Common Law S4 Ep. 3: Kristen Eichensehr Transcript

[THEME MUSIC IN, THEN UNDER]

Risa Goluboff: Today on Common Law, cyberattacks with UVA Law's Kristen Eichensehr.

Kristen Eichensehr: There's a lot of concern about if a hot conflict were to break out, what does the cyber aspect of that actually look like, and a lot of fear that that would actually be extremely destructive.

[THEME MUSIC UP, THEN UNDER AND OUT]

Risa Goluboff: Welcome back to Common Law, a podcast of the University of Virginia School of Law. I'm Risa Goluboff, the dean. Today we're welcoming a new co-host, UVA law professor Danielle Citron. Danielle is a pioneer in the field of intimate privacy and was named a MacArthur Fellow in 2019 for her work in that area. Her book "Hate Crimes in Cyberspace" is considered a landmark work, linking cyber-stalking and civil rights, and the way online abuse jeopardizes people's key life opportunities. She is also the inaugural director of the Law School's new Law Tech Center, which focuses on pressing questions in law and technology. Her new book out this summer is "The Fight for Privacy: Protecting Dignity, Identity and Love in the Digital Age." Danielle, it is such a pleasure to welcome you to the show.

Danielle Citron: Thank you so much for letting me join in on the fun.

Risa Goluboff: We are thrilled to have you and fun it is going to be. Can you tell us a little bit more about how you first began writing about intimate privacy?

Danielle Citron: So when I was writing about cyberstalking, I noticed that the privacy invasions that so often victims suffered were sexually demeaning and sexually threatening. And at the same time, those privacy invasions often were suffered by gender and sexual minorities. So it of course got me thinking what is the kind of foundational privacy that each and every one of us needs? One of the core foundations of privacy is intimate privacy, the privacy of our bodies, our love relationships, and all the different aspects of intimate life. So that's what got me sort of started on the road.

Risa Goluboff: You know, you work on the regulation of online platforms, you work on, digital impersonation, like deep fakes that are becoming more and more common. You're so wide ranging in what you talk about. I just think you're such a model for the research that you do and then applying it into the real world.

Danielle Citron: Thank you so much.

Risa Goluboff: Tell us who is up as your first guest.

Danielle Citron: Today, we're going to be talking to UVA law professor Kristen Eichensehr about her work on the attribution of cyberattacks. In addition to being affiliated with the Law Tech Center, Kristen is the director of the law school's National Security Law Center. She's also a member of the U.S. State Department's Advisory Committee on International Law.

Risa Goluboff: Well, this is going to be excellent. We will be right back with professor Kristen Eichensehr.

[THEME MUSIC UP, THEN UNDER AND OUT]

Danielle Citron: Kristen, thank you so much for coming on today and talking to us about your work.

Kristen Eichensehr: Thanks so much for having me.

Danielle Citron: So Kristen, could you set the stage for us and describe what you mean by cyberattack? And then perhaps just give a few examples.

Kristen Eichensehr: Cyberattack is a broad term that covers a wide gamut of things. Anything from distributed denial of service attacks, to ransomware, to destructive attacks that wipe hard drives, up to and including things like the Stuxnet attack against Iranian nuclear facilities.

Risa Goluboff: Can you say more about that? What was the Stuxnet attack?

Kristen Eichensehr: So that is an attack that has been widely attributed to the United States and Israel working together to compromise Iranian nuclear facilities and to slow down their development of a nuclear weapon.

> **NPR: STUXNET RAISES 'BLOWBACK' RISK IN CYBERWAR**
> **Tom Gjelten:** The Stuxnet attack in Iran physically destroyed centrifuges by working through the computers that controlled them. Now we have to worry someone will use a similar worm to attack critical facilities here in the U.S.

Kristen Eichensehr: That was a big wake-up call I think for people that, you know, governments are active in this space and there's a lot that can happen. And then for a while, everyone talked about intellectual property theft. And then for a while, everyone talked about election interference. And then if you think back just to the last year, a big story for the United States has been ransomware. What previously was thought of as just a law enforcement matter has now become a national security issue.

