CONNECTICUT
LAW REVIEW

VOLUME 49 SEPTEMBER 2017 NUMBER 5

Panel

Data Collection and the Regulatory State

HILLARY GREENE, DR. JAMES COOPER, PH.D, AHMED GHAPPOUR, DAVID LIEBER, & DR. FELIX WU, PH.D

The following remarks were given on January 27, 2017 during the Connecticut Law Review*'s symposium,* "Privacy, Security & Power: The State of Digital Surveillance." *Hillary Greene, the Zephaniah Swift Professor of Law at the University of Connecticut School of Law, offered introductory remarks and moderated the panel. The panel included Dr. Cooper, Associate Professor of Law and Director of the Program on Economics & Privacy at Antonin Scalia Law School at George Mason University, Professor Ghappour, Visiting Assistant Professor at UC Hastings College of the Law, Attorney Lieber, Senior Privacy Policy Counsel at Google, and Dr. Wu, Professor of Law and Faculty Director of the Cardozo Data Law Initiative at Benjamin N. Cardozo School of Law.*

Data Collection and the Regulatory State

HILLARY GREENE,[*] DR. JAMES COOPER, PH.D,[**] AHMED GHAPPOUR,[***] DAVID LIEBER,[****] & DR. FELIX WU, PH.D[*****]

HILLARY GREENE: My name is Hillary Greene. I am a professor here at UConn, and I have the honor of being the faculty advisor for this symposium. More to the point, I have the pleasure of moderating Panel Three. It's my pleasure to introduce our panelists, who collectively will help to situate many of the issues regarding privacy and security that we have been talking about today within the context of the global and economic environments.

One function of this panel is to consider a question posed most directly by Professor David Thaw. His question was: Where is this data coming from? That is among the things we will be looking at today. We are also going to be examining individual's privacy interests vis à vis the private actors, specifically the businesses, many of whom are household names, that aggregate this consumer information. I will turn quickly introduce each of our panelists. Each will then have ten-minutes to discuss a particular idea or issue most important to them, and then after that we are going to have some discussion amongst ourselves, and then open it up to the room.

James Cooper is an associate professor at George Mason University's Antonin Scalia School of Law. He is the director of the Program on Economics and Privacy, and he has a PhD in Economics.

Ahmed Ghappour is a visiting assistant professor at UC Hastings School of Law where he is the director of the Liberty Technology and Security Clinic. He has a degree in Electrical and Computer Science Engineering. Professor Ghappour, owing to travel difficulties, could not be with us in person, but he is with us virtually via Skype. He is able to listening to us. But it is okay, we gave him permission.

David Lieber is the senior privacy policy counsel for Google. Previously, he was in private practice at DLA Piper, and prior to that he

---

* Zephaniah Swift Professor of Law, University of Connecticut School of Law.

** Associate Professor of Law and Director of the Program on Economics & Privacy, Antonin Scalia Law School at George Mason University.

*** Visiting Assistant Professor, UC Hastings College of the Law.

**** Senior Privacy Policy Counsel, Google.

***** Professor of Law and Faculty Director of the Cardozo Data Law Initiative, Benjamin N. Cardozo School of Law.

worked as a legislative assistant for Senator Dick Durbin.

Finally we have Professor Felix Wu from Benjamin Cardozo School of Law where he also the faculty director of the Cardozo Data Law Initiative. He has a PhD in Computer Science. You can see there is a theme emerging. We have got a lot of economics, business, and technology smarts on this panel.

We will begin with the basic proposition that data does not collect itself. In fact, as was discussed, much of the data at issue, the very data that government at times covets so greatly, is collected by market participants as it is part of their business model. It is how they make money, and it's how they supply the goods or services that so many of us want so much. It is essential to have their interests represented. What we lack in terms of volume of participants we have, perhaps, made up for in terms of size. I am pleased to have as our first speaker David Lieber from Google.

DAVID LIEBER: Great. Thank you, Hillary. Thank you once again to the University of Connecticut Law School, the Law Review, to Gavin and Eric, and Chantelle. I'm not sure if she's still here. But while the adulation that's being heaped upon all of you may seem excessive, for her in particular, she should really relish it. As a new parent, this may be the last time in her life that anybody in her life says, "Thank you." [Laughter] So, big thank you to Chantelle, who's been in touch with many of us.

We're at the point of the conversation where I'm conjuring up an old Washington adage, it's not that everything hasn't been said, it's just that not everyone has said it. So, into that void I go. I want to pick up a little bit on one of the conversations we had earlier, which I think is one of the more interesting and least-discussed aspects of this, which is sovereignty and jurisdiction. Since its embryonic stages, the internet, the advent of the commercial internet in particular, has challenged traditional principles of jurisdiction. And that's becoming more acute as companies like Google expand their ambitions, reach new audiences, and establish new footholds in other countries. It shouldn't come as a surprise when that happens that those countries want access to digital evidence on the same terms that the US government gets access to that.

One of the concerns, I think, that we as a company have is that when those countries enact laws that create conflicts with US law, we're placed in an untenable position of either complying with the laws of the United States, or those of the different country. And a deeper concern is that we are moving now toward a world of chaotic, conflicting laws.

That puts us in that untenable position. Our platforms, perhaps not unsurprisingly, are increasingly being the conduits through which governments conduct worldwide surveillance. And that has negative implications for a number of different stakeholders. It adversely affects the privacy interests and rights of non-US persons. It ignores the equities of other countries whose citizens may be surveilled under the policies of

another government. And it invariably creates a conflict of laws, which I was alluding to before. It creates problems for companies like Google, where we are faced with the choice of complying with one law and violating the law of another country.

So, I want to focus a little bit on how these tensions have surfaced in the US, which is not to identify the US as a culprit in particular, but the conversations in some respects have matured to a point where some of these issues are more concrete, and they can be discussed in that way. For quite some time, we've operated within this legal aphorism that Google, we are a US company bound by US law, and that's worked quite well for a long time. The challenge is that it's no longer tenable for the reasons I mentioned. We're moving into new countries. We established footholds there. Those countries believe they have jurisdiction over us, and they want access to digital evidence in the same terms that the US government has.

