The John Marshall Law School
Center for Intellectual Property, Information & Privacy Law

62nd Annual Intellectual Property Conference
Current Developments in Intellectual Property, Information Technology & Privacy Law

Friday, November 2, 2018

Concurrent Sessions I
Session C: IT & Privacy

***Moderator*:**
Charisse Castagnoli
Vice President, Security, General Counsel,
Tucker Path Inc.

Panelists:

Ian Ballon
Shareholder, Co-Chair,
Global Intellectual Property &
Technology Practice Group,
Greenberg Traurig LLP

Robert Newman
Partner, Co-Chair, Privacy, Security &
Data Innovations Practice Group,
Loeb & Loeb LLP

Gareth Dickson
Partner, WIPO UDRP Panelist,
Taylor Vinters

David Poell
Associate, Sheppard, Mullin,
Richter & Hampton LLP

Jim Lai
Cyber Risk Manager, KPMG

Thomas Smedinghoff
Of Counsel, Locke Lord LLP

* * *

MS. CASTAGNOLI: Thank you all for coming to the non-patent part of this conference. We're going to stray into the area of IT and privacy. We've got a fantastic group of people on our panel.

First, we have Ian Ballon from Greenberg Traurig. He is going to be updating us on the Telephone Consumer Protection Act (TCPA).

Next to him is Rob Newman. Rob has all sorts of interesting fun facts for us. He's like an important dude and you can look up his bio online. But, most

importantly, his firm is a sponsor of this conference, so thank you very much to Loeb and Loeb.

Gareth Dickson came all the way across the pond. He is a Partner at Taylor Vinters. You might want to say a few words about your firm because these are mostly U.S. people here, so they probably don't know much about it.

MR. DICKSON: My firm is Taylor Vinters. It is headquartered in the United Kingdom and has three offices: one in Cambridge, one in London, and a third one in Singapore.

The firm traditionally was a regional law firm, but over the course of the last ten years, management has seen technology and innovation and entrepreneurship as something that really inspires the people who come to work for us and as the future of law, so the firm has pivoted away from those more traditional sorts of work and now focuses on innovation and entrepreneurship.

Our objective is to be a leading law firm for innovators and entrepreneurs operating globally, so we like to partner up with the right law firm in any particular territory rather than having a specific network that we are obliged to use for any given scenario.

Today I am going to talk a little bit about some of the European aspects of IT & Privacy.

MS. CASTAGNOLI: And I'm going to throw you a zinger.

MR. DICKSON: Brilliant! Let's hope I'm last.

MS. CASTAGNOLI: For those of you who aren't familiar with the area of IT and the law, Tom Smedinghoff is absolutely one of the founders of bringing this to the forefront of the American Bar Association. In fact, he started the ABA Identity Management Legal Task Force. He still runs an old-school listserve, which is my go-to every time I want to know something that's edgy about identity in the law. I highly recommend that you get onto that if you're not. Tom will be happy to sign you up, or you can sign up on the ABA website

David Poell, from Sheppard, Mullin, Richter & Hampton, is stepping in for Lisa Thomas.

Jim Lai is Cyber Risk Manager at KPMG.

We have a few prepared remarks and topics, but this will definitely be an interactive session. Our goal is to introduce you to areas of IT, data privacy, and risk management.

How many people are in-house?

[Show of hands]

Excellent. You're going to love this.

How many people are with a law firm?

[Show of hands]

How many people are just curious?

[Show of hands]

Even better.

If you were at this panel last year, I can say that everything is now completely different. Since last year we've had the EU General Data Protection Regu-

lation (GDPR)[1] go live on May 25th, and apparently the only thing the media knows about it is how to calculate 4 percent of global revenue — not very helpful.

We have had a number of really interesting shifts in policy in the United States, with net neutrality and changes in how the Federal Communications Commission (FCC) approaches data privacy issues.[2]

And of course, the gift that keeps on giving, the data breach *de jour*.[3] I tried to do a really quick add-up of the number of records that have been breached in the last three months, any major breach that's over 10 million records, and I gave up counting when I got up to about 892 million. If you've flown Cathay Pacific in the last nine years, they just graciously dumped your passports into the Dark Web.

I am a technologist by trade. I love data privacy. They don't let me talk about it anymore because I mostly just tell people what to do and don't do any real work.

Let me give you my three privacy and security assessments (PSAs), which I'll try to keep short and sweet.

Number 1: If you don't know, the only good thing to come out of the Equifax breach is Congress did pass a law,[4] and credit breaches are now —

AUDIENCE: Free.

MS. CASTAGNOLI: The second PSA comes to you by way of Director Wray from the Federal Bureau of Investigation. Who knows what a Business Email Compromise (BEC)[5] is?

[Show of hands]

Who has an Interest on Lawyer Trust Account (IOLTA)?[6]

---

[1] Regulation (EU) 2016/679, General Data Protection Regulation (GDPR), O.J. L 119 (4 May 2016); cor. O.J. L 127 (23 May 2018): Regulates the processing by an individual, a company or an organization of personal data of all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas. The Regulation went into effect on May 25, 018.

[2] United States Federal Commc'ns Comm'n, Open Internet Order, Report and Order on Remand, Declaratory Ruling, and Order, Adopted Feb. 26, 2015 ("Net Neutrality"). In December 2017 the FCC voted to repeal regulations on net neutrality, full text available at https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-166A1.pdf. The FCC's Restoring Internet Freedom Order (Jan. 4, 2018), which took effect on June 11, 2018, provides "a framework for protecting an open Internet while paving the way for better, faster and cheaper Internet access for consumers." *See also*, United States Federal Communications Commission › General Data Protection Regulation (GDPR).

[3] *See* Breach Level Index: Data Breach Statistics by Year, Industry.

[4] S.2179, Data Security and Breach Notification Act, 115th Congress (2017–2018).

[5] A business email compromise (BEC) is an exploit in which the attacker gains access to a corporate email account and spoofs the owner's identity to defraud the company, its employees, customers, or partners of money.

[6] Attorneys continue to fall victim to sophisticated scams targeting their IOLTA accounts. Although there are multiple variations, the scam typically begins with an email from a potential overseas client who requests representation in a commercial collection matter against a local debtor. The client executes a retainer agreement and returns it by email. Almost immediately after the retainer is signed, the client reports that a settlement has been reached independently with the debtor and that the client has informed the debtor to mail the settlement proceeds via bank or cashier's check to the attorney. The client advises the attorney to deposit the debtor's check when it is received, then to wire the net proceeds to the client after deducting the attorney's fee. The

[Show of hands]

Oh, you guys are lucky.

Who has a chief financial officer?

[Show of hands]

Something else you need to keep track of: $6 billion so far this year in ACH wire fraud.[7] If you don't know about it, if you do get a call from a client or from somebody internal, if they catch it quick enough, there is technically — not well-known— a three-day kill chain even on a wire. So if you catch it quickly, what's the first thing you do?

AUDIENCE: Kill it within three days.

MS. CASTAGNOLI: Call the Fraud Department of the initiating bank. They're your best hope to try to get it stopped.

Finally, from by favorite security blogger, Brian Krebs, "Krebs on Security" — how many of you have children?

[Show of hands]

Do you think that they might have installed the Bank SMS app from their bank allowing them to use their phone as an ATM card? If they have, you need to immediately educate them that the bank will never send you a Short Message Service (SMS) message, the bank will never send you an email, and the bank will never call you asking you for your account information. Just around the corner from here, $60,000 was extracted from seventeen accounts through SMS texts where they took control by reassigning the mobile device to the digital wallet associated with their bank. As we all know, debit transactions are not treated the same way as credit card transactions. I hope those people get their money back.