Risa Goluboff: What first piqued your interest in cyberattacks and whether and how we name the perpetrators of cyberattacks?

Kristen Eichensehr: My interest in cybersecurity issues more generally goes back more than a decade. It was sort of a hypothetical interest of how would international law deal with a cyberattack? And it's obviously something that has gotten more concrete as we've had more cyber incidents play out.

Danielle Citron: Yes.

Kristen Eichensehr: I wrote a paper a couple of years ago called "Public Private Cybersecurity," and that was the place I first discussed the cyberattack attribution question, because it was really striking to me when I wrote that paper that you had private companies going after states saying, you know, we believe this foreign intelligence service or this foreign military is responsible for a cyberattack against our customer. And that just struck me as a really interesting development to see companies kind of tussling with states in that way.

Risa Goluboff: Right.

Kristen Eichensehr: The more attributions we saw play out both from companies and from governments, it seemed like the time was right to think about the legal issues surrounding attribution as well.

Danielle Citron: So we're tossing around this word attribution, but for listeners who might not fully understand what that means, can you define it for us?

Kristen Eichensehr: So attribution is the process of assigning responsibility for the commission of a cyberattack. So it can be technical attributions, so that's the computer from which an attack was launched. You can talk about also legal and policy aspects of it. So you might be talking about the individual who operated the computer that launched the attack, or you might be talking about the state or criminal enterprise that employs the person who sat at the computer and launched the attack.

Danielle Citron: So you've been doing a lot of research into attributions. How many are we talking about anyway?

Kristen Eichensehr: It used to be that I was tracking, you know, one or two a year, and then it really started to be a whole flurry of them. So we were seeing a lot more, a big uptick and not just in the United States, but other allied countries joining in, private companies in the game. And so I started to think, what are the legal issues related to this? Oftentimes attribution is framed as kind of a press release, but there are a lot of legal issues embedded in it. And so unpacking those became a big part of my research.

Risa Goluboff: So talk a little bit about state-sponsored cyberattacks. When did we start to see and talk about those in particular and how have those changed over the past decade?

Kristen Eichensehr: Well, we started to see them long before people really started talking about them – or certainly before states started talking about them. There were sort of whispers about state actions in the mid-2000s, but things really accelerated a lot with the revelations about the Stuxnet attack in that period.

Risa Goluboff: Okay.

Kristen Eichensehr: That was years before the United States established Cyber Command, but that kind of opened the flood gates of talking more about state-sponsored actions.

Danielle Citron: So just by way of background, the United States Cyber Command is a Department of Defense unit, which was created in 2009 and focuses on cyberspace.

Kristen Eichensehr: Yeah. The first time the United States formally accused another foreign government of a cyberattack was in an indictment of Chinese People's Liberation Army officers in 2014. And that was for intellectual property theft from U.S. companies.

> **AP: ATTORNEY GENERAL ERIC HOLDER ANNOUNCED CYBER-ESPIONAGE CHARGES MONDAY AGAINST FIVE CHINESE MILITARY**
> **Eric Holder:** Today we are announcing an indictment against five officers of the Chinese People's Liberation Army for serious cybersecurity breaches against six American victim companies. These represent the first-ever charges against known state actors for infiltrating United States commercial targets by cyber means.

Risa Goluboff: Why is attribution important? What work is attribution doing?

Kristen Eichensehr: It's truly a great question. The early theory was sort of going public with state action was going to be naming and shaming. This was going to deter states from engaging in this bad activity. There's a lot of skepticism about that. Instances where China has engaged in allegedly intellectual property theft well after 2015 agreeing with President Obama that they would stop doing that sort of thing.

> **OBAMA: U.S., CHINA WON'T ENGAGE IN CYBER THEFT OF TRADE SECRETS**
> **President Obama:** We've agreed that neither the U.S. or the Chinese government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information for commercial advantage.

Kristen Eichensehr: There's a lot of skepticism about that kind of macro-level deterrence. I think you can argue maybe that there are other purposes to attributions. So when you have an individual who's charged and then an indictment or sanctioned, that makes the consequences pretty personal. So you might think about kind of micro-level deterrence, changing the behavior of particular foreign government employees or entities, companies that are sanctioned. Also what we've seen, I think, with some of the more technical attributions that come with indicators of compromise and other sorts of technical information aimed at companies and other entities, the attributions are, are made public to allow people to secure their systems and networks, right? They're informative in a way that lets them respond and protect themselves.

