University of Colorado Law School
Colorado Law Scholarly Commons

Articles | Colorado Law Faculty Scholarship

2020

Symposium: The California Consumer Privacy Act

Margot Kaminski
University of Colorado Law School

Jacob Snow
ACLU of Northern California

Felix Wu
Benjamin N. Cardozo School of Law

Justin Hughes
Loyola Law School Los Angeles

Follow this and additional works at: https://scholar.law.colorado.edu/articles

 Part of the Constitutional Law Commons, First Amendment Commons, Internet Law Commons, Privacy Law Commons, and the State and Local Government Law Commons

Citation Information

Margot Kaminski, Jacob Snow, Felix Wu, and Justin Hughes, *Symposium: The California Consumer Privacy Act*, 54 Loy. L.A. L. Rev. 157 (2020), *available at* https://scholar.law.colorado.edu/articles/1333.

Copyright Statement

Copyright protected. Use of materials from this collection beyond the exceptions provided for in the Fair Use and Educational Use clauses of the U.S. Copyright Law may violate federal law. Permission to publish or reproduce is required.

This Article is brought to you for free and open access by the Colorado Law Faculty Scholarship at Colorado Law Scholarly Commons. It has been accepted for inclusion in Articles by an authorized administrator of Colorado Law Scholarly Commons. For more information, please contact jane.thompson@colorado.edu.

SYMPOSIUM:

THE CALIFORNIA CONSUMER PRIVACY ACT

Margot Kaminski

Jacob Snow

Felix Wu

Justin Hughes, moderator

Loyola of Los Angeles Law Review is pleased to publish the third "symposium discussion" series in which leading experts are invited to engage in an evening symposium on a new or emerging area of law. The subject of our second evening symposium was the California Consumer Privacy Act (CCPA), a statute signed into state law by then-Governor Jerry Brown on June 28, 2018 and effective as of January 1, 2020.

As with most new law, there are many unsettled issues, disagreements about the likely impact of the law, and much to be developed as regulations are established and the law is tested in court. To shed some light on the CCPA, the symposium panelists were:

- MARGOT KAMINSKI – Margot Kaminski is an Associate Professor at the University of Colorado Law School and the Director of the Privacy Initiative at Silicon Flatirons. Prior to joining Colorado, Margot was an Assistant Professor at the Ohio State University Moritz College of Law (2014–2017), and served for three years as the Executive Director of the Information Society Project at Yale Law School. She received her B.A. from Harvard University and her J.D. from Yale.
- JACOB SNOW – Jacob Snow is a Technology and Civil Liberties Attorney at the ACLU of Northern California, where he works on a variety of issues, including consumer privacy, surveillance, and the preservation of free speech online. Prior to joining the ACLU, Mr. Snow was a staff attorney at the Federal Trade Commission.

He holds a B.A. in Physics from the University of California at Berkeley and a J.D. from Georgetown Law.

• FELIX WU – Felix Wu is a Professor of Law at Cardozo Law School, Yeshiva University, where he is also Director of the Cardozo Data Law Initiative. Professor Wu's information law scholarship spans freedom of speech, privacy law, and intellectual property. He received his B.A. in computer science summa cum laude from Harvard and both his J.D. and Ph.D. from the University of California at Berkeley.

And our moderator,

• JUSTIN HUGHES – Justin Hughes holds the Hon. William Matthew Byrne, Jr. Chair at Loyola Law School, Loyola Marymount University.

JUSTIN HUGHES: Good evening, everyone. On January 1st of this year, the California Consumer Privacy Act[1] came into effect making our state the first in the nation to pass a comprehensive law giving each consumer substantial control over the data collected on that person, both on the internet and in more traditional business transactions. Much has been said comparing California's new law to the General Data Protection Regulation in European Union.[2] If you go to some websites now, you're given a choice: if you're a California resident, you can move into one direction for privacy controls and if you're a European Union resident, you can move to another area of the site.

Tonight, we are going to focus on the CCPA itself so that everyone has a better understanding of what it does, what questions courts are likely to have to address, how businesses are responding to the new law, and some of the challenges of making the CCPA compatible with First Amendment concerns. We could parse the different rights of the CCPA in different ways. I'm going to give you

1. *See* CAL. CIV. CODE §§ 1798.100–1798.199 (Deering 2020).

2. *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR]; Danielle Kucera, *CCPA vs. GDPR: Similarities and Differences Explained*, OKTA (July 9, 2020), https://www.okta.com/blog/2020/07/ccpa-vs-gdpr/ [https://web.archive.org/web/20200815060313/https://www.okta.com/blog/2020/07/ccpa-vs-gdpr/].

the bumper-sticker version because our panelists will elaborate much more on each element of the law. First, there is a right to learn—or right of access to—what personal information is being collected about the consumer, the sources of the information, the categories of the information, the purposes for which the business is collecting them, and the specific information.

I really recommend, if you have not done it, to go to Facebook and download all the information that they have about you.[3] It's pretty interesting. Second, there is the right to have that personal information deleted. And, third, there is the right to opt out of having that personal information sold. The CCPA does not apply to businesses below certain thresholds, nonprofit organizations, or journalism.[4] Nonetheless, best estimates are that it will affect about half a million businesses in California and the result is quite possibly a sea change in both privacy rights in the United States and in the global information economy.

To discuss the law with us, we have a distinguished panel. First is Professor **Margot Kaminski**, who is an Associate Professor of Law at the University of Colorado Law School where she teaches and researches and writes on law and technology. Before joining the University of Colorado, Professor Kaminski was on the faculty at Ohio State University, clerked for Judge Andrew Kleinfeld of the Ninth Circuit, and served as the Executive Director of the Information Society Project at Yale Law School.

Next is **Jake Snow**, who is a technology and civil liberties attorney at the American Civil Liberties Union (ACLU) in Northern California, and has been at the forefront in the fight for consumer protection of privacy. He works on consumer privacy, surveillance, and the preservation of free speech online. Before joining the ACLU, Mr. Snow was a litigator at the Federal Trade Commission in San Francisco focusing on consumer protection. He also clerked for Judge Ronald M. Whyte of the Northern District of California.

Our third panelist is Professor **Felix Wu** from the Benjamin N. Cardozo School of Law in New York, where he is also the faculty director of the Cardozo Data Law Initiative. Professor Wu writes on online intermediary immunity, data de-identification, commercial

3. *How Do I Download a Copy of My Information on Facebook?*, FACEBOOK, https://www.facebook.com/help/212802592074644 (last visited Oct. 4, 2020).

4. *See* CAL. CIV. CODE § 1798.140(c), (f) (defining "business").

speech protection, and the relationship between privacy and theories of free expression.

Let's start with Professor Wu, because a key element of this I'd like you to explain for us is what personal information is. As I understand it, the CCPA has a very broad definition of personal information—that it's anything reasonably capable of being associated with or could be reasonably linked to a particular consumer.[5] Professor Wu, could you start the conversation by talking about that?

FELIX WU: Right. Thank you, Justin. Thanks for having me here at this panel. It's great to be here. It's great to have this opportunity to talk a little bit about the CCPA and its nuances. As described, whenever you have a privacy law, one of the key questions is, What's the scope of the law? And one of the key questions for determining the scope of the law is, What is the concept of personal information that the law will cover? I want to make four points briefly in the time that I have here.