Those are my PSAs.

Now let's talk about the law.

Does everyone know what the Telephone Consumer Protection Act (TCPA) is? It's the only useful data privacy statute we have in the United States because it actually has statutory damages.

The TCPA has seen an incredible amount of uptake in class action lawsuits.[8] In fact, one recent article I read said it's the second-most-popular cause of action in class action lawsuits. I don't know what they are comparing it to, but that was a fun fact.

And we happen to have an expert with us on TCPA. So, Ian, bring us up to speed.

MR. BALLON: Thank you.

I actually don't think TCPA is a very good statute. Because it allows statutory damages, it is being used for a great deal of frivolous litigation. The statute

---

check is deposited into the attorney's IOLTA account, and then the net proceeds minus the attorney's fee are wired to the client's account overseas. When the attorney's bank presents the debtor's check for payment from the issuing bank, the check is returned because it is a forgery.

[7] Association for Financial Professionals (AFP), 2018 Payments Fraud and Controls Report.

[8] Consumer Action, Class Action Database. *See also* U.S. Chamber of Commerce, Institute for Legal Reform, TCPA Litigation Sprawl A Study of the Sources and Targets of Recent TCPA Lawsuits (2017).

prohibits certain calls and texts. It has generated approximately 5000 new lawsuits a year. So it is generating a great deal of litigation.

I am an intellectual property litigator by training. Back when Al Gore created the Internet, much of my practice moved to Internet litigation. [Laughter] Although I still do a lot of copyright, trademark, right of publicity, and other kinds of IP litigation, about half my practice these days is defending data privacy and security breach class action suits, including TCPA class actions.

There is currently a split in the circuits on the issue of what constitutes an automatic telephone dialing system (ATDS) and there is a tremendous amount of litigation.[9]

It is a risky time for companies to engage in text marketing. There are a number of risks, including litigation over vicarious liability. Many of the companies that I have successfully defended in litigation hired a marketing firm that engaged in text marketing; or they are franchisors sued because of the alleged misconduct of a franchisee.

MS. CASTAGNOLI: Can you indemnify yourself against this in your contract with your marketing firm?

MR. BALLON: Oh yes, sure, you absolutely can, but indemnification is only as good as what it's worth.

MS. CASTAGNOLI: And those markets are all out there.

MR. BALLON: A problem in this area is that too many companies simply hand over to plaintiff's counsel a bag of money to settle these cases quickly because of the risk of statutory damages. When they start looking at damages of $500 to $1500 per text multiplied by large numbers of messages sent, the risk of exposure may seem overwhelming. However, companies that are quick to settle suits that can be won may end up being sued again. And companies that overpay to settle cases raise plaintiffs' counsel's expectations and contribute to the flood of litigation.

Sending text messages, *per se*, is not illegal. However, if an ATDS is used to send a text message or a call to a mobile phone number, consent (or for marketing messages express written signed consent) must be obtained. In fact, however, many calls and texts do not involve use of an ATDS.

The statute defines an ATDS as "equipment which has the capacity (a) to store or produce telephone numbers to be called, using a random or sequential

---

[9] *Compare* Dominguez v. Yahoo, Inc., 894 F.3d 116, 121 (3d Cir. 2018) (holding that, after *ACA*, the "key" question under the TCPA is whether the equipment "had the present capacity to function as an autodialer by generating random or sequential telephone numbers and dialing those numbers"), *with* Marks v. Crunch San Diego, LLC, 904 F.3d 1041, 2018 WL 4495553, at *7–9 (9th Cir. 2018) (agreeing that after *ACA* "only the statutory definition of ATDS as set forth by Congress in 1991 remains ...," but disagreeing with the Third Circuit that number generation is required by the plain terms of the statute, holding instead that the definition of an ATDS is ambiguous, and, based on Congress's failure to amend the TCPA to account for FCC regulations subsequently struck down in *ACA* as arbitrary and capricious, construing the statute to define an ATDS to include even equipment that merely has the capacity to dial from a list of stored numbers).

number generator; and (b) to dial such numbers."[10] The Third Circuit, in a case that I won, held that the plain terms of the statute require number generation.[11]

Since I have just referenced a case of mine, I should also give my usual disclaimer: Nothing I say represents the views of my law firm or my clients ... or indeed even myself, and should never be cited back to me in a brief, please. Anything I say is offered for the abstract purpose of furthering CLE at this great law school. [Laughter] With that disclaimer, let me continue.

The Third Circuit, quite correctly, held that the language "to store or produce telephone numbers to be called, using a random or sequential number generator" means that the statute applies when the technology generates numbers either randomly or sequentially.

The intent, if you look at the legislative history back in 1991, before text messages even existed, when Congress enacted the statute was to prevent calls to blocks of numbers, either sequential numbers (001, 002, 003) or randomly generated numbers, because those included numbers that were unlisted or were emergency numbers.[12] For those of you who are Millennials, an unlisted number meant it didn't exist in a phone book, which was something that existed in homes and phone booths. [Laughter] Congress was concerned about unwanted calls to emergency numbers and unlisted phone numbers.

In *Marks v. Crunch*[13] — a case where I represented the party that lost but should have won — the Ninth Circuit concluded that the statute was ambiguous and that what it means "to store or produce telephone numbers to be called, using a random or sequential number generator" is ambiguous.

This was a surprising conclusion because years earlier the Ninth Circuit had held that the definition of an ATDS was "plain and unambiguous,"[14] and a subsequent appellate panel is bound to apply earlier precedent. To get around the earlier holding, the Ninth Circuit in *Marks* explained that the earlier panel meant only that one word in that statute – *capacity* — was unambiguous and that the remaining part of the definition was unclear.

After concluding that the statutory term was ambiguous, the Ninth Circuit then looked at the legislative history — but not the legislative history from 1991, when the statute was enacted. The panel looked at a narrow amendment in 2015, at the time that the FCC had just issued expansive regulations that were subject to challenge but had not yet been invalidated, and concluded that Congress approved of FCC Regulations that arguably allowed for dialing from a list.[15] The panel then proceeded to essentially rewrite the statutory language to require *either* dialing

---

[10] 47 U.S.C. § 227(a)(1).

[11] Dominguez v. Yahoo!, Inc., 894 F.3d 116 (3d Cir. 2018).

[12] See *1991 Senate Committee Report*; (October 1991); *Congressional Record - Senate* (Nov. 7, 1991); *1991 House Committee on Energy and Commerce Report* (Nov. 15, 1991); *Congressional Record - House* (Nov. 26, 1991); Congressional Record - Senate (Nov. 27, 1991).

[13] Marks v. Crunch San Diego, LLC, 904 F.3d 1041, 2018 WL 4495553 (9th Cir. 2018).

[14] Satterfield v. Simon & Schuster, Inc., 569 F.3d 946, 951, 953 (9th Cir. 2009).

[15] *See* Federal Commc'ns Comm'n, FCC Actions on Robocalls, Telemarketing; FCC releases omnibus Declaratory Ruling and Order concerning several requests for clarification of the Commission's TCPA rules; FCC Adopted Rules and Regulations Implementing the Telephone Consumer Protection Act of 1991 as amended by the Bipartisan Budget Act of 2015, Report and Order.

from storage or dialing from numbers generated randomly or sequentially, which would broadly make every one of the more than 300 million smartphones currently in use in the United States an ATDS because every smartphone has the *capacity* to dial from a list of stored numbers, such as an address book.