> **TODAY: APPLE ISSUES EMERGENCY SECURITY UPDATE**
> **Miguel Almaguer:** This morning, an urgent warning from Apple alerting all users to update the software on their devices. Independent researchers warned an Israeli spyware company NSO Group developed a tool to secretly take control of nearly any Apple computer, iPhone, or watch.

Kristen Eichensehr: And then I also think – this ties into my international law work – that another purpose the attributions have is to bring clarity to what's going on in cyberspace, and this plays into discussions about norms and international law.

Danielle Citron: Does the state's attribution of a cyberattack have an impact on domestic law and the way companies act and might a state actor kind of hold back from an attribution in the thought that companies don't want them to do it, or it might have implications for insurance?

Kristen Eichensehr: As a matter of domestic law, government attribution can have certain kinds of effects, at least potentially. You mentioned insurance. That's been one of the sort of hot topics. And it's not exactly clear how that's going to play out. So there was a cyberattack in Ukraine in 2017 called NotPetya, widely attributed to Russia.

> **AL JAZEERA: MASSIVE CYBER ATTACK SPREADS RANSOMWARE VIRUS GLOBALLY**
> **Mereana Hond:** Cyber specialists for companies around the world joined the scramble to contain it. From Russia's state oil giant Rosneft, Danish shipping conglomerate Maersk, U.S. drug company Merck, to India's largest container port in Mumbai.

Kristen Eichensehr: It initially spread from tax software in Ukraine to all around the world, eventually caused about $10 billion worth of damage, and hit a number of companies. So Merck, Mondelez, a bunch of others. And those companies had cybersecurity insurance. So they tried to collect under their policies and they were denied under exclusions for "hostile and war-like action." There was just a recent state court decision in New Jersey about Merck. And there, the court said the exclusion did NOT apply, so their property insurance coverage DID cover the damage from NotPetya. But it's really an area that's evolving a lot and it's not clear which way courts are going to go on that.

Risa Goluboff: Attribution right now is in the hands of so many different actors, right?

Kristen Eichensehr: Yeah.

Risa Goluboff: States, nongovernmental bodies like security firms or the media, and the amount of information that gets revealed about each attack, why a certain actor is believed to be the perpetrator, the level of evidence necessary to make an attribution, right? These just vary incredibly widely. So you're proposing to change this kind of anything goes way of doing things. So what do you see as the problem with the current approach and why isn't it working?

Kristen Eichensehr: If you look at the kind of high-end of state action – so things like use of force in self-defense against an armed attack – there's at least some emerging consensus there. You need kind of clear and convincing or clear and compelling evidence. But if you're talking sort of the normal – I hesitate to say it – but becoming more run-of-the-mill cyberattacks that we're seeing, they're not at that high level. So then what's the legal standard? So what I've argued is that when there's a public attribution to a state of a cyberattack, that attribution should be accompanied by sufficient evidence to enable cross-checking of the attribution by other parties. Risa, you mentioned there are a lot of different entities who are engaging in attribution, so you might have a government attribution that a private-sector cybersecurity company can confirm, can sort of validate.

Risa Goluboff: How do you ensure that kind of standardization or consistency across different sovereign states that might not be interested in the same level of disclosure or playing by the same rules?

Kristen Eichensehr: It's incredibly messy.

Risa Goluboff: I mean, that's a question for international law, right? An endemic question.

Kristen Eichensehr: Yes. Yes, it is. I have this legal proposal that I think is sensible and reasonable and helpful. But it's worth noting that states that have taken a position on the question, including the United States, have said that they are NOT legally required to give evidence to support their attributions. They say that they, you know, they might do that as a matter of policy, but they are not legally required to do that. You know, this is a, this is a bit of an uphill battle that I'm waging.

Danielle Citron: And I guess it's in part because they don't want to have to show the work.

Kristen Eichensehr: Yeah.