The challenge that we, Google, operate under an existing statutory framework, the Electronic Communications Privacy Act, enacted in 1986. One of the interesting aspects of that particular law, which governs our ability—or really, the government's ability to compel the production of user data from us, we cannot disclose communications content to non-US governmental entities. Mutual legal assistance treaties [MLAT], those were mentioned before. These are legal mechanisms under which other governments can obtain user data that belongs to US companies. Those MLATs have helped to fill the gap that's created by the Electronic Communications Privacy Act.

But the MLAT system is somewhat troubled. It's increasingly taxed by the number of requests that foreign governmental entities are making. It's slow, and it's cumbersome, and it's laborious, and labor-intensive. On average, MLATs take ten months to fulfill in the US, and that creates a lot of problems for foreign governments who are investigating ordinary crimes in their countries. Just consider for one moment the example of a crime that takes place in Germany, where the perpetrator is German, the victims are all German, the relevant conduct has taken place in Germany, but the relevant evidence lies with a US provider like Google. There are real, important questions to answer about whether in that particular circumstance US law ought to control.

And so, what we're seeing is governments become frustrated with the MLAT process. They're increasingly resorting to data localization laws, or even the naked, or extra-territorial assertion or application of their laws. And in many situations we have employees in foreign jurisdictions, who aren't part of the process of making US law, developing Google policies to comply with those laws, and they face civil and criminal sanctions when other governments seek to apply their laws in extraterritorial ways to US companies.

So, there's no panacea, I think, for the challenge we're facing in this

particular realm, but there is room for creative policy-making. The MLAT system is going to continue to be the primary means by which many countries obtain electronic evidence from US companies. There are certainly a lot of ways to improve that process. Resources is one way, but there also are many process-based improvements that can be made, and that's something that we and others have been working on for quite some time. But there also needs to be complementary mechanisms to the MLAT process to enable, in the example that I provided, other governments to reach out and to obtain this evidence directly from companies.

Now, this has to be done within the right statutory and rights-respecting framework. Countries that can meet internationally established due process, privacy, and human rights standards should have the right to come directly to the Googles of the world, and that may lead to more requests from us, and the production of more user data for people that are abroad. But as I mentioned before, we are sort of on the trajectory where we're going to have this clash of conflicts of laws. And when companies like Google are in other countries, and we're operating there, and we have establishments there, and countries have legitimate arguments that they can exercise jurisdiction over us, the ability of companies in the long term to be able to withstand these demands I think is going to diminish.

So we have an opportunity now, I think, to lift up standards, privacy standards, in other countries. In some ways, it's an exchange. If they lift up their privacy standards, they will be able to do something they can't do right now, which is to issue legal requests to companies like Google, Microsoft, Facebook, Yahoo, and others, and obtain user data, but it has to be done within the right framework. And there's a discussion now that's commenced in the United States; the Department of Justice in July released legislation, unveiled legislation, that would enable other governments to issue orders to Google and other types of companies, and we would be able to produce that data under an exception to the Voluntary Disclosure provisions of the Electronic Communications Privacy Act. I think there's going to be quite a bit of discussion around that. There already is.

There are very legitimate concerns that have been raised about whether this can be the privacy and due process-protecting regime that it ought to be. And I think we're having those conversations right now with civil society groups, with the US government, and with other governments that are interested in this particular type of scheme. So, I am going to stop there. I am happy to answer a lot of questions; I'm sure many of you have them, and hopefully we'll delve into some other issues, too.

HILLARY GREENE: Fantastic. Thank you so much for the presentation, David. Now we're going to turn to Felix. David's discussion underscored how, particularly in today's information economy, big business means global business. And as it turns out, one thing that varies across countries are preferences with regard to privacy. And so Felix is

going to help us to understand a number of things, including how differences in privacy values manifest across the globe, including with regard to the US and in the EU. He is also going to help us really dive down and reconsider what exactly privacy means from the inimitable perspective of the computer scientist that he is. Privacy is an abstract value, and we need to understand what it means in terms of the underlying data, or more specifically, data sets. And with that introduction, Felix, please.

FELIX WU: Great. Thanks, Hillary. So, I'm going to talk about two things which on their face may not seem entirely related, but which I'm going to try to connect together. So, the first is trying to think about the question of what counts as personal information or personally identifiable information, a question which has great legal significance because oftentimes the coverage of laws, regulations, or even just practices depends upon defining what class of things this law, regulation, or practice is going to apply to. But it's generally defined in terms of some notion of personal or personally identifiable information.

So, I'm going to start with thinking a little bit about this question. This is a question I wrote about a few years back, in a paper called "Defining Privacy and Utility in Data Sets," and so I'm going to talk a little bit about some of the conclusions that I draw in that paper. But then where I want to go with it is to try to use that as a lens through which to think about the contrast between primarily European and American privacy. We've heard a couple of times here about the differing privacy standards in different jurisdictions. Here is a place in particular where, while David was describing previously about this idea of trying to lift up privacy standards in other countries, I think the Europeans have the same notion of us, which is to say that they have the notion that they want to try to lift up the privacy standards in the United States.

In any event, I want to try to use this question of what counts as personal information as a lens through which to think about this contrast between American and European approaches. Okay, so first, what do I mean by trying to think about what counts as personal information? So, on its face it would seem as if maybe this question is obvious. I mean, those of you in the know I think probably know this is not obvious, but if you're just thinking about this for the first time it may seem like, well, some things obviously are personal data and some things obviously are not, right?

But let me throw out a few hypotheticals and see what you think of them. So, imagine for example, I mean, this obviously exists, but imagine for example the database of all of the videos viewed on YouTube, okay? But, here's the thing—and I don't mean to pick on YouTube in particular, but here's the thing: imagine the database stripped of user names, stripped of user names, stripped of all things you might think of as identifiers of any sort, even stripped of IP addresses, anything of the like, right? And so, all

you know is that person 42651 viewed this list of videos on these days, in this particular order, or whatever, right? And that's all you've got. Is that a database of personal information, or not? Okay, so that's one thought.

Think about a database of medical records. Again, I strip out all demographic information, all identifying information, but all I know is that person 42651 visited the doctor on such and such a day, complaining of such and such a symptom, was prescribed such and such a drug, returned for a follow visit a week later, had this result, and the like. Again, but no identifying information, even demographic information. I don't otherwise know anything about this person, other than this is their history of medical encounters in the world.