The Ninth Circuit's premise that Congress approved of dialing from a list by not reversing the FCC's 2015 Regulations when it made a very narrow technical amendment to the statute is itself flawed. The Third Circuit, for example, had construed the FCC's 2015 Regulations as not expanding the statutory definition of an ATDS and requiring number generation.[16] While those challenging the 2015 Regulations in litigation argued that the FCC had sought to expand the statutory definition of an ATDS, given the Third Circuit's 2015 construction of those regulations it is not reasonable to infer that Congress necessarily understood and approved of an expanded definition of an ATDS — beyond the scope of the statutory definition — by failing to modify the definition of an ATDS when it enacted a narrow amendment to the statute relating to collection calls.

The D.C. Circuit ultimately invalidated those portions of the 2015 Order that addressed the definition of an ATDS as arbitrary and capricious — and this ruling is binding on all circuits.[17] In light of this ruling, the only thing that remains is the plain terms of the statute.

But the Ninth Circuit effectively revived a broad interpretation of those invalidated regulations in *Marks.* The panel did so by misapplying rules of statutory construction and English grammar. In *Marks* the panel read § 227(a)(1) "to provide that the term automatic telephone dialing system means equipment which has the capacity — (1) to store numbers to be called or (2) to produce numbers to be called, using a random or sequential number generator —and to dial such numbers."[18] But, under the TCPA, the phrase "using a random or sequential number generator" must be read as modifying ***either*** "store" ***or*** "produce" in the preceding phrase. "A dependent clause that precedes a main clause should be followed by a comma."[19] Thus, the phrase "to store or to produce numbers to be called" must be read as dependent on the main clause, "using a random or sequential number generator ... ." In other words, the main clause — "using a random or sequential number generator" — modifies either term in the dependent clause, "to store or produce telephone numbers to be called ... ." Any argument to the contrary reads the provision as though there were a comma after "store" before "or produce," where there is none.[20]

That is a preview of some of the arguments we will make in support of our petition for cert. within the next ninety days.

---

[16] *See* Dominguez v. Yahoo!, Inc., 629 F. App'x 369, 373 n.2 (3d Cir. 2015) (rejecting the argument "that the FCC [in its 2015 regulations] has interpreted the autodialer definition to read out the 'random or sequential number generator' requirement ... .").

[17] *See* ACA Int'l v. Federal Commc'ns Comm'n, 885 F.3d 687 (D.C. Cir. 2018).

[18] *Marks v. Crunch*, 904 F.3d 1041, 2018 WL 4495553, at *9.

[19] THE CHICAGO MANUAL OF STYLE § 6.30 (16th ed. 2010).

[20] As the Ninth Circuit had pointed out in an earlier case, "both we and our sister courts have recognized the punctuation canon, under which a qualifying phrase is supposed to apply to all antecedents instead of only to the immediately preceding one where the phrase is separated from the antecedents by a comma." Yang v. Majestic Blue Fisheries, LLC, 876 F.3d 996, 1000 (9th Cir. 2017).

At the moment it's a risky time to engage in text marketing.

MS. CASTAGNOLI: But don't you feel like databases now are much bigger than they were in 1991? I could generate a database of every single phone number, and then I'm not generating it, I'm just looking it up.

MR. BALLON: Well, that's an issue for Congress, isn't it? It is up to Congress to amend a statute, not the courts. In *Marks* the Ninth Circuit acknowledged that it was construing the statute differently than as written.

The FCC has asked for comments on the definition of an ATDS both in light of the D.C. Circuit's ruling in *ACA*[21] and the Ninth Circuit's ruling in *Marks*.[22] The FCC may clean this up. If not, we hope the Supreme Court will.

MS. CASTAGNOLI: So, if you're passionate about this, write to the FCC.

The Peer-to-Peer (P2P) Alliance submitted a Petition for Clarification to the FCC with regard to whether the sending of SMS texts[23] is going to be rolled in under the TCPA as well, even though right now it is a human individual send.

Anybody else on the panel have any experience with this or want to add something?

MR. POELL: Yes. I do a lot of TCPA class actions as well.

Just to build on what Ian said, this is an area of law that always seems to be very much in flux. It would be nice if the Supreme Court would go out on a limb and take this case and try to provide some clarity. I don't think they have weighed in on the TCPA since the *Mims* case in 2012,[24] which was basically a decision on a jurisdictional issue.

On the human intervention issue, what you have to do to actually be an ATBS, I don't think that the Ninth Circuit's opinion ultimately will provide that much clarity. It is going to be really a piecemeal situation where a motion to dismiss on ATBS grounds will probably almost always be denied. The case will go forward and, hopefully, the FCC or the Supreme Court can provide some additional guidance to help us wade through these cases, because right now, in my opinion, it couldn't be more unclear.

MR. NEWMAN: The only other thing I would add is if you are an in-house counsel counseling your client on this, ask what the return on investment is of your plan to market using text messages.

MS. CASTAGNOLI: Dude, why do you think they're doing it? It's huge.

MR. NEWMAN: I am not sure that it is. You could do the same thing with an email, and there's basically no regulation with significant teeth of that. No one spends a lot of time worrying about CAN-SPAM these days because CAN-SPAM

---

[21] ACA Int'l et al. v. Federal Commc'ns Comm'n, No. 15-1211 (D.D.C. Mar. 16, 2018).

[22] Federal Commc'ns Comm'n, Public Notice, Consumer and Governmental Affairs Bureau Seeks Comment on Interpretation of the Telephone Consumer Protection Act in Light of the D.C. Circuit's ACA International Decision, DA/FCC #: DA-18-493, Docket/RM: 02-278, 18-152 (May 14, 2018); Public Notice, Consumer and Governmental Affairs Bureau Seeks Further Comment on TCPA in Light of the Ninth Circuits Mark v. Crunch San Diego, LLC Decision, DA/FCC #: DA-18-1014, Docket/ RM: 02-278, 18-152 (Oct. 3, 2018).

[23] Federal Commc'ns Comm'n, Consumer and Governmental Affairs Bureau Docket No. 02-278, Public Notice seeking comment on the Petition for Clarification filed by the Peer-to-Peer Alliance ("P2P Alliance") (May 23, 2018).

[24] Mims v. Arrow Fin. Servs. LLC, 565 U.S. 368, 370 (2012).

has no private right of action.[25] If you could do the same thing by email or by the push notification in a mobile app, why take the risk on the TCPA?

MS. CASTAGNOLI: Yes, push notification in the mobile app, I will agree with you, probably has the same success rate. Marketing colleagues have told me the reason that they're doing SMS marketing is because it works.

MR. NEWMAN: I don't know if it works to the tune of $10 million in damages.

MS. CASTAGNOLI: Yes?

AUDIENCE [Prof. Dennis Crouch, University of Missouri School of Law; Patently-O Blog]. I think we've seen a huge increase in telephonic robocalls. Do those fit into this same statute?

MS. CASTAGNOLI: That's what it was written for.

MR. BALLON: Yes. In fact, there's a certain president in this country who has been sending text messages to random Florida area codes. I live in California, but my wife has a 305 area code.

MS. CASTAGNOLI: And area code 954, too.

AUDIENCE [Prof. Crouch]: Yes, but I'm talking about voice calls.

MR. BALLON: The TCPA addresses, among other things, calls to mobile numbers. If you use a landline phone, you are essentially free to call anyone you want (other than numbers on the National Do-Not-Call database).

MS. CASTAGNOLI: Because it used to cost money. Now the cost of an incremental minute is pretty close to zero, and you used to be able to impose costs on the person receiving a call — and in some jurisdictions you still can, right?

MR. SMEDINGHOFF: All I can say is, judging by the number of calls I get, I don't think this statute is working. [Laughter]

MS. CASTAGNOLI: Okay. So we've got two for more and we've got everybody else for less.

I want to turn to a technology topic that I will ask Tom to lead us through, which is the whole notion of identity. I'm putting all our GDPR participants on hold until after we talk about identity. Identity is embedded and ingrained in our personality, but we treat identity in the United States very differently than it is treated in the European Union.