Danielle Citron: They may reveal sources and methods. What's your take on that?

Kristen Eichensehr: I think it's pretty short-sighted. It's a view derived from a position of luxury at the moment where the U.S. and the UK are some of the most prolific attributors. And so they're thinking of it in terms of how it would affect their own behavior and not in terms of how it would affect the behavior of other potential attributors going forward. So I'm very worried about these kind of "trust us" attributions that don't come with evidence, because you could easily imagine states that just get it wrong or states that deliberately get it wrong and accuse other states and use that as a pretense for all sorts of things. I think that the US/UK position is a little bit short-sighted for that reason. I think they should be looking longer term.

Risa Goluboff: Is there something proprietary about the information or, you know, what's on the other side of the ledger, what would make someone not want to share that information?

Kristen Eichensehr: Yeah, I mean, there is a risk to disclosing sources and methods, and governments have an almost visceral dislike of publicly disclosing information in a lot of circumstances.

Risa Goluboff: That's just kneejerk. That's just – we're not going to show it if we don't have to.

Kristen Eichensehr: Exactly.

Risa Goluboff: Right.

Kristen Eichensehr: To a large extent, they're already doing it. You see indictments that are 50, 60, 70 pages. They're quite detailed. And so they've shown that they CAN actually provide that information. And moreover, you also see the U.S. government in particular, fairly often relying on attributions done by credible private-sector entities. This has been true since 2013. One of the big sort of moments in the history of attribution of cyberattacks was when a company called Mandiant released what it called the APT1 report, which was a very long, very detailed report that accused China of intellectual property theft.

> **FRANCE 24: THE INTERVIEW - GRADY SUMMERS (VP MANDIANT) ABOUT CHINA'S CYBERWARRIORST**
> **Grady Summers, VP Mandiant:** These hackers are a group that we call APT1 or Advanced Persistent threat One, are in fact members of the People's Liberation Army unit 61398 ... It's not an accusation that we make lightly. Uh, we're certain of it based on the evidence that we've put together. The good thing though, is that we've been very open with this evidence. We've released over 3,000 indicators, a 60-page report, a lot of details that other researchers can review and draw their own conclusions as well.

Kristen Eichensehr: In the wake of that, you would see U.S. government officials saying, "Well, you know, as Mandiant has said, China is engaged in this kind of behavior." You see the government using private-sector information and private-sector attributions to talk around classified information. A lot of these attributions could be done with substantial evidence.

Danielle Citron: Do you come down on any particular standard? That is, the amount of evidence that you have to show that would qualify as an attribution?

Kristen Eichensehr: The standard I sort of settle on in the paper is something akin to a verifiable preponderance standard, so it sort of mixes process and amount of evidence, right? You see in international law, assertions that, you know, states have to act reasonably. To me, I think reasonable means "more likely than not to be true." You have to have the states that are acting in good faith and saying, "we believe this to be true." You don't have to be 90% sure it's true, or even 75% sure that it's true, but it has to be your sort of best assessment of the truth of the accusation.

Danielle Citron: Are you worried at all about mischief makers? You know, a sock puppet scenario where A accuses B and it's definitely not B, but it's this other story that they're not going to tell us about. And would your verifiable preponderance of the evidence standard catch that?

Kristen Eichensehr: I hope it would catch it. And I am worried about that. I'm worried about false flag operations. We've seen it happen. And I think we're likely to see more instances of that going forward. And so I hope that a requirement to disclose evidence and support accusations would foster the catching of those kinds of erroneous claims, whether they're deliberately erroneous or accidentally erroneous. They're both, as you said, mischief-making so I do think having more evidence guards against that kind of error.

Risa Goluboff: The U.S. announced this "defend forward" policy in 2018, this new Defense Department cyber strategy and a U.S. Cyber Command vision document. The strategy – I'm going to quote from it – aims to, quote, "defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict," end quote.

Kristen Eichensehr: So this was a shift in posture to a much more active idea of what it means to defend. What they mean by that is defending outside U.S. government systems. So they talk about defending as close as possible to the origin of the attack. They're operating inside other people's systems, often abroad.

Risa Goluboff: It's pretty aggressive as a defense, right? It seems like calling it "defend" is a little bit on the line.