Finally, imagine—this goes back to sort of the metadata conversation—imagine a metadata database in which you actually removed all the phone numbers themselves. All you know is that person X calls person Y and person Z; person Z calls person A and person B. And you don't know anything about who these people are. They're just points, like points in a massive graph of connections here. Is that a database of personal information? Okay? And in each one of these cases they've stripped out lots and lots of information that we'd normally think of personal, but I think in each one of these cases there's still the possibility for stuff to be done with the data that's left, right, some of which might be actually quite useful, but some of which might have the potential to be more privacy-invading.

And part of what computer scientists have been able to show over the last several years is you can kind of do more with this data than it might seem at first glance. So, for example, my example of the YouTube videos, right? It may turn out, for example, that all you need to know is just a little but about some of the videos that somebody viewed, particularly if you happen to know about when they viewed them, let's say, right? Such that, if you then had access to this massive database, you could pick out their record in among all of these records.

Now notice, you had to start with some information in order to make this possible. If you literally know nothing about someone, you probably won't be able to do much with this database, okay? But if you know a little bit about someone, maybe you can actually pick out their information, right? So, for example, in the medical database, I could almost surely pick out my own medical history in the database. But of course it's my own medical history; what's the big deal, right? I already know my own medical history. But I can probably also pick out family members; I can probably pick out friends and the like. And that might make a difference, right? It might make you think differently about what some of the possibilities are with a database of that sort.

Okay, so, the results that have been generated from computer science and the like have led legal scholars and regulators to be of two minds in

thinking about, then, what should count as personal information or not? So, some scholars have taken these kinds of results to suggest that therefore pretty much everything is personal information. There's almost situation in which these kinds of things are not personal, because pretty much all the time you can describe one of these attacks on the data, as you might say, a way of using the data to then find out something about someone, okay? Other scholars have argued exactly the opposite, which is to say, none of this stuff really should be considered personal information, and none of it's really personal because the kinds of attacks that I'm describing are purely hypothetical things, the chances of which are so slim that we should just not worry about them at all.

So, what I want to suggest is that in that debate, part of what's being hidden is essential questions about what should count as a privacy violation in the first place, and that ultimately your view on what counts as personal information is very much dependent upon your view of what counts as a privacy violation, right? So, is it a privacy violation if I end up being able to find out a little bit of medical information about a friend that that friend didn't otherwise tell me? Or, is it only a privacy violation if a random hacker could do the same thing, right? Is it a privacy violation if an insurance company can adjust rates based upon this data?

Now, they may not still necessarily know, literally know, much about any one individual, right. They may not in fact be able to identify people who are sick, or something along those lines. But maybe they adjust the rates according to the database. Is that a privacy violation? Is it a privacy violation, for example, for someone to be served ads that depend upon their YouTube video viewing habits, right, even without the person serving the ads actually being able to know anything more about this person than in fact that they viewed this sequence of videos on YouTube?

Your answers to each one of those questions, then, will often determine whether or not you regard the underlying data set as actually personal information or not. And so debates over what counts as personal information are often hiding more fundamental debates about what it is we mean to protect when we say we're trying to protect privacy. And so, the notion that we can just kind of look out on the world and say, "Yes, here's personal information. No, this part is not personal information," that notion is really kind of hiding the ball in some ways. We really have to be more cognizant of thinking about the way in which that question about what counts as personal information fundamentally implicates a question about what kind of things we need to protect through privacy. So, that's first on personal information. What does this have to do with Europe and the US?

One way of thinking about what's characterizing the more European approach to privacy, as compared to an American one, is one in which the European approach is much more based around a notion of rights, right? This notion that privacy is a fundamental human right, and that therefore

we kind of don't ask why, at least not at the individual level. We don't ask why this particular person gets to protect this particular bit of information about them, right? We just say, "Well, it's a fundamental human right." And we can give all sorts of why answers about why it's a fundamental human right generally, but we don't ask it in the specific, right, we just say that, because it's a fundamental right, that's the reason it should get protected.

And I think that's very much contrasted with an American approach in which we tend to ask why, right. And we say, "Look, well, maybe if the answer is because it's medical data, then we'll protect it." Or, "Maybe because it's going to lead to identity theft, then we're going to protect it." And so that's the potential, the origin, of having all of these sectoral laws that say we protect medical data, we protect financial data, but we don't just necessarily protect data, full stop. Okay?

But, here's the thing. The European approach really only works if, in fact, the notion of what counts as your data is fully definable, and in fact that's part of how these European laws are crafted. They apply to personal data, but not necessarily to non-personal data, and the thing about it is that then when you go to try to figure out what things count as personal data, you're going to have to have some notion, still, of what kinds of things count as privacy violations, or not, in order to be able to properly define what counts as personal data or not. And when you take that approach, you can't just say, "Well, okay, anything that violates someone's rights is a privacy violation," because the very question is trying to figure out whether or not this is the data over which you have rights in the first place, or not, and so it would be circular to try to do that.

So, what I want to suggest is that under a more rights-based approach, even under that approach, there needs to be some conceptions of what things count as privacy violations and what things don't, and that maybe this provides some opportunity for conversions, or at least dialogue, between these two contrasting approaches, right? That maybe through the lens of personal information, we can start to have more of a conversation about both what kinds of things are the kinds of things that European law and European citizens mean to protect, and things American law and American citizens mean to protect. And as the potential to provide a source of convergence in thinking about how, even though you start from very different places, you might potentially end up at least somewhere closer together, or understand better where your differences lie, which might provide some attempts to begin to ameliorate some of the differences that I think David was describing, and that some of the other panelists in previous panels have described, about some of these global differences in privacy protection. Thanks.

HILLARY GREENE: Fantastic. Thank you so much, Felix. And now we are going to turn to James who is going to introduce what seems to be a

foreign concept of a different kind. We're not talking about the EU or a foreign land; what we're talking about is economic thinking. And the question is, to what extent can we use economics to understand preferences with regard to privacy, and perhaps even to help design a system that best reflects those preferences? And it seems that the incorporation of economic thinking would have particular relevance in this context, because we, of course, are working from the baseline assumption that some of the biggest data aggregators in the world are businesses working with economic incentives, and so much of the data exchange is taken within the context of the marketplace. Take it away, James.