You may not know this, but you have multiple identities. You have a Facebook identity that is not the username and password you use. It is a digital conglomeration, what Facebook has accumulated about you in order to identify you with a cohort.

The ABA, and I think the bar in general, has struggled with the notions of identity and identity proofing. The Supreme Court has said it's okay to take a DNA swab of you even if you've only been arrested,[26] and now that is in a federal database — or a state database, even worse, because it's going to get hacked — and we have seen reversing of cases where DNA was voluntarily given out by relatives.

---

[25] The Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003 (CAN-SPAM), 15 U.S.C. ch. 103, 117 Stat. 2699 (Dec. 16, 2003), established national standards for the sending of commercial e-mail and requires the Federal Trade Commission to enforce its provisions.

[26] Maryland v. King, 569 U.S. 435 (2013).

This is an area where we should really understand what the emerging thoughts are in the jurisprudence and understand how that might impact everything from contract formation, to litigation, and eventually to our privacy rights.

MR. SMEDINGHOFF: Let me start off with a slightly different concept and try to bring this all together.

Think about anything you do on the Internet — whether it's entering into a contract, sending somebody an email or some sort of message, accessing a website or a database, or whatever — in all of those we need to consider the "question of trust" with respect to that whole transaction. Trust has a couple of elements:

(1) First, do you trust the party you're dealing with? If I'm buying something from Amazon, do I trust that Amazon is going to actually deliver it? Identity is not going to help you with that aspect of trust, *per se*. Either it is a reputable company or it is not.

(2) The second element I call "trusting the transaction." That boils down to identifying with whom you are dealing, and do you trust that the identification of that person or entity is accurate?

We have all dealt with phishing emails. Perhaps you fall for it, you think it's really your bank or you think it's really eBay or whoever's logo they put on the phishing email, so you click on it. The sender has falsely represented his identity, but you rely on that false identity and log in using your own identity credentials — i.e., your username and your password. Of course, once the bad guys get that, that's their key to get into your account to do all kinds of fun things.

The bottom line is identity is a critical foundational issue with respect to everything we do on the Internet. We don't worry about identity in many of the transactions we do — we buy things from Amazon and we log into Facebook and we think everything's fine — but, as the significance and the value of those transactions increase, it is going to be really important to know who is at the other end. Your bank needs to know it's really you before they let you transfer money out of your account, and you need to know it's your bank before you log in and give away your password. So there is a potentially significant identity component.

As the significance of transactions increases — think about the order to launch the nuclear missiles — you want to know that it is the president who is giving the order and not a hacker.

MR. BALLON: Well, maybe not under the present circumstances. [Laughter]

MR. SMEDINGHOFF: Yes. Well, maybe not the best example.

But the bottom line is that identity is key to everything, and so we struggle with what is identity and how are we going to verify it, and so forth and so on.

Is there anybody in this room named Tom other than me?

[Show of hands]

We have one. All right. I was going to say if I'm the only one, then "Tom" would be a perfect identity for me in the sphere of this room. We have two, so we need an additional attribute to distinguish us within this community. But that's all we need. We don't need an address, a Social Security number, we don't need a lot of detail, because within this group we could easily determine which of the two Toms we are talking about and that would distinguish us from everybody else.

But as the group gets bigger — maybe it's Facebook, maybe it's Google, maybe it's Amazon, maybe it's the whole country — we need more attributes to make an identity unique. Attributes are information elements about you. It could be your address, it could be your name, it could be your Social Security number, it could be your hair color, it could be your biometric information, and I can go on and on and on.

The attributes that you need as part of your identity, of course, depend on the situation in which you are using the so-called identity. To establish that identity in an online transaction we have to do two things.

Take a live body, anybody who you've never met before. Somebody has to figure out who that person is in a manner appropriate for the context. If they are looking for Social Security benefits, they have to know what their name is and what their Social Security number is. If they are looking to buy something on Amazon, maybe they need to know their Amazon account information, or whatever it is. But they need to know information about somebody.

That's typically called "identity proofing." We go through this when we get a driver's license and we go through this when we get a passport.

MS. CASTAGNOLI: When you get a new a job.

MR. SMEDINGHOFF: Yes, exactly. That's a huge element.

So we have to go through an identity-proofing process to get an identity credential. That credential could be a driver's license or a passport in the paper world. In the online world it could be a username, or it could be a digital certificate using encryption and all kinds of complex technologies.

MS. CASTAGNOLI: Don't talk about that.

MR. SMEDINGHOFF: I won't.

But the bottom line is you go through an identity-proofing process and you get a credential.

Then, when you go somewhere to do something — you want to log into the nuclear power plant database, you want to log into Amazon, you want to log into Facebook, whatever you want to do — they have two questions: "Who are you?" and "How can you prove it?"

When you go to Facebook, they ask "Who are you?" You give them your username, "I'm Tom Smedinghoff." They say, "Well, that's great. We'll let you into his account if you can prove that you're Tom Smedinghoff because we know enough about him to know that he goes with a particular account and we're willing to let him in." Or my bank will say, "We know enough about Smedinghoff that we'll let him transfer funds." But how do they know that I'm the guy who has previously been identified as "Smedinghoff?" That's the key element. That's the authentication part of it.

MS. CASTAGNOLI: And that's where we're in big trouble.

MR. SMEDINGHOFF: That's where we're in big trouble.

MS. CASTAGNOLI: Now I'm going to start throwing in the fun facts.

MR. SMEDINGHOFF: All right.

MS. CASTAGNOLI: This is important, right? What we do innately as human beings, but we drop on the floor when we're dealing with a computer, is we make risk decisions all the time.

How many of you share a password across multiple websites? I know everybody does. Even I do, but only in low-risk accounts.

[Show of hands]

What we don't know is that part of this identity-proving problem that Tom is talking about has become too easy to be taken over. Our baseline identity-proofing right now on the Internet is still username and password. So we've got to go to something else.

So biometrics has emerged. Illinois is now a hotbed of biometric lawsuits. Two states, Illinois and Texas, have biometric identity protection laws. I guess the Illinois one is really exciting. I don't know what happened, because the law has been around since 2008, but the amount of litigation has gone through the roof.

MR. NEWMAN: Illinois is the only state with a private right of action.

MS. CASTAGNOLI: Ah, there we go!

MR. SMEDINGHOFF: That's the reason, right.

MR. NEWMAN: Washington and Texas both have laws, but neither state has a private right of action. So all the action is here.

MS. CASTAGNOLI: Okay, so all the action is here in Illinois. There are a substantial number of cases now, mostly around consent to use biometric identification associated with timecards.

So is this good or bad?

MR. SMEDINGHOFF: Timecards are a great example because when you are working in a factory you pick up your timecard, you punch in, you punch out, and that's how you get paid.

MS. CASTAGNOLI: It's all on computer now, Tom.

MR. SMEDINGHOFF: But the point is you could have somebody do it for you, right?

MS. CASTAGNOLI: Right.

MR. SMEDINGHOFF: We want to get around that to ensure that you only get paid for the time you worked. So companies are going to biometrics, and in some situations (depending on how they implement it) that runs afoul of the Illinois biometrics law. But it is an attempt to come up with additional information to identify you, so the authentication process will absolutely verify that it is you and it can't be spoofed.

MS. CASTAGNOLI: Is there a question?

AUDIENCE [Steven Fallon, Greer, Burns & Crain]: There are a couple of solutions that I am aware of. One is two-factor authentication, having something with you, whether it's an RSA SecurID token or something like that. Another solution is there are some experiments going on with blockchain, obviously within a closed user group, where once the consumers agree to opt into it and their identity is verified, they are able to go to multiple sites because they are now trusted. And then you've got the biometrics, like what is done in India, where there are two different biometrics.