Kristen Eichensehr: It's a marketing tool to be sure.

Danielle Citron: Do we know what pushes the U.S. to take this aggressive defend forward or offensive measures policy?

Kristen Eichensehr: I think it was just the idea that U.S. attempts to be truly defensive and defend its own systems were failing. The United States was constantly getting hit with different kinds of cyberattacks, and other states to which these attacks were being attributed were not backing off, right? This is in the wake of Russia's interference in the 2016 election, in amidst fears looking forward to the 2018 midterms. It's sort of in that environment that you see the executive announce these policies. They were also getting pressure from Congress. Congress passed a couple of years ago in one of the National Defense Authorization Acts, what some people refer to as a mini cyber AUMF, or a mini cyber Authorization for the Use of Military Force, that explicitly authorizes the military to take action in certain circumstances against cyber threats that are attributable to Iran, North Korea, China, and

Russia. So there's pressure from Congress, there's I think pressure within the executive branch to be better positioned to fend off attacks, and more public awareness, particularly in the wake of 2016, about foreign governments successfully attacking United States infrastructure.

Risa Goluboff: Let's say the international community were to agree to a law of attribution and agree to the level of evidence that you think is right, or some other one. But let's, let's just say, for example, the Eichensehr Plan.

(Kristen laughing)

Risa Goluboff: How much confidence do you have that nations will stick to the plan, given their different relationship to the problem?

Danielle Citron: I love how polite that was – their different relationship to the problem.

(All laughing)

Kristen Eichensehr: I think some states would stick to the plan and some probably wouldn't because they don't stick to many plans in international law.

Risa Goluboff: Right.

Kristen Eichensehr: I still think, you know, even if there's not perfect adherence, there is benefit to greater transparency. So, the attribution statements that we're seeing from states and from private companies are some of the best information we have about what's going on behind the veil of the states' cyber commands or their intelligence services, —— what they're actually up to in cyberspace. So, I think the attributions can be important for that reason. But states – to my mind, at least – are kind of underutilizing them. I wish they would be clearer, not just about their evidence, but also about what they think actually violates international law.

Risa Goluboff: I wonder if you could say more about that.

Kristen Eichensehr: So we see attribution statements that condemn all sorts of behavior, call it irresponsible and reckless, but they sort of hold back from actually showing their cards about what they think is an international law violation versus what is just a domestic law violation or otherwise just bad behavior. So I think they could be doing more and more to foster this clarity about international law and sort of set up the rules of the road going forward.

Danielle Citron: What do you make of the argument that all law of attribution is just political all the way down? So international law has no sort of place. You know what I'm saying? As I was reading your work over the weekend, which I lovingly did, someone tweeted me or DM'd me to say, “ah, it's all political hogwash or whatever.” So what do you say to those folks?

Risa Goluboff: Can I just say for those who can't see, Kristen put her head in her hands when Danielle suggested it might be political all the way down. Okay, go ahead.

Kristen Eichensehr: Well, when I teach cybersecurity, I teach cybersecurity law and politics because I don't want to have to disentangle the two in a very robust and, you know, hard-line fashion. I do think there's a hefty dose of politics involved, but we have seen circumstances throughout recent history where international law constrains states and shapes their behavior. But even beyond constraining states, I think international law provides a coordinating mechanism. So even if you can't get states to agree, I think there's value to setting up rules that allow states to understand where other states' red lines are. So that's a pretty realist answer in light of some of the actors we see in the world today that are big actors in both the cyber and the non-cyber sphere. But I think there's value to the international legal system, even beyond getting everyone happily to agree and comply and move along.

Risa Goluboff: Thinking about the relationship between cyberattacks and hotter conflict, that brings to mind the cold war.

Kristen Eichensehr: Yeah.

Risa Goluboff: Do you see a spectrum of cold to hot?