The first is that the definition of personal information under the CCPA is indeed quite broad,[6] broader than what you tend to see in other privacy laws particularly in the United States.[7] Second, there's a reason for this breadth. There are reasons to want to have a pretty broad conception of personal information being covered in order to be able to address certain kinds of privacy issues that might arise. Third, the breadth of this definition combined with the relative breadth of the different forms of rights provided under the CCPA can lead to some interesting and difficult puzzles when it comes to implementing some of the rights that are in the CCPA. Finally, that maybe the California Attorney General's regulations and other ways in which the law is being implemented might at least start to ameliorate some of the difficulties that I will identify, but perhaps not all of them, and I think there is still work to be done.

First on the breadth of the definition here. It's quite common to see fairly general definitions of what counts as personal information

5. *See id.* § 1798.140(o) (defining "personal information").

6. *See id.*

7. *See, e.g.*, Video Privacy Protection Act, 18 U.S.C. § 2710(a)(3) (2018); Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.501 (2002).

in many privacy laws.[8] It is common to see phrases like: not only information that directly identifies some individual, but information that is reasonably identifiable and could be reasonably used to identify someone.[9] That concept of "reasonably identifiable" in the CCPA's definition of personal information is a relatively more common part of the definition;[10] it's part of the definition in the CCPA and increasingly true even of other statutes that don't specifically mention the concept of "reasonably identifying."

I will flag here though that even just the concept of information being "reasonably identified" with a particular person hides some difficult questions.[11] In particular, it potentially hides the question of, "reasonably identifiable by whom?" What I mean by that is that, when you're trying to figure out whether it's reasonably possible to connect information to a particular individual, you often have to think about: Who are we thinking of as the relevant actor? Who is the one that might do this potential linkage or identification? It matters a lot what other information that particular actor or individual or entity already has, with respect to how reasonably identifiable or reasonably linkable some information might be.

We've seen this previously, for example, in the context of a different privacy law, the Video Privacy Protection Act,[12] where some courts have interpreted the concept of reasonably identifiable in the context of that law to mean reasonably identifiable by a total stranger.[13] As a result, courts have held that certain kinds of

8. *See, e.g.*, 18 U.S.C. § 2710(a)(3); Cable Communications Policy Act of 1984, 47 U.S.C. § 551(a)(2)(A) (2018) (rather unhelpfully stating that "the term 'personally identifiable information' does not include any record of aggregate data which does not identify particular persons"); GDPR, *supra* note 2, art. 4, at 33 ("'personal data' means any information relating to an identified or identifiable natural person").

9. *Cf.* 45 C.F.R. § 160.103 (defining "individually identifiable health information" as information "(i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual"); GDPR, *supra* note 2, art. 4, at 33 ("[A]n identifiable natural person is one who can be identified, directly or *indirectly* . . . ." (emphasis added)).

10. *See* CAL. CIV. CODE § 1798.140(o)(1) ("'Personal information' means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.").

11. *See* Felix T. Wu, *Defining Privacy and Utility in Data Sets*, 84 U. COLO. L. REV. 1117, 1158–59 (2013).

12. 18 U.S.C. § 2710.

13. *See, e.g.*, Eichenberger v. ESPN, Inc., 876 F.3d 979 (9th Cir. 2017); *In re* Nickelodeon Consumer Priv. Litig., 827 F.3d 262 (3d Cir. 2016).

information are not personal information under the law—even if that information might actually be identifiable by the person who is, in fact, holding that information or to whom the information is going to be conveyed.[14]

So, it matters whether we're thinking about reasonably identifiable as reasonably identifiable by a complete stranger or reasonably identifiable by the particular entities who are holding on to data or who might be receiving the data. As I said, though, that's a problem that we've addressed at least in some measure before the CCPA—maybe not satisfactorily, but at least we have seen it before.

One of the ways in which the CCPA is unusually broad though is, for example, the coverage not just of information that is identifiable with respect to an individual but information that's identifiable with respect to a household.[15] Moreover, the definition includes not just information that *identifies* a consumer or a household, but also information that *relates to* or *describes* such a consumer or household.[16] These concepts are expressed in the alternative, suggesting that the definition goes beyond actually *identifying* an individual or a household. There's some question as to what that would mean: What does it mean for information to relate to or describe an individual or household even if the information is not necessarily identifiable to that individual or household?

So the CCPA's definition of personal information is quite broad. Why might we want such a broad definition of personal information? I think one of the key things that the CCPA was meant to address is the problem of profiling. When you look at some of the things that are specifically listed as forms of personal information—things like collections of commercial transaction activity, collections of web browsing activity, and the like[17]—I think the idea is very much that when companies take this information and create a profile of

14. *See Eichenberger*, 876 F.3d at 985–86 (holding that a Roku device serial number and plaintiff's watch history were not personally identifiable information within the meaning of the VPPA); *In re Nickelodeon*, 827 F.3d at 281–90, 295 (rejecting plaintiffs' claim that static digital identifiers such as IP addresses and cookies were personally identifying information).

15. CAL. CIV. CODE § 1798.140(o)(1) ("'Personal information' means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or *household*." (emphasis added)).

16. *Id.*

17. *Id.* § 1798.140(o)(1)(D)–(F).

somebody, even when they don't specifically attach a name to that profile, that is still the sort of activity that raises privacy concerns.

These kinds of profiling can raise privacy concerns for lots of reasons, one of which might be, for example, the possibility that it's used to target individuals or to shape their experiences online even when the targeting or shaping is, again, not linked to a particular name. We might worry about it also because of the ways in which this creates a kind of surveillance of individuals by these larger companies that then enables those companies to exploit the power they have over their users or that could lead to some sort of chilling effect.

There are lots of reasons potentially to be worried about profiling. If you're going to worry about profiling, that necessitates a fairly broad definition of personal information in order to cover these profiles, even when the profiles are not directly linked to traditional identifiers like names or addresses or email addresses. Not everyone thinks that regulating profiling is the right thing to do, of course,[18] but it is at least a sensible reason to want to have a broad definition of personal information.

At the same time though, having such a broad definition of personal information can get really tricky when you also have a number of different kinds of rights and they are all linked to exactly the same definition of personal information. I want to flag in particular this right to access or right to know. Now, we have had access rights in other laws, but often tied to particularly narrow definitions of personal information. An example here would be the federal Privacy Act,[19] which has a weird and oddly narrow concept of personal information. It has to be not just personal information of some sort; it has to be a "record which is contained in a system of records."[20] That

18. *See* Adam Thierer, *Relax and Learn to Love Big Data*, U.S. NEWS & WORLD REP. (Sept. 16, 2013, 12:10 PM), https://www.usnews.com/opinion/blogs/economic-intelligence/2013/09/16/big-data-collection-has-many-benefits-for-internet-users.

19. *See* The Privacy Act of 1974, 5 U.S.C. § 552a (2018); *The Privacy Act of 1974*, U.S. DEP'T OF JUST., https://www.justice.gov/opcl/privacy-act-1974#:~:text=The%20Privacy%20Act%20of%201974,of%20records%20by%20federal%20agencies (last visited Oct. 4, 2020) (The Privacy Act of 1974, 5 U.S.C. § 552a (2018) establishes standards for the "collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies."). Pursuant to 5 U.S.C. § 552a(d)(1) "[e]ach agency that maintains a system of records shall . . . upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him."

20. 5 U.S.C. § 552a(b).

is, it has to be information that can be retrieved using the name of the person involved in order to be covered under the Privacy Act.