I know we've got the situation with passwords, but if the end goal is to ensure these trusted IDs are something that can't be readily hacked, what do you see the solution being? Is it something that I mentioned, or do you see something else coming down the line?

MR. SMEDINGHOFF: Frankly, I'm not sure what I see as the solution, and I'm not sure that biometrics by itself, or even blockchain, is necessarily the solution.

One example which is neither of those is Facebook Connect. Has anybody logged into a website using your Facebook ID?

MS. CASTAGNOLI: Don't do that.

MR. SMEDINGHOFF: Well, Facebook had a big data breach a while ago and I believe 50 million of those IDs were compromised. So now, if I'm the bad guy, I can log into all these other websites as you because I have your Facebook ID. Not a good situation.

MS. CASTAGNOLI: We know how to fix that.

MR. SMEDINGHOFF: Well, maybe we do. But the point is that's one of the concerns.

MS. CASTAGNOLI: Yes, but it has always been the tradeoff between security and convenience.

What we are also seeing now if you do online banking in many other places — not the United States, but it has become popular in in London with HSBC — is Jumio facial recognition. In fact, the ACLU recently sent a Freedom of Information Act request to the Department of Homeland Security on facial recognition.[27] In addition, Amazon has its own facial recognition program.

MS. CASTAGNOLI: How many people here feel like it's a good idea for Amazon to be able to facially recognize you?

[Show of hands]

MR. SMEDINGHOFF: It might be more secure, but it also raises privacy issues. So that's the tradeoff here.

MS. CASTAGNOLI: That's the point.

MR. SMEDINGHOFF: As we do identity we are collecting data about you, different elements — it might be biometrics, facial recognition, fingerprints; it might be a password; it could be all kinds of things — we are collecting data about you and then exchanging that data with the entities you are logging into, your bank or whomever, and we are able to track where you go and what you do because you are leaving a trail every time you use it.

MS. CASTAGNOLI: And remember that when we talk about GDPR.

AUDIENCE [Gary Friedlander, TransLincoln LLC]: Your face is exposed to all this right now. If I take a picture of you, I could do facial recognition using any number of software programs.

MR. SMEDINGHOFF: Yes.

AUDIENCE [Mr. Friedlander]: It's your public face.

MS. CASTAGNOLI: Not in the European Union.

MR. SMEDINGHOFF: So do I not have any privacy rights in my facial image — I mean my name is public too and my address is public?

---

[27] American Civil Liberties Union, ACLU FOIA Request to DHS on Facial Recognition (Oct. 24, 2018); *see also* Jay Stanley, Senior Policy Analyst, ACLU Speech, Privacy, and Technology Project, *How the TSA's Facial Recognition Plan Will Go Far Beyond the Airport* (Oct. 23, 2018).

AUDIENCE [Mr. Friedlander]: The right to privacy is like photography in public. We have never had a right to privacy in public. Your face is probably your most public attribute.

MS. CASTAGNOLI: Remember that as we transition into the GDPR.

Who does not know what the GDPR is?

[Show of hands]

The General Data Protection Regulation is founded on the principle that you have fundamental human rights in the European Union, unlike in the United States, that you have personality associated with your personal data, whether it's expressly private or not private, and any information that may be used to uniquely identify you. There are obvious things like your DNA. There are not-so-obvious things like your IP address. The core fundamental is that you are the owner of that and you need to grant consent to most people to use it, more or less, as opposed to in the United States, where you don't own anything about yourself and if it's readily available it can be bought, sold, or traded.

And try getting your bank not to send your transaction data to Yodlee. Good luck! They say, "Oh, it's anonymous." Yeah, it's immediately reidentified over at Acxiom in exactly two clicks.

That's very fundamental. There's this dichotomy in the background between how personal data is considered in the European Union versus in the United States.

Now we're going to go into the unintended consequences of the GDPR, which is going to be so fun.

MR. DICKSON: Before I start, can I go back to what we were just talking about, facial recognition? On the way over here on Wednesday, I had a client call about the same time that I was supposed to be boarding. I had to get my boarding pass from the check-in desk because they wouldn't let me check in online, which is a sure sign that you're going to be subjected to get extra searches.

MS. CASTAGNOLI: Randomly of course.

MR. DICKSON: Completely randomly.

So I have my boarding pass, and I walked up to the X-ray machine, there was nobody else there, but — ding, ding, ding — I've got to go for separate processing. Okay, kind of predictable.

I get to the gate. I am on the phone with my client. Boarding hasn't started, but my name is being called because I'm going to be subjected to additional searches. But I'm on the phone call, so I'm hanging around and I'm waiting, and I'm away from the crowd, and nobody is bothering me, and I finish the call.

I turn around when the call finishes and there's a guy standing there. He said, "Mr. Dickson." There was nothing about me that would have given him any indication as to who I was other than my face.

MS. CASTAGNOLI: Except your face.

MR. DICKSON: Right. So it looks like they had been able to track me walking through the airport.

Now, you can either be reassured by that or you can be terrified by it. You are probably on most occasions pretty indifferent. But that is just a really practical example of what we were talking about that I experienced on my trip here.

MR. SMEDINGHOFF: The airlines actually have an identity management project where they are trying to track you all the way through the airport.

MR. DICKSON: Yes.

MS. CASTAGNOLI: China does that already. They have been doing that since the 1990s.

MR. DICKSON: Yes. It's the premise of the TV show *Person of Interest*.

MS. CASTAGNOLI: They used to do it with physical photographs and humans. Now they do it with technology.

MR. DICKSON: Anyway, back to unintended consequences, I am going to use an example from the online world, from the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN manages the domain name system. It converts IP addresses into domain names and makes it easier for us all to navigate the Web. ICANN has a system of contractual relationships with *registries* of .com, .us, .net, and so on, and also with *registrars* who are consumer-facing and who liaise with consumers in order to allow them to register a domain name.

One of those contractual obligations is the requirement to collect personal information about domain name registrants. The registrars will get technical information and administrative information, but also registrant information so that the registrar can contact them. This has existed since pretty much the beginning of the domain name system, in the form of the WHOIS service. It is there for security and stability purposes. It is there for law enforcement, rights protection, and rights clearance as well. But it has always been unpopular with privacy advocates.

As time has gone on, we've seen how the publication of this data can be used for spamming. Your personal information is collected and entered into WHOIS and then it's published online. Anybody can access it, including through automated processes. So you open yourself up to spam. You open yourself up potentially to stalking. The justification is that this information is necessary for, amongst other things, tracking down bad actors. But, if you are a bad actor, you are never going to put your real information into the WHOIS anyway. So people can game the system. Query how much it actually meets the purposes for which it was designed.

And then the GDPR comes along, and the advocates for privacy jump on the GDPR and say, "You are only allowed to process personal data in certain limited respects. It has to be for a legitimate purpose and it can't be for anything more than is necessary. It has to be lawful and justified and not disproportionate. But there is no purpose served by *publishing* this information online. As long as somebody is keeping that information safe, and as long as those with a legitimate interest can access it, then that's fine; that should meet all of your needs. You don't need to publish it as well."

Under the GDPR there is a large maximum fine if you are found to have unlawfully processed personal data: you can be subjected to a fine of 4 percent of your global turnover or a fine of €20 million, whichever is higher. So, if you are approaching that line where maybe you can do something or maybe not, you will naturally look at the consequences of your options. What's the benefit and what's the risk? Where is your return on making that decision? If there is minimal benefit

to it but you could get hit with a €20 million fine, you are probably not going to do it.