JAMES COOPER: Well, thanks, Hillary. I want to thank the Law Review for inviting me. It's an honor to be part of such a great program, and you guys have been fantastic in setting this all up. Most of today has been devoted to this government limits on government collection of data, and I'm going to talk about now is how government limits the current regulatory program as far as limiting private entities' ability to collect and use data. As Felix just alluded to and I think others have talked about in the program earlier, the US has no central privacy law or regulation. There's HIPPA, there's FERPA. HIPPA's for healthcare, FERPA for educational records. COPPA for children, FCRA for financial data or data brokers—not data brokers, sorry, not data brokers. That's controversial.

But what that leaves is the Federal Trade Commission [FTC], for the most part, as the primary enforcer in this area. Beginning in the late 1990s, as e-commerce and the internet was burgeoning, there was a vacuum because of the lack of an overarching regulatory framework for privacy and data security. There was a vacuum, and they have this broad mandate to prohibit unfair and deceptive acts and practices,. They saw a regulatory vacuum and kind of jumped into it. This was, again, back in—first action was 1998, I believe, before an iPhone, before Facebook, before mobile apps.

So, at this point it was kind of a—and I was at the FTC soon thereafter—it's a fairly marginal part of the FTC's regulatory authority at that time. However, not surprisingly, as data has grown, as we hear all about—we have lovely symposiums like this. I participate in lots of them, it's a huge deal now. Data is a huge part of the economy. It's part and parcel of our modern economy. So, the regulatory footprint that the FTC's privacy program leaves on the economy has grown exponentially.

But what I want to talk about today in brief time is that unfortunately I think that as the importance of the FTC's regulatory endeavors here has grown, or at least the footprint it leaves on the economy has grown, the rigor of its analytic framework for this has not grown in a commensurate way. It's stuck back in the 1990s. To paraphrase what a friend of mine said with respect to the FCC's decision to adopt Net Neutrality, it's a economics-free zone, when they think about privacy right now, primarily

based on workshop reports and consent degrees, but for a regulatory endeavor that has such a huge footprint, it can and it should do better.

So, let me give just a couple examples of what I'm talking about. A couple of years ago, Facebook bought WhatsApp. WhatsApp is a—I've never used it; I should have asked my thirteen-year-old daughter how it works. I'm sure she knows a lot better than I do, but Facebook bought it, because it's popular with thirteen-year-old girls, I guess, and others. And, what I want to contrast is the way this was handled on the privacy side and the antitrust side. And, full disclosure, I began my life as an industrial organizations-trained economist, and an antitrust lawyer in private practice and at the FTC. So I come at this with a really heavy focus on competition; I'm kind of biased for antitrust. I think antitrust is a fantastic area of law, so that's my disclosure here.

But, so you have this merger. The FTC looks at this merger through the competition lens, and they analyze it under something that's called the horizontal merger guidelines, which is this—recently revived in 2010, but it's this framework that's a really robust framework, informed by industrial organization economics, to determine whether a combination of assets is likely to harm competition, which in turn is likely to harm consumers. Is it going to raise prices, reduce output, reduce innovation, reduce quality, those sort of things. And a very, again, a rigorous framework, and you take real data, and you run it through that framework, and you come up with an answer. Is this something that we're concerned about, or not concerned about?

Well, from the antitrust side this wasn't anything that they were really concerned about. It was cleared, no problem, again, through rigorous framework. But on the same day that the FTC gives their closing letter to the parties, saying, "Our investigation is done. We're not going to issue a second request. We're not going to go after this merger," the head of the Division of Privacy at the FTC sent a letter to Facebook and WhatsApp, saying, "Oh, well, you cleared the antitrust hurdle, but if you want to combine WhatsApp and Facebook's data, you're going to need express affirmative consent to do that." Okay, where did that come from?

Now, I'm not going to make a judgment whether that's right or wrong, but my point here is the analytic framework. Where does that come from? Well, you dig a little deep through the history of that—it comes from two consent decrees that were signed a year earlier, one by David's employer, another by Facebook, where they agreed to something called Fencing-In Relief. And I'm sorry to get into the weeds here, but when you sign a consent decree with the government, with the FTC, and I'm sure with other regulatory agencies it works the same way, one of the things you do is agree not to do the bad stuff you were doing.

But another thing that is often put into these orders is called Fencing-In Relief, to say, not only do you agree not to do the stuff that we allege

violated the law, but you're going to agree to not do some other stuff going forward, and that stuff doesn't violate the law; it's just sort of prophylactic. You were a bad actor before; we're worried you may be a bad actor in the future, so we're going to kind of fence you in. That's where the term comes from, Fencing-In Relief.

So, these are things that aren't required by the Federal Trade Commission Act. Nonetheless, they're in consent decrees, but this consent decree now becomes the basis for preventing the merger of the data between Facebook and WhatsApp, which is just as important, if not more important than the physical merger of the two. I mean, that's a big deal. And again, I'm not going to make a judgment whether that's right or wrong, but it's the framework, which is a zero. There is no framework. It's kind of taken out of whole cloth. Like, oh, express opt-in consent seems like the right thing. Let's put that there.

Not only was it for that merger; a year later it shows up on the FTC's Bureau of Consumer Protection website, in a blog posting from an FTC staffer, saying, "Oh, by the way, advice for merging parties in the future. If you're going to merge and you have data sets, you're going to need express opt-in consent from all of your users in order to merge data." Okay. Again, where did that come from? Same sort of citations underlie that. It's a blog posting. I mean, query whether it's entitled to chevron deference. I doubt it. But the point is, you violate that stuff at your peril. I know there are people out here who counsel clients, and as you counsel clients you read the tea leaves in the FTC and you say, you think really hard, even though this is a blog posting, but you think really hard about what it says.

So, here's another example, privacy by design, which is a mainstay, has become a mainstay of the FTC's privacy area, and one thing, kind of the background of this—in the privacy area, there are no litigated cases. They're all consent. Not, data security we've got one litigated case, Wyndham, and LabMD is coming through the 11th Circuit now. But I'm just talking about privacy here. There are no litigated cases, so this is all consent agreements. And apart from consent agreements, the primary thing is a couple of reports that they've released that already have become de facto guidelines.