Kristen Eichensehr: Yes. I've been focused mostly on states, but we see some level of just criminal activity all the time as well. And that's kind of going on in the background. And the other activity that's going on in the background all the time is espionage. States spying on each other – that's been going on forever. That's not a cyber issue, but the amount of it has increased, I think, with the cyber intrusion possibilities. And the possibility of intrusions that are designed initially for espionage being used for more destructive purposes, should the occasion warrant, has become a big concern. So if you see an intrusion by a state, you don't necessarily know at the outset, is this just espionage or is this laying the groundwork for something more destructive? Because having the access can mean it can be used in a variety of different ways.

Risa Goluboff: Okay.

Kristen Eichensehr: This was a big concern about a year ago when the Solar Winds compromise was discovered.

> **CBS SUNDAY MORNING: THE THREATS ARISING FROM THE MASSIVE SOLARWINDS HACK**
> **Dick Durbin:** This is nothing short of a virtual invasion by the Russians into critical accounts of our federal government.
> **Mitt Romney:** And it is an extraordinary invasion of our cyberspace.
> **Ted Koppel:** The Russians, it's believed, hacked into the software of a company called Solar Winds, causing them to push out malicious updates, call it a cyber virus, infecting the computer systems of more than 18,000 private and government customers.

Kristen Eichensehr: There was confusion at the outset about what is this that we're looking at? Is this espionage? Is this something more? That goes to your question about hot conflicts or cold wars. We're somewhere in a conflict that could easily escalate either deliberately or – very worrisome – unintentionally. But you see cyber popping up and it's being used as a tool by states, in conjunction with hot conflicts – so that's kind of Ukraine – but also in anticipation of potential conflicts later. So there've been reports that the United States is inside Russian networks and that the Russians are inside U.S. networks. Those are probably not the only states for which that's true. So there's a lot of concern about if a hot conflict were to break out, what does the cyber aspect of that actually look like? And a lot of fear that it would actually be extremely destructive.

Danielle Citron: We saw in your work that it's only really in 2014, that the U.S. seems to make an explicit or official attribution for cyberattack. Why'd it take so long, cause clearly there was stuff going on long before then.

Kristen Eichensehr: So it took a while for the United States to be willing to show its cards about what it knew about what China was doing. And it took a lot of building frustration at U.S. businesses being hit over and over and over with theft of intellectual property, before the government would do anything. Defensive measures weren't working, nothing was seeming to stop these incidents, and so this was a move to go public by the government and kind of try and change behavior. So going back to the kind of macro deterrence idea, changing state behavior with naming and shaming didn't really work. And I think the other reason the government ultimately went public in 2014 is because private companies, cybersecurity companies had started doing these attributions. And so everybody who was involved in this issue or in the cybersecurity field, knew what was happening, knew who was responsible. And so the government began to look a little silly because they wouldn't actually name names. And so I think the shift in 2014 was to be a little bit more transparent and to try and throw the weight of the government behind an attempt to change behavior. After the Mandiant report in 2013, you sort of knew if the government said, “Oh, it's an advanced, persistent threat,” they meant either Russia or China. So, the government finally started saying, “No, actually we mean China.”

[THEME MUSIC COMES IN]

Risa Goluboff: Thank you so much for this conversation, Kristen, it was really fascinating.

Kristen Eichensehr: Thanks so much for having me. This was great.

[THEME MUSIC UP, THEN UNDER]

Risa Goluboff: Danielle, I take it, the fact that we're all so implicated in this virtual world means we're all vulnerable to these cyberattacks.

Danielle Citron: Yes.

Risa Goluboff: So where do you see the intersection between the cyber security and the attribution questions that she's talking about and the subjects that you study?

Danielle Citron: Human beings are our weakest link, like, we're the biggest problem, really not necessarily systems. And we saw that with the DNC hack. It was John Podesta's emails. He clicks on a link, and that then gives access. You know, once you get inside a system, then you can run amok. And so, you know, absolutely the world of, of our interconnected communications, social media, has a direct link to cybersecurity because it's human beings that are allowing people into systems.

Risa Goluboff: Right, right.

Danielle Citron: Kristen is more focused on the threats that come from state actors, but those state actors are gaming and manipulating the individuals that I write about too. The intimate privacy violations that I write about also has a government cybersecurity story because governments are targeting journalists and creating deepfakes, deepfake sex videos to discredit the journalist who then doesn't write about human rights abuses. The world of cybersecurity and the vulnerabilities that individuals create are the same vulnerabilities that state actor hackers are going to glom onto as individual perpetrators do and companies do. And the companies are the digital handmaidens of the state actors.