ICANN's response to the advent of the GDPR was to implement a Temporary Specification that said, "You no longer need to *publish* any of this WHOIS information."[28] That was against the cries of rights owners who said, "We rely on this information in order to detect counterfeiting, to detect cybersquatting, all the sorts of infringements that protect brand owners." So they are at one end of the scale. But there are also people who are victims of fraud because somebody registers a bank name with a small misspelling or an internationalized domain name and then sends out emails.

MS. CASTAGNOLI: Yes, and then someone buys a Mack truck online. That actually happened last week.

MR. DICKSON: You maybe don't even have to have a website. You could just be sending emails to people.

MS. CASTAGNOLI: They reported they were redirected to the legitimate website. They just have the cybersquatting domain name, and they literally used that to leverage an identity and buy a $250,000 tractor trailer. It was actually wire fraud.

MR. DICKSON: So one unintended consequence of the GDPR is that by ICANN telling registrars that they no longer need to publish WHOIS information, it has become much harder to protect consumers from fraud and for rights holders to enforce their rights against cybersquatting and counterfeiting.

The way ICANN works is via a bottom-up, multi-stakeholder model, which means that everybody has a say, and there's a consensus that's supposed to be built. But you've got privacy advocates on the one hand, you've got rights holders on the other hand, you've got other people in the middle, and everybody has a different perspective. Trying to find a solution which fits everybody's requirements is going to take a very long time.

MS. CASTAGNOLI: Never going to happen.

MR. DICKSON: Until somebody actually steps up and says, "This is what we have to do."

MS. CASTAGNOLI: In the meantime the cybersquatters are going gangbusters.

MR. DICKSON: Exactly.

MS. CASTAGNOLI: That's an example where if you are a brand owner or if you are in an industry that is at risk for a business email compromise and you are now compromised, this will be really important to you.

But there are some other effects of the GDPR. Rob, are you going to talk about all the other annoying things that are happening with the GDPR?

MR. NEWMAN: Well, there are some annoying things that I can name.

MS. CASTAGNOLI: Yes, name them.

MR. NEWMAN: For example, we have U.S. companies that have just decided to block EU traffic altogether. I don't think the European Union neces-

---

[28] ICANN, Temporary Specification for gTLD Registration Data (effective May 25, 2018). *See also* Göran Marby, ICANN President and CEO, ICANN GDPR and Data Protection/ Privacy Update (Sept. 24, 2018); Jeremy Malcolm, Electronic Frontier Foundation, Privacy as an Afterthought: ICANN's Response to the GDPR (Apr. 18, 2018).

sarily planned on that. There are several publishers, for example, who, rather than go through all the hoops, just say, "If you are from the European Union, you have an IP address originating in the European Union, this website is not for you." I think that was unintended.

I also think, unintended or intended, the biggest issue that we are grappling with now is the California Consumer Privacy Act of 2018 (CCPA).[29] This is a new law that will go into effect January 1, 2020. It's a California law, but, as the fifth-largest global economy, it is going to affect all of the United States, and also probably companies throughout the world.

The CCPA does not require consent or legitimate interests or other things that are required under the GDPR, but it does require all sorts of disclosures about what information you are collecting on a granular level. It also grants data subjects several new rights. For example, if a consumer calls you and says, "I want you to delete my data, I want access to my data, I want it to be portable" — these are all rights under the GDPR — they are now going to be rights in the United States come January 1, 2020.

MS. CASTAGNOLI: Who does the CCPA impact? They have a set of criteria about what organizations it impacts.

MR. NEWMAN: It will apply if you are a large company with $25 million or more of annual revenue. If you collect personal information — and "personal information" is extremely broadly defined in both the GDPR and the CCPA — from or about a California resident and you have $25 million or more in revenue, then you are basically stuck with this law.

MS. CASTAGNOLI: I'm more interested in the part of it that says, "if in 10 percent of your business you are acting as a data broker." Have you ever tried to get anything fixed on your credit report? I'm just going to get an address in California and use that.

MR. NEWMAN: Right. But I think non-data brokers are not going to be able to escape this.

MS. CASTAGNOLI: I just thought that was amusing. It says that if in 10 percent of your business you are acting as a data broker, regardless of residency — boom! — you're subject.

MR. NEWMAN: It will be difficult for a lot of companies that thought they were out of the woods on GDPR, that they didn't have to go through the data mapping and the record of processing and all these things that they were going to have to do under GDPR, and now they are behind the eight ball.

MS. CASTAGNOLI: How many people have done a GDPR Readiness Assessment?

[Show of hands]

Bless your hearts. You're here. You survived it.

How many of you have clients who you think should have done it but haven't?

[Show of hands]

[29] Amendments passed as SB 1121 on Aug. 31, 2018 and signed into law by Gov. Brown September 23, 2018.

Well, take this panel transcript and say, "You have no choice now. California is coming."

MR. BALLON: Well, there is a year before it goes into effect. Congress may yet enact a federal consumer privacy law that preempts the CCPA.

MS. CASTAGNOLI: One side effect, I think, of the CCPA is that we've seen interest from a lot of tech companies. What have you heard about it, and what do you like and not like about the proposed federal legislation?[30]

MR. BALLON: I can't speak about specific legislation. I'm just saying that the CCPA may yet be preempted by federal legislation, in the same way that an overly aggressive anti-spam email law in California prompted federal legislation (the CAN-SPAM Act) to preempt it back in 2003.

MS. CASTAGNOLI: Well, there is a proposal that was sent to Congress.

MR. BALLON: I'm a litigator, so I don't typically closely analyze proposals. A proposed law isn't binding in my practice until it is signed by the president or enacted by Congress overriding a veto. Otherwise, it is all hypothetical.

MR. NEWMAN: Until the complaint comes in, right?

MS. CASTAGNOLI: I honestly don't think the proposed federal legislation will pass because this is just not a priority for Congress right now. They have other things to worry about. I think California is going to slip in by default, and then we're in for an exciting time.

The biggest complaint I've heard about the proposed federal legislation is that it eliminates the private right of action. The only remediation it is suggesting is fines. We have seen how effective the FCC has been with its fines — they look like three seconds' worth of profit, and they are statutorily limited.

MR. BALLON: But the private right of action under the CCPA is limited to security breaches.

MS. CASTAGNOLI: I'll take anything.

MR. BALLON: As amended in September 2018, it really only deals with security breaches. Now, there will be a lot of litigation because of the availability of statutory damages, and I can tell you as a litigator that these types of claims impose a tax on doing business. If the government wants to impose a tax, it would be more efficient to raise taxes — and use the money for social good such as healthcare — rather than to impose a "tax" that merely enriches a small group of plaintiffs' class action lawyers.

---

[30] The U.S. Chamber of Commerce submitted a proposal and statement and is lobbying Congress to pass a federal omnibus privacy and data protection law that would preempt the CCPA and other existing and future state data protection laws. The Internet Association, a trade group that represents leading Internet companies, has also released a proposed framework for federal legislation. On Sept. 24, 2018, the Interactive Advertising Bureau, with 650 digital advertising industry members, joined in the calls for a federal omnibus law to pre-empt CCPA in a letter to the Senate Committee on Commerce, Science, and Transportation.

U.S. Senate Committee on Commerce, Science, and Transportation Hearing, Examining Safeguards for Consumer Data Privacy (Sept. 26, 2018). The hearing focused on the potential for federal privacy regulation. The discussion centered on two issues: (1) the potential for Congress to pass a federal privacy law, including the scope and model for any such law, and (2) the role of the Federal Trade Commission in regulating data privacy practices. Representatives from Apple, Amazon, AT&T, Charter Communications, Google, and Twitter testified. *See* Reuters, David Shepardson, Tech companies back U.S. privacy law if it preempts California's (Sept. 26, 2018).