And one of the mainstays that is in these reports that shows up in speeches, and in the bully pulpit that the FTC uses, this notion of privacy by design. It's this notion that privacy needs to be thought of at every stage of the design process. If you're making an app, if you're making a piece of software, if you're making a piece of hardware, you've got to think about privacy. And they've used this theory in enforcement actions, one against HTC, and one now against D-Link, which is just filed in California. Again, I don't want to make a judgment whether this is right or wrong, but privacy by design necessarily implies that there is some tradeoff there, right?

So, the FTC is saying that you need to make privacy baked in as sort of

the primary thing at every stage of your product. Why not speed by design? Why not convenience by design? Why not all of these other things by design, to the extent that you trade off privacy and other values at the design stage? I've talked to general counsels from large tech firms, and to a one they've all told me that they have conversations with engineers, and engineers tell them they can do X with this app. And they say, "Well, you shouldn't do X with this app. It would work better, but you can't because we're worried about privacy issues."

So, the thing is that the FTC is making this tradeoff, saying companies have to make this tradeoff at the design stage. Again, I won't judge =whether that's the right or wrong tradeoff, and whether the FTC needs to mediate that tradeoff, or whether the market can, nonetheless, what's the analytic framework from which this tradeoff came? There is none, okay. It's a workshop report, which is essentially, look, three of four of us are smart up here. But this is kind of what it is, like, two or three workshops with smart people, and then you get the transcripts and staff go through it, and you write it down. Read those reports and look for a cite to any economic articles, look for data. Zero, okay? No data, no economic articles. It is a workshop report. Is that how you regulate the tech sector, and tell them how they should design things?

So, the question here is, where do we go? And I alluded to antitrust before, but antitrust wasn't always such a coherent exercise, either. Back in the '60s up until, really, the early 70s, antitrust was probably a similarly incoherent body of law. It was used to go after large firms just because they're large. It was used to go after pricing, because, hey, if you come into a market and you offer low prices, and you drive the small business out, that's bad for the small business, even if it's good for consumers. That would be an antitrust violation. There were cases like that.

As industrial organizations economics was coming into its own, as pioneers like Richard Posner, and Robert Bork, and George Stigler, these ideas started to seep into antitrust, and along with a few Supreme Court cases in the late '70s and early '80s, antitrust embraced this notion of a consumer welfare standard that was going to be guided by economics. And we were off to the races, and what we were left with now is this very consumer-focused analytic framework that has enjoyed wide bipartisan support since that time. That's one of the beautiful things about antitrust is that from administration to administration—there are little marginal arguments. What else are law professors going to argue about at conferences? But for the most part, there's huge support for the bulk of it.

So, my thought here is that privacy is now ripe for a similar revolution. It's time to grow up so its analytic framework is just as complex and sophisticated as the footprint that it leaves on the economy. So, here's a couple of things to map out. First, and I think most importantly, and it fits into some of the stuff that Felix was saying, I think, need to identify harm.

Harm is the key here. You need to identify it more precisely. Number one, not only is harm the legal touchstone for the FTC to act. Unfairness requires by law substantial consumer injury; deception requires material deception. Materiality is something that kind of tricks consumers into doing something they otherwise wouldn't.

So, you've got harm, you've got some kind of consumer harm at the base of that. And, from a policy standpoint, harm's important, because if you're going after practices that don't cause harm, you're unnecessarily deterring beneficial practices. Okay? So, harm should be a necessary condition to acting, and I think the FTC needs to be a little more precise in identifying what sort of harm it is. It's not there in the privacy reports. So I think that they need to look at revealed preference rather than stated preference. Revealed preference is what do consumers do in the real world? Stated preference is a survey: "Am I worried about my data? Yes." And all a stated preference tells you is that something has value. A revealed preference tells you that the tradeoffs of things have value. How much am I willing to trade off one thing of value for another thing of value?

[Wrapping up,] there are a couple of other things that we'll get into in our little Q and A, but I think focusing on harms, focusing on the empirical lit that's out there, and training the FTC's very formidable research capabilities to this task. I would say I've said some bad things. I think the good news is, is also the institution in charge of this is the FTC. I was at the FTC for eight years and I'm a huge FTC cheerleader. It was designed with economics and policy in mind 100 years ago. That's what it was for. It developed as this institution that would research and create norms in competition and consumer protection policy. Back in the '80s, the FTC revolutionized advertising law based on economics. And I think it's up for the task, it can do it again. So, I'll leave it at that.

HILLARY GREENE: Thank you so much. Continuing with the marketplace metaphor, we have been talking about legal markets. When you have a legal market you also have what are called the so-called black markets. And what Professor Ghappour is going to discuss is the equivalent of a black market within the context of this symposium. We're going to consider one way in which individuals can evade government surveillance, and that's through the so-called dark web. And not surprisingly, he's going to be looking at what the government has, can, or should do in response to activity on the dark web.

AHMED GHAPPOUR: Good afternoon, everyone. Thanks so much, Hillary, for the introduction, and thank you to the conference organizers and my co-panelists as well. My name is Ahmed Ghappour, and I'm not supposed to be making this appearance on Skype. Unfortunately, and due to a set of circumstances that are far too complex even for a conference about encryption, I missed my red eye last night. But thanks to the marvels

of modern technology, we were able to bridge the gap and I am actually sitting in my car now for a wholly separate but related set of complex circumstances. [Laughter]

Modern technology enables us to conduct transactions across the globe. It allows us to scale and automate those transactions in ways that reaps benefits. Today I'm going to be talking about the other face of technology. Using the dark web and anonymity tools as an example, I will address the use of technology to plan and execute wrongful acts, and the hurdles that certain technologies present to the administration of criminal justice and national security. I'm also going to be talking about the regulatory response by governments, whether that is through the development of new investigative methods and policy, or just policy, using as an example the new surveillance method that allows investigators to hack computers on the dark web in order to conduct searches and seizures.

The dark web itself, for our purposes, is a private network of computers that use a cryptographic protocol to communicate in such a way that users can conduct transactions anonymously, without revealing any trace of their location. Civil liberties advocates promote the use of the dark web to maintain free speech, privacy, anonymity. They point to the fact that the organization that makes the leading software used to get on the dark web is, for the most part, funded by the U.S. government. For example, anonymity tools can be used to circumvent certain types of government censorship. They can be used to allow users to access online destinations that would otherwise be blocked by certain authoritarian regimes.