This leads to weird results when the government ends up disclosing information, but you might think of it as actually a fairly sensible definition when what you're getting is an access right to this information. This definition means that the government only needs to look up stuff that they can actually look up—that is, look up the stuff that's actually tied to your name. But we don't have that in the CCPA. We have one definition of personal information that applies both to the right to know (or right to access) as well as the right to opt out and the right to delete. There are lots of situations where we want to give individuals control over the profiles that are potentially being made about them, to be able to opt out of the profiling, say, but it's much harder to figure out what it would mean to give them access to those profiles when those profiles are not, in fact, linked to their names.

Just think about a record that lists a whole bunch of transactions in it. That long list of transactions is almost surely personal information under the California law, but it is the sort of thing that may be difficult to isolate and find and therefore spit back at the person who is asking about all of the bits of personal information that the company holds about him or her.

What can we potentially do about this? Now, I think there's no easy answer as to exactly how to address this, but I do want to point out at least one part of the Attorney General's regulations that might ameliorate some of these concerns—namely, this idea of when can you reasonably verify someone's access request.[21] One of the provisions in the Attorney General's regulations says that if you can't reasonably verify someone's request, you don't necessarily need to fulfill the request.[22] Mostly, this was meant as a security measure because personal information, of course, can be highly sensitive. If you give it to the wrong person, that's going to create more problems than the ones you were trying to solve in the first place.

This concept of verifying a request, I think, was largely designed with those security concerns in mind, but the draft regulations do say

21. *See* CAL. CODE REGS. tit. 11, § 999.313(c)(1) (2020) ("For requests that seek the disclosure of specific pieces of information about the consumer, if a business cannot verify the identity of the person making the request pursuant to the regulations set forth in Article 4, the business shall not disclose any specific pieces of personal information to the requestor and shall inform the requestor that it cannot verify their identity.").

22. *Id.*

that if you can't reasonably verify a request then that's a valid ground for not fulfilling the request. In a way, some of what I'm describing are situations in which it's arguably not possible to reasonably verify a request. How do you know whether a long list of transactions is, in fact, this person's transactions unless you actively go through the list trying to figure it out? It would seem like a bad idea to ask companies to do that. So maybe this part of the regulations might help.

I will say, though, that this part of the regulations applies only to the access right and not to the opt-out right, which means that it is still going to be the case that when an individual opts out of the sale of their data, it will be tricky to figure out how a company will find all the relevant profiles in order to ensure that they are not, in fact, transferred in a sale transaction. I think there will continue to be difficult problems with, again, the breadth of the rights combined with the breadth of the definition of personal information.

JUSTIN HUGHES: Thank you. Professor Wu has already raised so many interesting questions and I should add what I should have said in the introduction is that the law is not enforceable until the middle of this year and the California Attorney General has been in the process of issuing regulations of which there have been two iterations?

MARGOT KAMINSKI: Yes.

JUSTIN HUGHES: Two iterations. Now, Professor Kaminski, I think the regulations are actually shorter than the law itself. Is that right?

MARGOT KAMINSKI: Yeah.

JUSTIN HUGHES: All right. When we refer to the regulations, we're referring to the draft regulations that are not yet made official, is that correct?

MARGOT KAMINSKI: Yes, the comment period ends the end of this month, February 25.

JAKE SNOW: Yeah.

MARGOT KAMINSKI: But the reason we're both reacting is because there will probably be retroactive enforcement of the regulations that are not in place yet.[23]

23. *See* Chris Mills Rodrigo, *Historic California Data Privacy Measure Leaves Companies Scrambling*, THE HILL (Jan. 1, 2020, 6:00 AM), https://thehill.com/policy/technology/476368-historic-california-data-privacy-measure-leaves-companies-scrambling.

JUSTIN HUGHES: Yes, that's another bizarre issue. There may be retroactive enforcement of regulations that the companies don't yet know. The Act will be effective on July 1, correct?

JAKE SNOW: The language of the statute is that the Attorney General (AG) can't bring an enforcement action until that date. That means the AG can't actually file a lawsuit to enforce the law until July, but the AG has said—and I think if you look at the law, it is the most sensible reading of it—that there is a requirement to comply with the law as of January 1. But there can't be an enforcement action filed in court until July. Despite what you may have heard, we're not talking about *The Purge* for privacy until July of 2020.[24]

JUSTIN HUGHES: Well, that leads into just the thing I wanted to ask you to talk about. What is happening on the ground, Mr. Snow? How are businesses reacting? Are best practices emerging? What's happening on the ground in terms of compliance with the law?

JAKE SNOW: Thanks for the question. It's really good to be here and to talk with all of you. I'll talk about three areas where developments in regulations and enforcement strategies could affect your rights as consumers under the CCPA and how you actually can exercise those rights. The first one is personal information, and how the definition of it operates. I'd like to talk a little bit about a different aspect of the concept of personal information than Professor Wu talked about. And then second, the opt-out of sale rights and how they're operationalized.

The scope of personal information is properly broad and it includes illustrative examples written into the definition—IP addresses, email addresses, postal addresses, things like that.[25] The definition includes anything that is reasonably capable of being associated with a person, and that is because the law takes into account the fact that personal information as it is used today can be transformed to other kinds of information, and vice versa. A browsing history is also a medical record if you're searching for information about a disease that you're concerned you might have. Location data are personal information, but if combined with locations of people who you're spending time with, location information can reveal a

24. *See* THE PURGE (Universal Pictures 2013). The central premise of *The Purge* is a society in which all crimes are legal for one twelve-hour period every year. *The Purge*, WIKIPEDIA, https://en.wikipedia.org/wiki/The_Purge (last visited Oct. 4, 2020).

25. CAL. CIV. CODE § 1798.140(o)(1)(A) (Deering 2020).

record of people's past associations. And, of course, other kinds of personal information can be extracted from your location data as well—your interests, your religious affiliations, the identities of your coworkers, your political commitments.

Location information is very difficult to separate from an individual's identity, because as it turns out, most people spend a lot of their time at two places—where they work and where they live. With location data that have a unique identifier linked to each person—even if that person is not otherwise identified—you can just see where they go at night, and that's probably their home. Then you can, for example, look at public voter rolls to find their address and you may have identified the person. I imagine everyone saw the recent *New York Times* piece that looks at a huge data set[26]—a set of twelve million phones and the location data associated with those phones—and identifies people in those records. That includes secret service agents who were with President Trump.[27] According to the article, even without the identities, it was child's play to convert dots on a map to specific people.[28]

How does this affect the CCPA and the best practices in how it's being implemented? In the legislative session last year, 2019, there was a bill that sought to change the definition of personal information by creating an exception for what is called "deidentified information."[29] Now deidentified information under the CCPA is

26. Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

27. Stuart A. Thompson & Charlie Warzel, *How to Track President Trump*, N.Y. TIMES (Dec. 20, 2019), https://www.nytimes.com/interactive/2019/12/20/opinion/location-data-national-security.html.

28. Thompson & Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, *supra* note 26 (noting that location data companies, using smartphone location information, "can see the places you go every moment of the day, whom you meet with or spend the night with, where you pray, whether you visit a methadone clinic, a psychiatrist's office or a massage parlor").