MS. CASTAGNOLI: That is what the United Kingdom is trying to do.

MR. BALLON: The notion that this kind of litigation helps consumers is not true.

MS. CASTAGNOLI: But it makes us feel better.

MR. BALLON: In most cases it operates as a tax, where money is transferred from companies to a small group of plaintiffs' lawyers.

MS. CASTAGNOLI: Yes, most of it goes to the lawyers.

MR. BALLON: That's not efficient. Create safe harbors to encourage good behavior (as under the DMCA[31] or the new Ohio security breach law[32]), or provide exclusively for regulatory enforcement so that suits are brought for reasons other than financial enrichment, but don't just put money into the pockets of a small group of lawyers for no broader social good.

MS. CASTAGNOLI: Do you have an undergraduate degree in economics?

MR. BALLON: Yes.

MS. CASTAGNOLI: Aha! I didn't know that before.

AUDIENCE [Mr. Friedlander]: Would the purpose of the federal bill be to preempt the states?

MS. CASTAGNOLI: Yes, that's what they want.

MR. NEWMAN: The concern that many people have is that the federal law will only set a floor and then you would end up with fifty-one state laws.

MS. CASTAGNOLI: Like the situation with data breach notification.

MR. NEWMAN: Yes, right. We have the federal data breach laws that are sector-specific and then we have fifty states with general data breach notification laws. If we get a CAN-SPAM-like law that preempts state law, I think that would be great. Whether or not that is going to happen remains to be seen.

MR. BALLON: The concern is that other states, like Vermont and others, will pass their own versions of the CCPA.[33]

MS. CASTAGNOLI: Nobody has mentioned my biggest annoyance with regard to GDPR. You walk off the plane, and as soon as you open up your phone and try to access a website you get hit with all these consent notifications — "We use cookies — consent." You know how hard that is to do. And there's no cookie manager on my phone. I have a password manager, but I don't have a cookie policy manager.

And they are not very good at remembering who you are. If you move around a little bit, it gets lost. I guess they aren't tracking your phone, your International Mobile Equipment Identity number, because they are not allowed to anymore. So you get hit with those notifications every time, over and over again.

MR. DICKSON: Yes. There is a new set of regulations coming as well to update the law on cookies, the ePrivacy Directive.

---

[31] Digital Millennium Copyright Act, Pub. L. 105-304, 112 Stat. 2860 (1998).

[32] The Ohio Data Protection Act (2018 SB 220) (effective Nov. 2, 2018).

[33] Vermont Financial Regulation, H.764, An act relating to the regulation of data brokers. *See also* Colorado's new privacy legislation, an Act Concerning Strengthening Protections for Consumer Data Privacy (HB18-1128) (effective Sept. 1, 2018).

MS. CASTAGNOLI: Which is also going to deal with the IP address question?

MR. DICKSON: Yes. It's an ongoing process.

MS. CASTAGNOLI: But I don't think that is going to hit until 2020, right?

MR. NEWMAN: They say 2019.

MR. LAI: It may not ever get there.

MS. CASTAGNOLI: All right, let's take a vote. What did I hear? I heard "not ever" — who said "not ever?"

MR. LAI: It may not ever get there. The Commission and the Parliament and the Council have released drafts that are wildly divergent.

MS. CASTAGNOLI: Nice!

MR. LAI: They run the gamut from "everything is mostly going to stay the same as it is now" to "really what we want to do is make behavioral advertising illegal."

MS. CASTAGNOLI: There is currently a Directive.

MR. LAI: There's not one guy who has the pen here. There are three different drafts. The EU governance is really weird.

MR. DICKSON: It's not uncommon to have three different versions of a piece of legislation come out, and they may start very far part, but eventually they usually get something that makes everybody unhappy.

MR. LAI: They will eventually negotiate their way through.

MS. CASTAGNOLI: Who said 2019?

MR. NEWMAN: I said 2019. That has been the rumor.

MS. CASTAGNOLI: And your basis for that?

MR. NEWMAN: Folks have been saying since May that 2019 was a likely date.

MR. DICKSON: But in the meantime you don't just have to get ready to be compliant with the GDPR. One of your obligations under the GDPR, if you are selling anything to consumers in the European Union or monitoring your behavior, is to stay up-to-date with developments. There is an ongoing accountability obligation as well.

MS. CASTAGNOLI: Oh yes, which brings us to my favorite part of the GDPR — this is great for you as a litigator; I'm going to get a whole new career for you — which is what is "reasonable security?"

MR. DICKSON: Well, here's the question. Even if somebody says, "Okay, you're from the European Union, we are going to block you from there" — okay, that might be one workaround. But how long before financial institutions, for example, start to say, "We can see that GDPR is a good way of monitoring personal data and we can see overlaps between the GDPR and how we should be managing your financial information." So the GDPR might actually become a good benchmark for dealing with information — maybe not in the United States, but maybe in other places.

At some point a lot of these are going to converge and we will have a base level of compliance, whether it's under GDPR or whether it's under financial regs or something else. It doesn't matter. It's all going to change our perception of what is "reasonable."

One of the objectives of the GDPR is "privacy by design," trying to change hearts and minds, so that we put the consumers at the center of all the transactions and make sure that they are not commoditized.

MS. CASTAGNOLI: Yes.

MR. LAI: Understandably commoditized.

AUDIENCE: One of the ironies of this is the United Kingdom also has Open Banking.

MR. SMEDINGHOFF: Yes.

MS. CASTAGNOLI: Right, application program interface (API) connectivity.

AUDIENCE: There is a transfer of data. On the one hand, they are saying "secure." On the other hand, they are saying, albeit with consumer consent, "allow it to be shared freely."

MS. CASTAGNOLI: No, no, no. That's going to be over a highly authenticated, with deep identity proofing, secure API.

MR. SMEDINGHOFF: In theory.

MR. LAI: Well, that goes to your question, right? What is "reasonable security" for a bad-use case is going to be very different than for something else.

MS. CASTAGNOLI: Yes. But let's back up. You brought up a very interesting point. Is it a national law, is it a UK law, or is it an EU law regulating banking that is requiring banks to create APIs to allow third parties to integrate with your bank account?

MR. SMEDINGHOFF: That's EU law.

MS. CASTAGNOLI: Now I will tell you I really want that here in the United States. Right now the only people who have open API access to your bank account are the data brokers — Yodlee, Acxiom — so they exist, but they are only for companies. As an individual, if I wanted API access to my own banking information, they won't give it to me. I've tried. I've asked nicely — "Hey, I'm a dude, I'm a programmer, I can do this, you can trust me" — and I've asked not so nicely but they still said "No."

It will be interesting to see what happens with Open Banking. Do you know when it goes into effect?

MR. DICKSON: No, I don't.

AUDIENCE: It's not that far off.

MR. DICKSON: There's Brexit in the middle of all this as well.

MS. CASTAGNOLI: Oh yeah, that's right, so you're busy

MR. DICKSON: Yes, which may or may not have an impact.

MS. CASTAGNOLI: I think something like the Open Banking API is probably going to be a matter of commercial self-interest. If it goes EU-wide, then, even if you're UK-based banks, you are going to have to have this.

MR. DICKSON: Why would they not want to, right?

AUDIENCE: I have some questions. I've heard a couple different things, but not from anyone who is an expert on or who has done a lot of reading on GDPR. Is there anything that applies to companies that may be targeting U.S. citizens generally? And do they also need to be concerned about an EU resident living in the United States with regard to being compliant with GDPR?