Risa Goluboff: In addition to the reasons, you know, particular states might be interested or, or international lawyers might be interested, I would think that the attribution process is also educative of people, right? I mean, the high-profile nature of many of these incidents and then the increased profile of them by attribution, would make those of us who are mere civilians in this world, more aware of the vulnerabilities that you're talking about.

Danielle Citron: It's so important, right? The educative value of talking about these kinds of incidents and realizing that it's just the everyday person who clicks on a link, or downloads software, visits a site that's not secured, and then wreaks havoc on the system that this person is a contractor for or subcontractor for the U.S. government. And then we've got big stakes. And so, absolutely, I think it's incredibly important for us to be able to see that we're the bug in the code. And I think talking about it is so important to teach us. We just click, like, share, we don't think about it. And I think if we had these events in our forefront of our minds, we might do less of it.

Risa Goluboff: Yeah. This relates to something Kristen said in talking about the proliferation of different kinds of cyberattacks. She said what's considered a national security matter has broadened as a result, and that all these different categories are now considered national security issues. And I'm curious, do you think that's a good thing or a bad thing? I mean, what are the implications of moving from a cyber mob to a cyber brigade? What does that do to the way the law operates, the way we think about it, the way harms and benefits are distributed.

Danielle Citron: That's a positive development in the sense that we're taking account of harms and seeing them and recognizing them. So to the extent that national security is widening its aperture for what's harmful and destructive, it's still not wide enough. We're not going to have a cyber Pearl Harbor, we haven't had it yet. But many steps below a cyber Pearl Harbor, many steps below Stuxnet are the smaller-scale attacks that as Kristen was saying, well, but we probably would not remotely recognize as requiring attribution are the kind of embedding in software – spies to wait, viruses to wait until the opportune moment strikes. And those create vulnerabilities because once it gets deployed, A, there's nothing we can do about it. And B, it can be profoundly harmful to hundreds of thousands of people. And so I'm glad to see us move a little bit, move that window of what harm counts. But we need to do better because so often we dismiss harms that aren't physicalized and economic. We just wave it away. If you think about how many individuals, livelihoods and opportunities are linked to these devices, they're in the millions and billions. And so we've got to appreciate that even though the risks are downstream, they can be grave and they can be activated at a much later date when it's too hard to line up all the actors responsible.

Risa Goluboff: Well, this was fascinating, Danielle, and I'm so glad I got to hear from both Kristen AND from you on these issues from such different perspectives, but all so interrelated, so thank you for the conversation.

Danielle Citron: This was such a wonderful introduction to being a co-host on Common Law.

Risa Goluboff: So happy to have you as a co-host.

Danielle Citron: I’m excited to do more of these with you.

Risa Goluboff: Me too.

[THEME MUSIC UP, THEN UNDER]

Danielle Citron: That does it for this episode of Common Law. If you'd like more information on Kristen Eichensehr's work on cybersecurity, please visit our website, Common Law Podcast dot com. There you'll find all of our previous episodes, links to our Twitter feed, and more.

Risa Goluboff: And in two weeks, I'll be joined by my fourth new co-host, UVA Law's Greg Mitchell. Together, we'll speak to Tom Tyler of Yale Law School about the role of procedural justice in policing.

> **Tom Tyler:** Whether people think the law is legitimate is AS important as whether they think they'll be caught and punished in determining whether to follow the law in everyday life.

Risa Goluboff: We can't wait to share that with you. I'm Risa Goluboff.

Danielle Citron: And I'm Danielle Citron. Thanks for listening.

[THEME MUSIC UP, THEN UNDER]

Emily Richardson-Lorente: Do you enjoy Common Law? If so, please leave us a review on Apple Podcasts, Stitcher, or wherever you listen to the show. That helps other listeners find us. Common Law is a production of the University of Virginia School of Law and is produced by Emily Richardson-Lorente and Mary Wood.

[THEME MUSIC UP, THEN OUT]