29. Assemb. B. 873, 2019–2020 Reg. Sess. (Cal. 2019) ("[The] bill would revise the definition of 'deidentified' to instead mean information that does not identify, and is not *reasonably* linkable, directly or indirectly, to a particular consumer, provided that the business makes no attempt to reidentify the information and takes reasonable technical and administrative measures designed to ensure that the data is deidentified, publicly commits to maintain and use the data in a deidentified form, and contractually prohibits recipients of the data from trying to reidentify [the data]."); *see also* Maria Dinzeo & Nick Cahill, *Efforts to Gut Consumer Privacy Act Largely Fail*, COURTHOUSE NEWS SERV. (July 10, 2019), https://www.courthousenews.com/efforts-to-gut-consumer-privacy-act-largely-fail/ (discussing technology companies' support for Assembly Bill 873); Issie

information that can't be associated with a person according to a strict standard.[30] So remember those location records *The New York Times* picked people out of? Those would *not* qualify as "deidentified" under the CCPA's definition.[31] The bill would have amended the law so that under normal circumstances, an IP address, for example, or device identifier, would not qualify as personal information.[32]

That bill failed, but language similar to it has come back into the draft regulations.[33] This is going to be consequential because all of this information collected as people browse the internet and move about the world doesn't have people's names or addresses associated with it. But you can both group that information with other information about the person without knowing their name and also, with a little work (as *The New York Times* did), find out their name. The problem is that there's a very concerted effort to eliminate people's rights for information like this by carving it out of the definition of personal information under the CCPA. If that effort is successful, if you want to opt out of that information being sold, you won't be able to. The AG's regulations with respect to this point will be very consequential and, unfortunately, the outcome will be mostly invisible—consumers won't know what they don't know.

Lapowski, *Tech Lobbyists Push to Defang California's Landmark Privacy Law*, WIRED (Apr. 29, 2019, 3:09 PM), https://www.wired.com/story/california-privacy-law-tech-lobby-bills-weaken/.

30. *See* CAL. CIV. CODE § 1798.140(h) (CCPA currently defines "deidentified" as "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer" and requires the business to ensure that the data remain deidentified).

31. The location data would not fit the current definition of "deidentified" under CCPA because such data are reasonably capable of being associated with a particular person. *See id.*

32. Because under the proposed Assembly Bill 873, information is considered "deidentified" when it "does not identify and is not *reasonably* linkable, directly or indirectly, to a particular consumer," location data and IP addresses would be considered "deidentified" and thus, would be excludable from CCPA protections. Assemb. B. 873 (noting that businesses may "[c]ollect, use, retain, sell, or disclose [deidentified] consumer information").

33. *See* Proposed Text of Modified Regulations, Cal. Code Regs. tit. 11, § 999.302, at 4 (Feb. 7, 2020), https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-text-of-mod-redline-020720.pdf [hereinafter Proposed Cal. Code Regs. tit. 11, § 999.302] ("Whether information is 'personal information,' as that term is defined in Civil Code section 1798.140, subdivision (o), depends on whether the business maintains information in a manner that 'identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household.' For example, if a business collects the IP addresses of visitors to its website but does not link the IP address to any particular consumer or household, and could not reasonably link the IP address with a particular consumer or household, then the IP address would not be 'personal information.'").

The second thing I would like to talk about is the possibility of opt-out that doesn't put the burden on people to go through and do all the opt-out separately. At the ACLU, we put forth a proposal in the California legislature last year called "Privacy for All" that would have required instead of an opt-out framework for sale of personal information, an *opt-in* framework for the sharing of personal information.[34] The reason for that is simple. If you want to exercise your rights under the CCPA to opt out of the sale of your personal information, the first thing you have to do is find out who has your information and then you have to go through and do the opt-out for each one.

Just think about all websites you've ever been to and then all the apps on your phone and then all the data brokers that might have your information. California just released the first data broker registry, a registry with 143 data brokers.[35] Add those 143 data brokers to your list. If you want the list of all these entities, by the way, you go to caprivacy.me or simpleoptout.com.[36] They have a long list of companies and links to where you can opt out. You can have hundreds and hundreds of companies on this list. You have to start at the top or you start at the bottom, I guess. You go through all of them and you proceed to call them or email them or click the button or fill out the forms or find the settings and go through an opt-out of a sale of your personal information.

After a while, you'll probably conclude that opting out like that is a charade designed to exhaust you. And so you'll give up and go back to living your life.

---

34. The ACLU proposal was introduced by Assembly Member Buffy Wicks as Assemb. B. 1760, 2019–2020 Reg. Sess. (Cal. 2019). *See ACLU Supports New California Bill to Ensure Privacy for All*, ACLU S. CAL. (Feb. 27, 2019), https://www.aclusocal.org/en/press-releases/aclu-supports-new-california-bill-ensure-privacy-all; Hayley Tsukayama, *It's Time for California to Guarantee "Privacy for All"*, ELEC. FRONTIER FOUND. (Feb. 27, 2019), https://www.eff.org/deeplinks/2019/02/its-time-california-guarantee-privacy-all.

35. As of November 20, 2020, the number of data brokers on California's registry is over 400. *Data Broker Registry*, STATE OF CAL. DEP'T OF JUST., OFF. OF THE ATT'Y GEN., https://www.oag.ca.gov/data-brokers.

36. CAL. PRIV. DIRECTORY, https://caprivacy.github.io/caprivacy/full/ (last visited Oct. 4, 2020) (providing a list of companies that collect information and links to contact them); SIMPLE OPT OUT, https://simpleoptout.com (last visited Oct. 4, 2020) (same). *See generally* Michael Hiltzik, *Column: Big Business Is Trying to Gut California's Landmark Privacy Law*, L.A. TIMES (Apr. 19, 2019, 6:30 AM), https://www.latimes.com/business/hiltzik/la-fi-hiltzik-cal-privacy-act-20190419-story.html (presenting a general discussion of political struggle between opt-out and opt-in in relation to CCPA).

The only reasonable way to address this is to have a single, device-based global setting which allows you to opt out once and then every piece of information that goes on and off your mobile device or through your browser is subject to that general opt-out.

The idea would be a metadata flag of some sort associated with that data that opts the data out of being sold. The important thing about that, I think, is that it actually provides an additional solution to the problem of all this information being associated with the person, which is that if you go to a website and the website is unsure of who you are, but you have this opt-out flag set, then the website can associate that opt-out flag with all of your interactions with the website and then under the law, it can't sell that information—even if it hasn't the foggiest idea that you are you and that you're accessing the website.

The AG draft regulations have a requirement that global opt-outs in devices or in browsers be respected, and that has been the subject of significant discussion in the comments on the draft regulations, but the law should retain that requirement.[37] If it does, then everyone would have the ability to opt out once instead of doing it hundreds and hundreds of times and eventually giving up.

Finally, I would like to talk about the issue of Facebook and what Facebook has said about the CCPA and how its business complies with the CCPA. Spoiler alert, I don't think what they're saying makes any sense at all. To explain, the question is how the CCPA treats information generated by apps you use or websites you visit which is then shared with Facebook. Facebook takes that information about you and displays an ad or reports analytics back to the app or website to track performance. And we recall that the CCPA allows consumers to opt out of the sale of their personal information. The question is whether that delivery of information from the app or website to Facebook is a sale. In simple terms, is Facebook buying your information from that website when that happens?

Facebook has said that it is not receiving personal information pursuant to a sale because it is a service provider under the CCPA.[38]

37. *See* Proposed Cal. Code Regs. tit. 11, § 999.302, *supra* note 33.