MR. DICKSON: Yes. The whole point of the GDPR is the effect that there can be over-coverage. So if you have 999,000 non-EU citizens in your database and just one EU resident, then, sorry, you've got to comply with the GDPR. Someone based in the United States could move to the European Union. You might be targeting the United States, but is there a hard block on anyone signing up to your database from within the European Union?

MS. CASTAGNOLI: Here's how I handle that. My terms of service says that the services here are not directed to EU citizens and if you as an EU citizen elect to opt into our services then you agree that the purpose is lawful, and then you're opting in.

MR. DICKSON: Yes, but your consent has to be specific and informed.

MS. CASTAGNOLI: Well, it is. We're clear and we inform, but they have to expressly agree.

MR. NEWMAN: But it's on page 57 of your terms of use, right?

MR. DICKSON: Even if it's specific on what exactly you are agreeing to, you are confirming that it's lawful. Now, if I don't know what's lawful in the United States or elsewhere, is my consent "informed?" Is it specific? If you just give a general "it is lawful," what does that mean? Is it lawful under what theory or under what cases?

MR. NEWMAN: But if you are not established in the European Union, if you are a U.S.-only company, no boots on the ground in the European Union, and you're not directing services to the European Union —

MS. CASTAGNOLI: And don't have privacy fields.

MR. NEWMAN: — but you have an incidental visitor coming to your site from the European Union and you're not systematically monitoring or profiling EU residents.

AUDIENCE: What do you think about an EU resident living in the United States?

MR. NEWMAN: If you don't fall within the definitional buckets — you're not established there; you're not directing services to the EU, and you're not monitoring or profiling EU residents – then I would not worry much about the GDPR.

MR. LAI: It's one of the areas where the GDPR is actually reasonably clear about whether you fall within its scope or not. You can go through "if (a), then (b), then (c)." In your case, the answer is probably no.

MS. CASTAGNOLI: I don't know. I think the privacy rights follow the citizenship, follow the person.

MR. DICKSON: It's one of the resources.

AUDIENCE: If they come to the United States, then they are not covered by the GDPR.

MR. NEWMAN: Right, exactly, so they're not covered.

AUDIENCE: The GDPR is very specific about it. It says "persons within the EU." If they come to the United States, they are no longer within the European Union.

AUDIENCE: But if a U.S. citizen goes to Europe —

MR. NEWMAN: Then they are covered.

AUDIENCE: But only for the time that they are in the European Union. Once they leave the European Union they're not.

MS. CASTAGNOLI: I'm sorry. I was referring to the EU citizen who's in the European Union accessing your services over the Internet. They are not physically in the United States.

MR. LAI: But if you are not systematically monitoring them, if you don't target your services — there are these very specific categories on what brings you within its scope. So you need to look there and make that judgment call based on what it is that your client is doing.

MS. CASTAGNOLI: One last question?

AUDIENCE [Mr. Fallon]: Is my Outlook contact list with all the people I know in the European Union and their phone numbers a violation of the GDPR? And what about my LinkedIn contacts where I'm keeping track of their activities theoretically in the European Union?

MR. DICKSON: In theory, any of those could be covered. You've got to define exactly what your processing is. So each individual stage of what you are doing with any of those contact lists will be a different instance of processing.

MS. CASTAGNOLI: He's an individual.

MR. LAI: Yes. And also why you're doing it, right?

AUDIENCE [Mr. Fallon]: Yes. But I'm using it for my firm practice. I have clients in Europe. I will be flying to Berlin next Thursday. Am I going to be arrested when I land?

MR. DICKSON: No. Just because you're processing something doesn't mean that you are breaking the law.

MR. LAI: Yes, but you'll be arrested a day later.

AUDIENCE [Mr. Fallon]: Will I be arrested in Paris or Berlin?

MS. CASTAGNOLI: Since we are in the great city of Chicago, which is home to *Wait Wait ... Don't Tell Me!*, which is a really funny political show on NPR, we are going to pull a predictor test out of one of those shows. I'm going to give you guys a scenario and each of you has thirty seconds to tell me what you think the outcome is going to be. Here we go.

MR. NEWMAN: We weren't prepared for this.

MS. CASTAGNOLI: I know.

AUDIENCE: That's the whole point.

MS. CASTAGNOLI: We have had some interesting situations here in the United States associated with the benefits of elements of a human. There are categories of medical waste when you go in for a process or procedure — your cells, everything. But we also now have proven that this is personally identifiable information. With the cells of Henrietta Lacks (HeLa) you can take these waste components and you can reidentify them to a specific individual.

My question is: If we get some GDPR-type legislation here in the United States, what happens to medical waste? Do you own it, do you control it, or not?

MR. BALLON: Well, we are not going to have GDPR-type legislation in the United States because of the First Amendment, among other things. We place greater protection on freedom of speech than protection of information in databases.

MR. NEWMAN: It seems to me that it would be possible that certain of this material could be viewed as a biometric identifier in our hypothetical future law, depending on how "biometric identifier" gets defined in the law.

MR. DICKSON: Yes. It all comes down to the aggregation of data. So you might be able to take a DNA swab from an arm on its own but if you don't have access to a database that identifies the DNA to a living person, then there's no GDPR problem.

MS. CASTAGNOLI: Because it would not be identifiable.

MR. DICKSON: It is not personally identifiable. If the person is deceased, then the GDPR also doesn't apply because it's only for a living individual.

MS. CASTAGNOLI: Nice.

MR. SMEDINGHOFF: Is "it depends" an acceptable answer? [Laughter]

MS. CASTAGNOLI: Of course.

MR. SMEDINGHOFF: That cell case — and I haven't followed it closely — is something that I don't think was on anybody's radar screen.

MS. CASTAGNOLI: Oh no, it has been done before. There is actually a Supreme Court case, *Maryland v. King*. There have been cases in the past where cells from certain procedures have been taken and then used to make drugs, especially autoimmune drugs, and the individuals were never asked, never gave consent, and the doctors made a fortune on it.

MR. SMEDINGHOFF: I don't think that comes under the GDPR.

MS. CASTAGNOLI: Okay.

MR. DICKSON: I don't either.

MR. POELL: I could see a creative litigator trying to make a case out of something like that.

MS. CASTAGNOLI: David?

MR. POELL: We creatively defend and make new law.

MR. LAI: It could be captured under something like CCPA, which is a little broader.

I'm going to answer your question with a question, though, which is another thing that we love to do. What do you think about the fact that this is going on right now with consumer genetic testing, where in their terms of service they reserve the right to resell that information to other people? Pharma companies are buying these sets of data to do discovery on, where they would previously have had to actually get your consent and probably pay you a lot more money than they are paying to 23andMe. From a commercial regulation standpoint, where do you think the individual's rights fall there?

MS. CASTAGNOLI: Don't use 23andMe.

MR. LAI: Also that.

MS. CASTAGNOLI: A very good question.

Does anybody have a really burning question?

AUDIENCE [Michael Baumert]: This is a question for Gareth: Are you aware of any investigations of U.S. companies that have no location in the United Kingdom?

MR. DICKSON: Not specifically. But the first enforcement action carried by the United Kingdom's Information Commission Office was against a Canadian company that was processing the data of British voters as part of the Brexit refer-

endum.[34] It's interesting — it really just goes to show the extraterritoriality of this — that the very first action they took was against a non-EU company.

MR. SMEDINGHOFF: No establishment in the European Union?

MR. DICKSON: No, just a contract.

MS. CASTAGNOLI: Great. If you have more questions, grab one of these guys. They know stuff. I just talk.

Thank you.

[34] *See* Jonathan Chadwick, *AggregateIQ Hit With First GDPR Enforcement Notice GDPR Enforcement: Test Case for ICO*, COMPUTER BUS. REV. (Sept. 21, 2018).