ALAN USAS: Hello. Welcome to Brown University Cybersecurity News podcast. I'm Alan Usas, program director for Brown's Executive Master in Cybersecurity. In this podcast series, we've been talking extensively about Apple versus FBI. To continue this conversation, we're here with Anna Lysyanskaya, associate faculty director in cryptography in the executive master in cybersecurity program and professor of computer science at Brown University. Her pioneering research and collaborations with leading companies in the IT sector, such as IBM, are driving the industry toward security solutions that balance the needs for privacy with accountability.

Anna, you recently wrote an op-ed piece in the Christian Science Monitor on why Apple should build a phone that even it can't break. Can you explain the argument that you make in that piece?

ANNA LYSYANSKAYA: So my main point in the piece is that Apple claimed when they first came out with this version of iOS, the operating system that the iPhone runs, when they first came out with it, they claimed that they could not break into it, even if they wanted to, that it was so secure that even if your phone fell into the wrong hands and Apple was somehow coerced to try to recover your data from it, they couldn't. And we now know that that claim was, in fact, not true, that they could be coerced. They have the technical capability to break into the iPhone, even this version of the iPhone, and in fact, that's exactly what the FBI is trying to get them to do.

So why does this create a problem? The problem is, of course, not with the FBI. We think that the FBI are trying to protect our interests here. The problem is that there are other governments and other players in the world, who might not be on the good guys' side. But now that they know that Apple has this technical capability to get at the data in the iPhone, they might want to coerce Apple to give them that capability, and they might act very adversarially towards Apple and towards whoever it is whose iPhone they're trying to break into.

So that's a security vulnerability that Apple introduced into its product. They didn't mean to, because they never meant to write this version of the iOS that would be able to retrieve data from a locked iPhone. They never meant to do this, but nevertheless, they are capable of doing it. So my main point is that this is a vulnerability that, in fact, they can fix rather easily.

The reason it's there in the first place is because you can update the operating system on your phone, and so Apple can write an update that would unlock it, to make a long story short. And
in order to eliminate this vulnerability, all Apple has to do is make the security features of the iPhone unupdateable so that once it’s locked, you cannot update that particular piece of it.

So that is my main point that Apple should have written it securely.

ALAN USAS: Thank you. Thank you very much, and it’s clearly an issue with a lot of nuances, and you’re very helpful in explaining them. But I wonder if you can now sort of project and think beyond the current iPhone issue and imagine yourself running product strategy at Apple. What direction would you be giving to your development teams?

ANNA LYSYANSKAYA: I think Apple has a unique opportunity right now, especially the way that they have positioned themselves in view of this legal battle. They are saying to the world, we want to lead when it comes to privacy. We really care about our customers’ privacy, and I think that the next move should be to put their money where their mouth is, to, first of all, fix that vulnerability that I talked about so that the next version of the iPhone and the next version of the iOS cannot be--you cannot update it out of security.

And secondly, create more privacy-friendly ways of storing your data on the cloud. Develop ways where your email, your phone conversations would be encrypted by default so that whenever you have an expectation of privacy, Apple would actually give you privacy. I think that’s something that is needed right now on a greater scale on the internet. We want our communications to be secure. We want our data to be secure, and we don’t realize how much information we’re leaking every time we’re doing anything. And Apple has an opportunity here to lead the whole world in the right direction.

ALAN USAS: To maybe come at this issue from a slightly different perspective, earlier in this podcast series, we spoke with Tim Edgar, who gave us some very interesting perspectives from a legal viewpoint and talked about the technology law gap around this particular case. As a technologist, Anna, what advice do you want to give to those focused on the law and policy aspects of this matter?

ANNA LYSYANSKAYA: I think that Tim made a really fascinating point in his conversation with you, Alan, when he said that lawyers and technologists are not speaking the same language when it comes to privacy. They often mean different things when they’re talking about privacy. What I think is really important is for both lawyers and technologists to understand what the other side is saying, for the lawyers to understand that there are limitations to what technology can do. So recently, President Obama gave a speech at the South by Southwest Conference in which he said,
look, you guys, you technologists, you have this absolutist view that once the data is encrypted, that’s it. The FBI can’t get to it. What’s up with that? Can’t we find some middle ground?

Well, the answer to that, President Obama, is that we can’t. Once data is encrypted, it is encrypted. Either you have security for everybody or for nobody, so there is no middle ground, and that’s sort of a computer science consensus. Nevertheless, I acknowledge, of course, that what President Obama wants is for law-abiding citizens to enjoy privacy and for the bad guys to not be able to get away with conducting criminal activity.

So I understand that where the president is coming from, where the FBI is coming from is a good place. They’re trying to do something good. And I also hope that they can also understand where we technology people are coming from. We’re also trying to do some good. What we’re trying to do is make sure that the internet is secure, because without security, the internet just won’t survive.

So right now, all this conversation about is encryption OK, the way that we see it is, is the internet going to survive or not? And so it’s really critical that encryption exists and that strong encryption exists and that it be built in as the default in every internet transaction. And unfortunately, right now, I’m not sure that the law and policy people are on the same page with us. But we’re not crazy privacy crusaders. We would love to be able to help the FBI. It’s just that we’re also realistic about the technological limits.

ALAN USAS:

It’s really clear to me that there are some really good and clear thinking going on on both sides of this issue, and I suspect that it will be in the conversation with the law experts and the technology experts for some time to come, even beyond the end of the Obama administration. So, Anna, I know you will want to continue and will continue to be a part of that. So thank you very much for helping us in our understanding of how encryption plays into the Apple versus FBI matter. In future podcasts, we’ll share additional perspectives on Apple versus FBI and on other cyber issues. For information on future podcasts, program news, and upcoming events, visit brown.edu/cybersecurity.