38. *See* CAL. CIV. CODE § 1798.140(v) (Deering 2020) ("'Service provider' means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners,

It is saying, in other words, we are a service provider and we're providing the service to those websites or apps that are sharing information with us, and so we're not a recipient of sold personal information. It's important to note that Facebook is not talking about its own conduct; it is saying that its customers—the apps and websites—are not violating the CCPA and don't have to let their users or readers opt out of sharing information with Facebook. Facebook has less skin in the game here than it might initially appear. Basically, the CCPA says that people can instruct businesses not to sell their information[39] and sale is defined quite broadly[40]—I think properly quite broadly—but it is essentially any sharing of information that is accompanied by, or in return for, valuable consideration. You probably remember that from contract law class and that concept is flexible. It allows this notion of "sale" to capture any circumstance where there is the sharing of information and the return of some value.

There's an exception to the definition of "sale" and that relates to service providers. The kind of quintessential service provider, in my view, is a website host or payment processor where that entity is providing a limited and discrete service to a business so the business can operate. That's why sharing those entities doesn't constitute a sale from which the consumer can opt out: because the service provider is merely enabling the original first party collector to operate, and nothing more.

But there's an important restriction on how service providers operate. If you look at section 140(v) and 140(w)(2),[41] the CCPA says,

---

that processes information on behalf of a business and to which the business discloses a consumer's personal information for a business purpose pursuant to a written contract, provided that the contract prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract for the business, or as otherwise permitted by this title, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business."). The CCPA generally imposes obligations on "businesses," not "service providers." *See id.* §§ 1798.100–.130.

39. *Id.* § 1798.120(a) ("A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information.").

40. *Id.* § 1798.140(t)(1) ("'[S]ale' . . . means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration.").

41. *See id.* § 1798.140(v), (w)(2).

in effect, that you can use that information to provide the service, but you can't do a whole bunch of other stuff with it.

So what does Facebook do? I will just add a proviso here that it is not clear from the outside exactly what Facebook does, but this is what I've surmised based on their public statements and their documentation. Apps and websites will often send information about your use of the app or the website to Facebook. Often that is so Facebook can return targeted advertisements to the app or website, but Facebook also provides various other services, like analytics services to its customers. To enable that, the app or website developer installs a tracker that sends that information back to Facebook. Facebook takes that information and provides a service, like returning a targeted ad for the individual or integrating that information into an analytics platform. But Facebook also takes that information and often integrates it into a comprehensive profile of that person, which it then further exploits to provide, in Facebook's terminology, "relevant advertisements to the person."[42] That, I think, is the key problem with the notion that Facebook is acting solely as a service provider.

Facebook actually has a tool for you to look at all this information. It's called their "Off-Facebook Activity Tool."[43] Using this tool, you can disassociate your off-Facebook activity from your Facebook account. When you do that, Facebook says the ads you see will be less relevant to you. I think that shows essentially what's going on is that Facebook is using off-Facebook activity—information provided by third-party apps and websites—and incorporating it into the profiles it maintains of people. Then Facebook uses the enhanced profile not just for targeted advertisements for the specific third-party app or website, but for all of the *other* targeted advertisements that Facebook provides to other businesses.

If *that* is consistent with the CCPA, then what can't a company do under the service provider exception? You can monitor people's

42. *About Facebook Ads*, FACEBOOK, https://www.facebook.com/about/ads (last visited Oct. 4, 2020) ("We take the advertiser's goal, desired audience and ad to show you ads that we think might be relevant to you . . . .").

43. *The Best Person to Be in Control of Data Is You*, FACEBOOK, https://www.facebook.com/off-facebook-activity (last visited Oct. 4, 2020). For criticism of Facebook's tool, see Louise Matsakis, *Facebook's New Privacy Feature Comes with a Loophole*, WIRED (Aug. 28, 2019, 5:56 PM), https://www.wired.com/story/off-facebook-activity-privacy/; Shoshana Wodinsky, *Facebook's 'Clear History' Tool Doesn't Clear Shit*, GIZMODO (Jan. 28, 2020, 3:40 PM), https://gizmodo.com/facebooks-clear-history-tool-doesnt-clear-shit-1841305764.

activity in excruciating detail online. You can build profiles based on that monitoring and combine that profile with other information that you have about the individuals. And then you can monetize all that information by selling ads to anyone you want. If that all fits within the service provider exception, that's not the loophole swallowing the rule, that's the loophole swallowing the earth. And I don't think the Attorney General's office will tolerate that kind of interpretation. I'll stop there. Thanks very much.

JUSTIN HUGHES: Thanks. The wonderful thing about listening to Professor Wu and Mr. Snow is you get the difference between someone who gets to live an academic life versus someone fighting in the trenches. I do want to come back to the problem of sales, but before we do, I want to ask Professor Kaminski to take us through some different problems related to these CCPA constraints on companies—what data they can keep, what data they can transfer to others. It sounds to me like there is a potential firestorm of First Amendment litigation. I'm not a particular believer that corporations need every single human right to the full extent of the Universal Declaration of Human Rights,[44] but that seems to be the spirit of our First Amendment jurisprudence at times. Can you talk about how privacy law in general—and the CCPA in particular—interact with the First Amendment?

MARGOT KAMINSKI: Yes. Again, thank you so much for having me. This is a really impressive panel to get to be a part of and it's really fun to connect with other people from around the country who are thinking seriously about these issues. I'm going to go through three sections as quickly as possible, but slowly enough that it can be transcribed, so that we can all get to the meat of the panel, getting to talk to each other.

The first thing I'm going to provide you all is a quick overview of First Amendment doctrine. How many people here have had a First Amendment class? Okay. This will be really basic because I can't give you an entire semester's course in eight minutes. The second thing I'm going to do is talk about potential First Amendment challenges to the CCPA. And then the third thing is to talk a little bit about where we might go from here or what I think is coming down the line.

44. G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948) [hereinafter Universal Declaration of Human Rights].

On the first issue—this is your First Amendment refresher for those of you who have studied this and the First Amendment overview for those who haven't. There are really two steps in determining whether First Amendment protection applies. The first step is to ask whether something is speech, which is effectively asking whether a particular activity is *salient* to the First Amendment. This might sound really obvious when you're talking about my sitting here and talking to you—that's clearly speech. But my knocking on the table is clearly not speech . . . except when it *might* be speech.[45] There's been a question recently in a number of cases about whether transferring data or data processing might be considered salient to the First Amendment—that is to say whether data is speech.[46] There are some nuanced issues with that question.

The second step is determining whether there is First Amendment protection. Just because you determined that something is covered by, or salient to, the First Amendment, does not necessarily mean that the First Amendment protects it. That is, just because it's speech doesn't mean it's protected by the First Amendment. Most of you have heard of at least some of the various exceptions to First Amendment protection such as the exceptions for child pornography, for incitement of violence, or for true threats.[47] Most of you have also probably heard that the US is very permissive in terms of the kinds of speech it does protect, so that hate speech is actually protected under the First Amendment unless it falls into one of those pre-existing categories of speech that are not protected.

To determine whether speech is not just covered but protected by the First Amendment, courts apply different levels of judicial scrutiny. Famously, most things that are considered to be pure speech are subject to strict scrutiny which is usually fatal in fact. That means that when judges apply strict scrutiny to the regulation or the law, the law usually fails. But some subcategories of covered speech, including

45. *See* Texas v. Johnson, 491 U.S. 397 (1989) (holding that flag burning is protected speech under First Amendment); Spence v. Washington, 418 U.S. 405 (1974) (displaying the United States flag upside down with a peace symbol taped thereto was protected speech); United States v. O'Brien, 391 U.S. 367 (1968) (burning of draft card was sufficiently expressive to trigger First Amendment analysis).