Not surprisingly, criminals and other malicious actors have flocked to the dark web for its promise of an anonymous and secure platform for conversation, coordination, and at times, action. Modern criminals use the dark web to carry out technologically driven crimes, such as computer hacking, identity theft, credit card fraud, IP theft, and so on. Platforms like the Silk Road, an online underground marketplace, provide a means for existing brick-and-mortar criminals to actually globalize and digitize their operations with virtual impunity.

According to the Department of Justice, the use of anonymity tools makes it impossible for investigators to use conventional surveillance methods in the pursuit of criminal suspects. For example, in computer crime cases, the most important piece of evidence is the device that was used to commit the crime. Until that computer is located and searched, investigators lack an evidentiary link, a critical evidentiary link, between a crime that was largely committed in virtual space and the person who committed it.

Anonymity tools are not at all the first technological change that has leapfrogged law enforcement surveillance capabilities. In fact, this happens so much that the FBI has termed the phenomenon "going dark," and aptly

so. In the 1990s, for example, law enforcement lost its ability to wiretap calls when telephone companies switched from copper cables to digital telephony. The result was, amongst other things, the passage of the Communications Assistance for Law Enforcement Act of 1994 [CALEA]. That, in turn, required telephone carriers to install standardized equipment so they could assist police with electronic wiretaps.

The government's go-to solution when it comes to the "going dark" problem has been through the regulation of third parties, and specifically communications providers with centralized routing facilities from which communications data could be intercepted. However, problems arise when third-party assistance is not technologically feasible, as is the case with certain anonymity tools. This could be because the technology's architecture is decentralized, its code is open source, or its core functionality requirements would be undermined if monitoring capabilities were to be mandated. The functional effect of these characteristics is that governments that promulgate regulatory schemes for compelled assistance will have difficulty implementing and enforcing them.

Law enforcement's response has been to roll out an investigatory technique that uses computer hacking to directly conduct remote searches and seizures of computers whose location is unknown, by using the internet to deliver malware to target computers. On December 31st 2016, an amendment to the Federal Rules of Criminal Procedure came into effect that allows courts to issue hacking warrants for computers whose location is unknown, addressing the Constitutional implications of this new surveillance technique on a case by case basis. But consider this important wrinkle. The clear majority of dark web users are outside of the United States, and since every computer's location is theoretically indistinguishable from the next, any law enforcement target pursued on the dark web may well be located overseas.

The overseas hacking operations that result from network investigative techniques are a significant change in the way in which the United States engages in cross-border law enforcement investigations. Conventional evidence collection methods have historically fallen in line with international law, where it is considered an incursion of sovereignty for one state to carry out law enforcement functions in another state, without that state's consent. Indeed, while the United States regularly enacts statutes that criminalize conduct that occurs totally overseas, we rarely, if ever, deploy law enforcement agents or their equipment into another country without first obtaining consent. Department of Justice guidelines go as far as directing agents not to make phone calls that target individuals overseas for fear of violating the sovereignty of other states. Hacking is a sea change from conventional law enforcement practice: The exercise of extraterritorial law enforcement functions will be unilateral. They will not be limited to matters of national security, nor will they be coordinated with

any agency that has an expertise in foreign relations or national security.

In a recent paper, I argue that these circumstances highlight the failures of the existing rules of criminal procedure, as applied to the new facts of cross-border network investigative techniques, and call into question the wisdom of authorizing rank-and-file officials and investigators to make enforcement decisions that may reverberate globally, without any meaningful interagency coordination or interbranch checks and balances. Instead, criminal procedure must evolve to balance the use of network investigative techniques against the countervailing foreign relations and national security interests that may result from these overseas searches.This may require adjustments to the criminal legal process that aim to minimize the risk of political fallout by maintaining the existing jurisdictional norms embedded in the way we conduct cross-border criminal investigations, and a number of structural modifications that resolve the existing institutional conflict between, on the one hand, the practice of law enforcement, and on the other, critical foreign relations and national security policies. On that note, I'm going to hand it over to Hillary.

HILLARY GREENE: Thank you so much for joining us and taking us for a brief foray into the dark web. For our discussion, we're also going to be joined on the dais by our very own czar. Mr. Arthur House [Connecticut's first "cyber-czar"], if you would please join us. I want to actually open up the floor to the audience to be able to ask questions and invite panelists to sort of supplement the comments that they made at the outset, and also to feel free to comment on some of the statements that others have made.

FELIX WU: Yeah, so, I just want to say a couple of things in response to James' presentation. So, the first is that I worry a little bit about using antitrust as a model for thinking about privacy regulation, in part because I think it's clear in the antitrust world that the ultimate harm we're looking at is economic harm, and I worry that porting that model over to privacy means that we primarily recognize only economic forms of privacy harm, rather than privacy harms more generally.

The second thing that I would worry about is trying to connect the idea that I was describing about defining what things count as privacy violations to this standard of trying to identify harms, because again, sometimes harms in this context ends up being interpreted very narrowly. I don't know whether that was your intention, your personal intention or not, but just in the conversation at large, it tends to be interpreted quite narrowly, and so therefore tends to exclude things like surveillance as a harm, independent of anything that happens to you as a result of that surveillance, for example, something that I think quite plausibly can be understood as a privacy violation, even if it doesn't necessarily lead to anything that you could directly identify as a harm.

And the last thing I'll say is that looking primarily to revealed preferences rather than stated preferences assumes that the notion of privacy should be fully encapsulated within individual preferences generally, right? And, I would argue that there are important social values to be protected through privacy that can't be defined simply by looking at personal individual preferences, and that instead need to be understood and defined from a broader social perspective, the same way we identify lots of other social goods, and social—things that we desire from society that we don't simply poll people to identify.

JAMES COOPER: Yeah, thanks, Felix. I would say I'm not talking at all about just narrowly economic harms. And I think when you think about the types of endeavors the FTC's involved in, the data security stuff's easy, right? When you've got a data breach, and you lose, and there's ID theft, and credit card. I mean, that's easy. But that's not what I'm limiting it to. I think your idea of surveillance, that can be a harm, I certainly do. I think what I would like to see more of, and what I'm arguing is that there are a lot of studies that try to get at willingness to pay for privacy, mostly, almost exclusively in the experimental economics realm. There are a lot of them.

