad that she knows about these things and is thinking about them.

RISA GOLUBOFF: Well, I'm hopeful that people out there thinking about the law and the killer robots will make sleeping at night easier and not because we're naive, but because the law really does play regulatory roles that we hope it will and does play those roles in positive and productive ways.

[MUSIC PLAYING]

LESLIE KENDRICK: Well, that's all we have for you today. If you like "Common Law" on the east coast, on the west coast, or anywhere in between, make sure to leave us a review on your favorite podcast app. Our algorithms are predicting you have good things to say.

RISA GOLUBOFF: You'll find a link to Ashley's paper, "Predicting Enemies," in our show notes at CommonLawPodcast.com. You can also check out our past episodes on "Game of Thrones," driverless cars, and much, much more.

LESLIE KENDRICK: And, Risa, before we go, let's give a shout out to our friends on the production staff-- Tyler Ambrose, Robert [INAUDIBLE], Tony Field, and Mary Wood. And also to Virginia Humanities. Our show is recorded at their studios. I'm Leslie Kendrick.

RISA GOLUBOFF: And I'm Risa Goluboff. We'll be back in two weeks with our season finale, where we'll hear what one federal judge has to say about the use of science in the court system.

SUBJECT: A major problem is that too many judges are intimidated by the notion that they would have to decide a scientific issue.

RISA GOLUBOFF: Hope you'll join us then.

[MUSIC PLAYING]