46. *See, e.g.*, Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57, 58–60 (2014).

47. *See* Virginia v. Black, 538 U.S. 343 (2003) (outlining the "true threat" exception to First Amendment protection); New York v. Ferber, 458 U.S. 747 (1982) (distributing child pornography is not protected by the First Amendment); Brandenburg v. Ohio, 395 U.S. 444 (1969) (holding that speech can be outlawed if is directed to incite imminent violence or unlawful action).

commercial speech, are subject to intermediate scrutiny which is more of a balancing test. Commercial speech is usually understood as "I am proposing to sell you something"—like an advertisement. The government has a lot more leeway to regulate in that space than it does when it is regulating, for example, what I'm saying right now on this panel.

As a second part, let's talk about aspects of recent First Amendment doctrine that raise particular problems for data privacy—I'm going to put these in three categories. One is the problem of what I've been calling the cat-out-of-the-bag doctrine—and I'll talk about a couple of those cases.[48] These cases effectively say once information is out there, the government can't try to control dissemination, but it turns out there are many nuances to this doctrine. The second is the data-is-speech doctrine: there's a number of cases that point to the idea that the Supreme Court at least is increasingly thinking it might be.[49] The third is the general trend of the First Amendment becoming more deregulatory along specific lines.[50]

First, I think the most important thing to get across here is the parameters of what I've been calling the cat-out-of-the-bag doctrine. The context for these cases is that the Supreme Court was vastly extending its First Amendment jurisprudence at that time, largely in response to cases that were brought by newspapers. These two Supreme Court cases from the 1970s and 1980s, *Cox v. Cohn*[51] and *Florida Star v. B.J.F*,[52] both addressed what are known as "rape shield" laws. There are laws in different states that say you can't, as a newspaper, print the name of a rape victim. In reviewing challenges to these laws, the Court arrived at the principle that once the government itself has let the cat out of the bag, that has made the name public either

48. Margot E. Kaminski & Scott Skinner-Thompson, *Free Speech Isn't a Free Pass for Privacy Violations*, SLATE (Mar. 9, 2020, 2:53 PM), https://slate.com/technology/2020/03/free-speech-privacy-clearview-ai-maine-isps.html; *see also* United States v. Suppressed, No. 16MC261, 2019 U.S. Dist. LEXIS 36565, at *7 (N.D. Ill. Mar. 7, 2019) ("As the Tribune puts it in a collection of mixed metaphors, post-publication 'the genie is out of the bottle,' 'the cat is out of the bag,' and 'the ball game is over.'"); Eugene Volokh, *"Once the Cat Is Out of the Bag, the Ball Game Is Over."*, REASON (July 13, 2019, 2:31 PM), https://reason.com/2019/07/13/once-the-cat-is-out-of-the-bag-the-ball-game-is-over/ (discussing the court's mixed metaphor language in *United States v. Suppressed*).

49. *See, e.g.*, Sorrell v. IMS Health Inc., 564 U.S. 552 (2011).

50. *See, e.g.*, Jeremy K. Kessler & David E. Pozen, *Introduction: The Search for an Egalitarian First Amendment*, 118 COLUM. L. REV. 1953 (2018).

51. Cox Broad. Corp. v. Cohn, 420 U.S. 469 (1975).

52. Fla. Star v. B.J.F., 491 U.S. 524 (1989).

in a court proceeding or a police report, it cannot go and tell newspapers not to print that information.

First of all, that principle is incredibly problematic for data privacy laws like the CCPA. CCPA covers a vast amount of personal information, but a lot of that information can be obtained publicly. Some of that stuff you can obtain publicly from a government record, so putting restrictions on its distribution can potentially raise problems within this doctrine.

My pushback to such reasoning is that the actual test that comes out of the rape shield cases is far more nuanced than a general cat-out-of-the-bag principle. Under those cases, for a government restriction on information to be unconstitutional, the information must be lawfully obtained and it has to be truthful.[53] It also has to be a matter of public concern to be covered by the holdings in those cases,[54] and arguably private information is not usually a matter of public concern. And, after all that, the state can still regulate under those cases if the state has an interest of the highest order.[55] This question of the magnitude of state interest in regulating ties into whether we recognize privacy harms to be important—more on that later.

The second aspect of First Amendment doctrine that raises a major hurdle for the CCPA is the question of whether "data is speech." In *Sorrell*,[56] the Supreme Court evaluated a Vermont privacy law, looked at some of the restrictions, said they were content-based (or even overtly speaker-based or viewpoint-based), applied something like strict scrutiny and found the law unconstitutional.[57] This suggests that data and data privacy laws are being seen by the Supreme Court as being close enough to First Amendment speech that they will apply some sort of scrutiny to these legal restrictions. Professor Wu can push

53. *Id.* at 533.

54. *Cox Broad. Corp.*, 420 U.S. at 492 (state could not criminalize the publication of a rape victim's name taken from public records because "[t]he commission of crime, prosecutions resulting from it, and judicial proceedings arising from the prosecutions . . . are, without question events of legitimate concern to the public").

55. *Id.* at 496 (while holding that "[o]nce true information is disclosed in public court documents open to public inspection, the press cannot be sanctioned for publishing it," the Court also found that government could shield information "by means which avoid public documentation or other exposure of private information").

56. Sorrell v. IMS Health Inc., 564 U.S. 552 (2011).

57. *Id.* at 580.

back on this later—there is a long conversation between the two of us on this.

Last, the general contours of the First Amendment have been increasingly deregulatory in ways that are problematic for all kinds of consumer protection law, not just data privacy. Because data privacy is a form of consumer protection law, this trend is definitely a particular concern. We have a number of cases recently in which the Supreme Court has said that it is not going to add new categories to its categories of unprotected speech[58]—which suggests that if what's being regulated by the CCPA is found to be speech, we're in trouble, since there's no explicit First Amendment exception for data privacy laws.

The second is that, content-based and speaker-based distinctions which trigger strict scrutiny have been expanding.[59] It used to be that something called the "secondary effects" doctrine, from a case called *Renton v. Playtime Theatre* (1986),[60] allowed courts to say just because a law names particular speech (such as pornography) doesn't mean the law is actually targeting particular content of information. That is, a state might be permissibly regulating not the speech itself but the secondary effects of that information, like what porn theaters do to a neighborhood. But this doctrine has recently been cabined in ways that are potentially bad for data privacy law—so that if you name a particular type of speech (such as personal information) even if you're not really targeting the content or viewpoint, you might risk falling under strict scrutiny.[61]

58. *See, e.g.*, United States v. Alvarez, 567 U.S. 709 (2012) (plurality opinion) (recognizing constitutionality of a content-based restrictions on "a few historic categories of speech" and that there may exist "some [other] categories of speech that have been historically unprotected," but declining to recognize a new category in the form of false statements); Brown v. Ent. Merchs. Ass'n, 564 U.S. 786 (2011) (rejecting any new categories of unprotected speech "without persuasive evidence that a novel restriction on content is part of a long (if heretofore unrecognized) tradition of proscription"); United States v. Stevens, 559 U.S. 460 (2010) (declining to find "depictions of animal cruelty" as outside First Amendment protection and rejecting "a freewheeling authority to declare new categories of speech outside the scope of the First Amendment").