One of the things that comes out of that is almost to a study, they all suggest that we're willing to pay very little for privacy? That comes out of pretty much all these studies which give rise to this idea of what's called the privacy paradox, that we have stated preference where people say we really, really care about privacy, then we have revealed preference both in the real world, where we have a billion Facebook users, and half the US people have Amazon Prime, and we live our lives online with the data exhaust that we've heard about all day. And then we have these studies that show that—for instance, one comes to mind where I'm willing to pay $5 for a phone that doesn't track me versus another one. That's not a huge amount. Or, a recent study came out in the Journal of Legal Studies, actually this month, by Lior Strahilevitz and Matthew Kugler, Chicago and Northwestern, and they find that with Gmail users, that the median, or, I should say the modal amount people—first of all, they get this group of people who are Gmail users, and they say, "Okay, let's go through in detail. We're attorneys. Let's go through in detail and tell you the privacy policy." And they all agree that, oh, wow, that they're scanning my emails to serve me ads? That kind of creeps me out, it's been stated.

FELIX WU: So, I don't doubt that willingness to pay might be relatively low, but I might say that if you were to determine willingness to pay for freedom of speech, that might be low, too, and that wouldn't necessarily provide any less reason to protect it.

JAMES COOPER: Well, first, I don't know, but that assumes a base notion, which I think goes to your, we have freedom of speech. And I don't know. And I'm not saying we don't protect privacy or privacy's valuable.

What's important is the tradeoffs, at least here in the commercial realm.

HILLARY GREENE: I am going to give the other folks on the podium a chance if they want to jump into that, but I also really want to turn to the folks in the audience. So let us start getting some hands going.

RIANA PFEFFERKORN:[1] This is a topical question, and maybe it's a little too fresh for anybody to have a response to yet, but we have a very fragile agreement in place with the EU regarding the transfer of EU persons' data into the United States, and how US companies are supposed to abide by EU standards for privacy protection. However, earlier this week the president signed an executive order requiring federal agencies to clarify in their privacy policies, to the extent consistent with applicable law, that non-US citizens and non-lawful permanent residents are excluded from the protections of the federal privacy act. And there's been some talk that this might be the thing that completely topples the fragile new US-EU privacy shield. And I was wondering if the panelists, and specifically David, who's probably been getting some heartburn over this recently, what your thoughts are on that, and whether there's any way to try and salvage the replacement that we now have from the previous way that we were trying to handle EU-US data flows, which is worth billions of dollars.

HILLARY GREENE: Thank you, Professor Pfefferkorn.

DAVID LIEBER: Yeah, so, I'll just say candidly, I thought the Executive Order, Section 14 in particular, as it applies to privacy rights sends an unfortunate signal to the European Commission about this administration's posture vis à vis the privacy rights of non-US persons. I will say, though, that I do think that what they were saying in that context, as I read it, is separate and distinct from the assurances that the US government has given to the European Commission, and distinct from the rights that were extended to non-US persons, or at least the process to extend those rights to non-US persons, under a law called the Judicial Redress Act, which was signed into law last year.

The executive order talks about effectively stripping away, or ensuring, I should say, ensuring that the Privacy Act does not extend to US persons, consistent with applicable law. And applicable law includes, in my view, the Judicial Redress Act. In the waning days of the Obama administration, the Justice Department designated, I think, 26 countries and the entire European Union as jurisdictions that should receive those additional privacy protections that have been afforded by the Judicial Redress Act. And the Judicial Redress Act was one of the mechanisms, the legal mechanisms, I think, that gave some comfort to the Europeans, that we had a surveillance regime and a privacy-respecting regime that was narrowly tailored, rule-bound, transparent, subject to oversight, and had redress

[1] Cryptography Fellow, Stanford Center for Internet and Society.

mechanisms, most importantly.

So, I think it's created, I think, an unfortunate storm and fire drill, but I think people recognize at least thus far that the intent is not to extend this to the rights that were created under the Judicial Redress Act. No doubt, I think that there's going to be a bigger discussion about some of the other policies that were implemented by the previous administration, including a presidential policy directive, PPD 28, which was a historic policy shift for the US in extending specific rights to non-US persons in the way—in the conduct of signals intelligence collection abroad. Those debates are sure to come, but certainly [laughs] even in the last 24 hours has created quite a firestorm.

RICHARD BORDEN:[2] I have a question about cybersecurity regulation. Those of you who know me are going to laugh. Art described how we're at the brink of disaster, and he's right about this. New York, the Department of Financial Services, has just, it's still proposed for a few more days, a financial services cybersecurity regulation. It's coming out at the state level, similar to what's happened with privacy laws in much of the country. So, my question is two-fold. One, is it good for us to have cybersecurity regulation, and if so, is the way that we're starting to do this the right way, or should we be thinking about it a different way?

ARHTUR HOUSE:[3] Thank you Counselor Borden. Well, because we're just starting all of this, we obviously don't know. I have a preference. I like Connecticut's approach better than New York's approach. Let me offer two things. When we looked at the very serious threat posed to critical infrastructure, I was chairman of the Public Utilities Regulatory Authority. We sat down and we talked to the utilities. Now, admittedly, we were the regulators, and we could go the regulatory route, and we said, "Let's talk about this. Can we agree mutually on a system that will start the dialogue, enable us to understand what's going on?" Why did we do that?

First of all, in this state, the governor was no longer willing to respond to a question, what's the state of cybersecurity with our regulators, by responding, "I don't know." Legislators were no longer willing to tell their constituents, "I don't know." So they said to us, the regulators, "Do something." We sat down with the utilities and said, "Can we work out a system by which we are able to have some sense of progress that you are making in cybersecurity on an annual basis, with agreed participants, according to agreed standards?" And we did. To me, that's an awful lot better. When you throw up a regulation, everybody has good attorneys.

---

[2] Counsel, Robinson & Cole, LLP, Hartford, Conn. Attorney Borden moderated another symposium panel, titled "Surveilling the Future."

[3] • Dr. Arthur House is Connecticut's Chief Cybersecurity Risk Officer. Dr. House gave a keynote earlier in the symposium and was asked to join the Q&A section of this panel.

You can find a way around it. You can weaken it; you can do all sorts of things with it. I would rather have a meeting of the minds, and a mutual effort to come up with a new system. And I hope that lasts.