59. *See* Reed v. Town of Gilbert, 576 U.S. 155, 163–64 (2015).

60. City of Renton v. Playtime Theatres, 475 U.S. 41 (1986).

61. *See Reed*, 576 U.S. at 171. *But see* Dan V. Kozlowski & Derigan Silver, *Measuring* Reed*'s Reach: Content Discrimination in the U.S. Circuit Courts of Appeals After* Reed v. Town of Gilbert, 24 COMMC'N. L. & POL'Y 191 (2019) (demonstrating that many lower courts have been interpreting *Reed* narrowly).

Okay. Some really quick but important caveats and then I'll try to let us get to discussion. The first is, I think that there is no current Supreme Court level law that clearly makes the CCPA unconstitutional. I think there is nothing at the Supreme Court level that clearly establishes the appropriate level of scrutiny for the CCPA. The Supreme Court has pretty consistently assessed the privacy/First Amendment interface on a sui generis, case-by-case basis.

You see dicta repeated in many of these cases saying, in essence, "We are not going to hold that regulators cannot regulate to protect private information."[62] The Supreme Court has also repeatedly suggested at least that there is a distinction between matters of public concern for which there may be more First Amendment protection and truly private matters for which there's less First Amendment protection, even though they say the opposite in almost every other area of First Amendment doctrine.[63]

Last, there is a sort of invisible history of tolerance between the First Amendment and privacy laws. There have been privacy laws in the US dating back to the '70s that contained many similar elements to the CCPA and none of them have triggered First Amendment scrutiny nor have any of them triggered court rulings as unconstitutional.

In conclusion, I want to get to what I think might happen. We have recently been seeing litigation in a number of states' supreme courts over revenge porn laws.[64] How many people here know what revenge porn is? Nonconsensual distribution of sexual images that one person has sent to another person under an expectation of privacy.[65]

---

62. *See, e.g.*, *Sorrell*, 564 U.S. at 574 ("This is not to say that all privacy measures must avoid content-based rules."); Fla. Star v. B.J.F., 491 U.S. 524, 533 (1989) ("We continue to believe that the sensitivity and significance of the interests presented in clashes between First Amendment and privacy rights counsel relying on limited principles that sweep no more broadly than the appropriate context of the instant case."); Cox Broad. Corp. v. Cohn, 420 U.S. 469, 491 (1975) ("Rather than address the broader question whether . . . the State may ever define and protect an area of privacy free from unwanted publicity in the press, it is appropriate to focus on the narrower interface between press and privacy that this case presents . . . .").

63. *See* Snyder v. Phelps, 562 U.S. 443, 452 (2011).

64. *See, e.g.*, People v. Austin, 155 N.E.3d 439 (Ill. 2019) (upholding Illinois' revenge porn law against a First Amendment challenge); State v. VanBuren, 214 A.3d 791 (Vt. 2019) (upholding Vermont's revenge porn law against a First Amendment challenge).

65. "Revenge porn" is "a popular label describing a subset of nonconsensual pornography published for vengeful purposes." *VanBuren*, 214 A.3d at 794. The phrase includes "images originally obtained without consent . . . as well as images originally obtained with consent, usually within the context of a private or confidential relationship." *Id.* at 794–95. *See generally* Danielle

Some of the concerns we have been raising here are true of revenge porn laws in addition to the CCPA. One state supreme court, the Vermont State Supreme Court, has effectively said, "we refuse to create a new category of information to which the First Amendment does not apply,"[66] and instead they applied strict scrutiny and held that the law was valid.[67] This never, or rarely, happens; remember, strict scrutiny is known to be fatal in fact. For First Amendment doctrine, the outcome was shocking; they turned strict scrutiny into a balancing test instead of treating it as fatal in fact.

Another approach—taken by the Illinois Supreme Court—was to apply intermediate scrutiny to a revenge porn law. That court effectively said, "really, the appropriate test for these kinds of things is to balance First Amendment concerns against the strength of the privacy interest here." The law again withstood the challenge.[68]

My punchline is that this is very complicated. There's no question in my mind the challenges are coming. There is no controlling Supreme Court case that would give us an outcome, let alone an actual level of scrutiny, but the judges are creative and norms are changing and have some faith, they will adapt the doctrine.

JUSTIN HUGHES: Thank you. I am going to take the moderator's prerogative to prompt some discussion, but then we will eventually open it up for some questions. I guess I want to ask all of you—starting with Professor Kaminski—for the cat-out-of-the-bag problem, do you think that line of cases can be constrained by using the issue of public concern and/or the state's interest being of the highest order to say, "We're going to uphold the privacy law in these spaces?"

MARGOT KAMINSKI: Yeah. I didn't talk about how this applied to CCPA because of time constraints, but the CCPA, as Professor Wu noted, has this incredibly broad definition of personally identifiable information[69] and then has a "does not include publicly disclosed

Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345 (2014).

66. *VanBuren*, 214 A.3d at 801–02 ("[W]e decline to identify a new categorical exclusion from the full protections of the First Amendment when the Supreme Court has not yet addressed the question.").

67. *Id.* at 800 ("[W]e conclude that the Vermont statute survives strict scrutiny as the U.S. Supreme Court has applied that standard.").

68. *Austin*, 155 N.E.3d at 466–72.

69. *See* CAL. CIV. CODE § 1798.140(o)(1) (Deering 2020).

information" exception.[70] But the definition of publicly disclosed information in the CCPA refers only to government records.[71] That almost—well, I don't want to say dooms it. This seems intended to address concerns about the cat-out-of-the-bag cases, but there's still a chance that a court looks at this and says, "Well, this doctrine applies because the information was lawfully obtained. It's not just about information being released in a public record and this doctrine applies more broadly than the exception the CCPA allows."

JUSTIN HUGHES: Gentlemen, what would you add to that?

FELIX WU: I think the question of the constitutionality of the CCPA is an easy case, much easier actually than revenge porn laws and here's why: because the CCPA addresses purely commercial activities. What do I mean by that? The transactions that Professor Kaminski is describing here are potential sales of information. It's the sale of information from one commercial entity to another; that makes it completely different from all of the previous Supreme Court cases, which involved the dissemination *from* a commercial entity but *to* a non-commercial consumer or other individual who themselves might have a kind of personal right to the information.

As far as I'm concerned, when two commercial entities are transacting in the data on a purely commercial basis, the First Amendment simply doesn't apply.[72] We should not, in fact, apply any level of scrutiny to that transaction whatsoever, unless you can show there's going to be some downstream effect on an eventual non-commercial user. Now, you might say, what about *Citizens United*[73] and other cases like that? Yes, but every one of those cases involved an actual person, at least as the recipient of the information.

If you have two commercial entities who are transacting amongst themselves on a commercial basis, as far as I'm concerned, the First Amendment has nothing to do with it. I'm not that optimistic, frankly, about this current Supreme Court necessarily going the way that I'm describing. On the other hand, for the reasons that Professor Kaminski

70. *Id.* § 1798.140(o)(2) ("'Personal information' does not include publicly available information.").

71. *Id.* ("'[P]ublicly available' means information that is lawfully made available from federal, state, or local government records.").

72. Felix T. Wu, *The Commercial Difference*, 58 WM. & MARY L. REV. 2005, 2048 (2017); Felix T. Wu, *The Constitutionality of Consumer Privacy Regulation*, 2013 U. CHI. LEGAL F. 69, 72–73.