Looking down the road, after we've learned a little bit about this, I would not be surprised, let's put it this way, if where we're headed in a period of time, five years, ten years, I don't know what it is, that because cybersecurity is so essential to the wellbeing of the citizens of the state, that we'll have a system whereby there would be a cybersecurity audit, the same way there's a financial audit. Now, we don't know today—none of us can take apart the finances of United Technologies, or Aetna, or Webster Bank, or any other institution, but they have auditors. And the auditors are trusted, and the auditors go through and they use Generally Accepted Accounting Practices, and they issue a letter. We rely on that letter to know, are the finances of this corporation solid or not? I could see us at some point in the future having cybersecurity firms. Some of those financial auditors today do cyber audits.

And it may well be that we're coming down to a system whereby a corporation company can pick its own cyber auditor. There will be agreed things that the auditors will examine, and they will issue a letter. "According to these eight major criteria, these are the scores we give to this company." Therefore, we as the public will be able to know, how are they doing? And of course, when there are weak areas, there will be remedial actions. So, that's a long way of saying, I would rather meet, first of all, to see if you can agree on a review system, and secondly I think inevitably where we're heading is that there are to be third party audits to answer the questions that you've posed, Counselor.

AUDIENCE MEMBER 3: My question involves a technical point, and a policy point. The assignment of names, transfer from the United States to an international body, I'm not myself happy with, and I see a great potential for mischief, in sometimes big ways, of being able to redirect traffic by letting the public see the name that they know—who knows, maybe even Google—and actually going someplace else that maybe looks like Google, and allows access to the user's computer, access to malicious information, etcetera. So, number one, is this a legitimate concern? Could that kind of thing happen, from our technical experts? And number two, what kinds of regulations and policy should we have to address that?

DAVID LIEBER: So, you know, right. So this is maybe getting beyond maybe my sort of knowledge. It might have been referring to what's affectionately referred to as the IANA transition. I mean, I can't speak too intelligently to this, but this is basically transfer of management oversight responsibilities from the US Department of Commerce to another body. This is something that has created quite a bit of consternation, but I mean, it just happened and I'm not sure that we've seen any of the ill

effects that I think some people thought that they'd see. In a lot of ways, I think we've heard over the years concerns about the US oversight and management of the internet, as if it's our sort of—as if it belongs to us. And I haven't seen any manifestations since the transition that would, I think, lend credence to some of the, for lack of a better phrase, parade of horribles that we heard about it before, so.

FELIX WU: And I guess maybe the one thing I'll say on this is that there are certainly ways of hacking the domain name system generally. I'm not sure any of them are made any easier in the transition. In other words, there are hacks that can happen whether the authority is in the United States or not. Now, I suppose if ultimately the concern is that the central authority itself gets corrupted, or that somehow you could somehow leverage that as an attack point, then I suppose that would be the potential concern there. I think the overall sense is that the chance of that is sufficiently low that it's not necessarily the primary vector that folks have been thinking about.

ARTHUR HOUSE: I have little to say on the legal side of this. I would just say, knowing the capabilities, there is cause for alarm. When I was in the intelligence community, if we needed to know something about a person of suspicion of a foreign country, we could very quickly look at every email he or she had sent over the past 20 years within a matter of days. The ability to penetrate thoroughly an individual's background is astounding. And so I concur with my colleagues on the panel who have said there need to be protections against that happening here in the United States.

HILLARY GREENE: Well, that was interesting. I've never seen someone so, at least temporarily, stump the panel. [Laughter] So, bravo. And I'm curious, do we have any last question from a student? Any of our students want to chime in? All of your questions are answered? It's quiet. Yes, Gavin [Tisdale].

GAVIN TISDALE:[4] So, just to reiterate a question from before. If you each had one bit of advice you would give the incoming administration, one thing to say, what would it be?

DAVID LIEBER: Well, I'll go, thematically, with one of the points I think I was trying to underscore. Maybe I did it implicitly rather than explicitly, but that there are implications for our surveillance policy that span well beyond national security. The question from Professor Pfefferkorn, I think, illustrates that, that when you have policies that are intended presumably to shore up national security, they can have unintended consequences when they're not necessarily thought through. The executive order's a perfect example, but you can look at this in a lot of

[4] Editor-in-Chief, *Connecticut Law Review*.

different ways. I suppose if you're the current administration, the protection of privacy rights for a non-US person can be a means to an end. The absence of protections for non-US privacy persons means that things like the Privacy Shield, which is the legal mechanism under which US companies transfer the personal data of citizens of the United States, that will be suspended, really annulled. And if that's the world that we want to march toward, then we can put to the side the rights of other people, and in particular their privacy rights. That's not a wise policy, in my view. It will have unintended consequences that will be adverse for economic growth in the US. So putting it in those terms I would say that's something I think the administration should keep in mind.

JAMES COOPER: I'll be brief. I think that, again, the only advice anyone would ask me for would have anything to do with maybe the FTC, not some of the bigger picture questions. But I'd say, try to focus on things that we think are likely harmful to consumers. And by harm, I'm not limiting it to economic harm. There's dignity harms, and autonomy harms—privacy's a huge area. But try to keep the focus on harm, and have a little regulatory humility.

FELIX WU: I'm thinking mine's exactly the opposite, [laughter] which isn't necessarily to say that we actually substantively disagree that far, but—

JAMES COOPER: Would it be regulatory hubris? [Laughter]

FELIX WU: No, no. But, more perhaps disagree about where the default position might lie with this administration, and which direction they might need to be pushed. And so, I guess my advice would be that, at a basic level, privacy is worth protecting, and it's worth protecting even when it's difficult to see the immediate benefits of protecting privacy. And I think that that would be my piece of advice.

ARTHUR HOUSE: I was on the Obama transition team for the intelligence community, so we had to answer these questions. I have three. One is, do not torture. It is illegal. It does not produce results, and it destroys the morale and the humanity of those people you are asking to commit the torture. Secondly, protect Americans' rights. The whole reason you're there is to defend the way Americans live, our laws, our culture. And third, for heaven's sakes, work with the intelligence community. There are 50,000 of them. They're like first responders. They're like the military; they will give their lives for this country. Don't demonize them. You're going to need them. Trust them, work with them. I guess those would be my three points.

HILLARY GREENE: So, thank you all so much for joining us today. [Applause]