73. Citizens United v. Fed. Election Comm'n, 558 U.S. 310 (2010).

described, at least everything I'm saying is perfectly consistent with all the previous case law.

JUSTIN HUGHES: Your position is that company to company data transfer isn't speech at all?

FELIX WU: I have a complicated view on the particular way you framed your question, but let's put it this way: it's not, in fact, something that should be subject to scrutiny under the First Amendment, not even intermediate scrutiny.

JUSTIN HUGHES: All right. Mr. Snow, anything to add?

JAKE SNOW: Nothing there.

JUSTIN HUGHES: Okay. Let me move to another question. Professor Wu, you said that in prior precedent—at least under federal privacy law—the measure of reasonably capable of being associated with a particular individual has been reasonably capable of being associated with a particular individual *from a stranger's perspective*. But the problem is that people are holding vast quantities of data that make some information reasonably capable of being associated with a particular individual when one has that information in context.

What's the right test a court should use when they are trying to interpret this "reasonably associated with" phrase? Should it be reasonably capable of being associated with a particular person *by the recipient of the data*? Or reasonably capable of being associated with a particular person *in the context of all the data held by the seller*? How would you frame it?

FELIX WU: Let me just start by saying, I do not think there is an all-purpose answer to the question of how you should frame almost any issue regarding personal information. Ultimately, the question is, what does the law aim to do and how do you implement that in the definition of personal information. To the extent that we think the CCPA is really designed to address the creation and use of the kinds of profiles I described earlier, then absolutely, it should be from the perspective of the holder of the data or the recipient of the data. And to the extent information is identifiable from the perspective of those entities that should suffice with respect to making it "personal information" under the law.

JUSTIN HUGHES: Let me press you a little bit more. Let's say I have a dataset that means nothing to me, but I know if I sell it to you, you will be able to associate a bunch of data points with 10,000 individuals.

FELIX WU: It's personal information.

JUSTIN HUGHES: Then it becomes personal information for the purpose of that transaction?

FELIX WU: Yes.

JUSTIN HUGHES: Okay. Professor Kaminski and Mr. Snow, agree or disagree?

MARGOT KAMINSKI: I think that's absolutely right. One of the things I didn't get to talk about before is the expanding notions of data privacy harm at the Supreme Court level. There's an increasing understanding at the Supreme Court—which also makes me slightly optimistic should any First Amendment issue go up to them—that data, as Mr. Snow was saying, are something that's more than just the individual pieces of information you have and you can take almost any individual data point and given enough related data points about the same person, re-identify the person.

JAKE SNOW: Yeah, I agree. I think that those kinds of data sets are personal information because of the real difficulty in protecting people from re-identification. It may be difficult, but it's very difficult for it to be impossible. I recommend the article *Surprising Failure of Anonymization* by Paul Ohm[74] which goes through a lot of these issues. It gives a lot of concrete examples and explains why information that doesn't have explicitly identifying information is quite easy to re-identify.

There are technical ways of protecting individuals from that kind of re-identification. Things like differential privacy[75] have real promise to allow access to datasets without revealing any information about an individual in the dataset and there are operations on encrypted data using techniques like homomorphic encryption. I do think that with technical progress and more innovation in the technical space, more will be possible while making really strong privacy guarantees to people who are present in the datasets.

---

74. Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010); *see also* Wu, *Defining Privacy and Utility in Data Sets*, *supra* note 11, at 1127–29 (reasoning that if "de-identification" is understood to mean absolutely no leakage of information about individuals, then it is trivially true to say that data cannot be usefully de-identified, but that for other reasonable understandings of "de-identification," de-identification may be possible).

75. *See* Alexandra Wood et al., *Differential Privacy: A Primer for a Non-Technical Audience*, 21 VAND. J. ENT. & TECH. L. 209, 211–13 (2018); CYNTHIA DWORK & AARON ROTH, THE ALGORITHMIC FOUNDATIONS OF DIFFERENTIAL PRIVACY 5–6 (2014).

JUSTIN HUGHES: Let me ask one last moderator's prerogative question. Jake, you were describing how ACLU prefers to have an opt-in system, but you were somewhat hopeful about how the regs are developing. Let me ask you this, will we see an app we can install in our phone or our laptop that simply acts as our agent and opts out of everywhere? I'm asking you partly as a question of agency law. In other words, do the likely regulations permit a future in which we will have an AI assistant to which we will say, "Get me out of here," and the AI assistant will opt us out of the sale at five bazillion websites?

JAKE SNOW: Yeah, I think that's entirely possible. The law has a provision for an agent exercising rights on behalf of a consumer and then there's also the browser flag issue that I talked about. I think both of those hold promise for making opting-out a lot easier. I do think, however, that opt-out is still problematic because people generally won't turn on the browser flag or install the app.

Some people who are concerned about privacy may do it but, if you look at the research, very few people actually change settings. If privacy is the default, the privacy is preserved without a person having to do anything. That's why an opt-in framework is still necessary despite the fact that we may have ways to help people who want to submit a whole bunch of opt-outs at once.

JUSTIN HUGHES: Margot and Felix, are you two more optimistic about that?

MARGOT KAMINSKI: I'm going to have a broader rant for a second which is that, individual rights often don't work—especially if there's no private right of action. If the CCPA came with a private right of action, you'd have a ton of class action attorneys ensuring that companies are complying. You don't. Individuals, who have a lot of things that they do with their time and have a limited amount of time to deal with the handling of their own rights, largely are not going to use things like an opt-out provision or an access provision.

That is just the pessimistic truth. One of my great frustrations with this law—and I think also the other panelists probably share it—is that it has very few backstops to protect consumers who don't invoke their own rights. In contrast, the General Data Protection Regulation and other data privacy laws around the world put substantive requirements

on what companies must do with information.[76] The CCPA doesn't do that. It relies on you to go and do things to protect yourselves, so good luck.

FELIX WU: I'm largely in agreement. I'm not sure if this is an even broader rant or not, but, again, at some level these are important issues that even an opt-in system is not going to address entirely. Whether you think of it as opt-in or opt-out, you are thinking about it as entirely an individual decision—and individual decision-making, particularly on a granular level, is, I think, ultimately going to be a difficult way of making progress on this.

Let me put in a brief defense of this notion that we don't want to just go by individual choice here—because some of you might be thinking, "Well, of course, we should go by individual choices. This is all just about individual rights and, therefore, choice is what really matters and it's all about identifying who chooses privacy and who doesn't choose privacy." But part of the idea here is that privacy is not just about you; that your privacy is not just about you. Ultimately, privacy is also a social value and the ways in which we jointly produce privacy and have privacy as a community makes a difference to the kind of society we have. That's a joint and collective issue that cannot just be devolved to an aggregation of individual choices made by individual people.

JUSTIN HUGHES: I think that was broader, but beautiful—and not a rant. I have many more questions for our panelists, but I would like to open it up a little bit to questions from the floor if there are questions. You should state the question as loudly as you can and then we will repeat it to make sure it gets in the transcription.

AUDIENCE QUESTION: Sure. Since we're talking about the opt-out framework, I'd imagine that very few people would actually opt-in to sell their data and get no monetary kickback from that, just for using a service such as Google or Facebook. That seems like a big concern because advertising revenue funds a lot of other services, like news publications.

JUSTIN HUGHES: Your question is, will the opt-out framework, if utilized by many people, cause a diminution of advertising revenue?

76. GDPR, *supra* note 2, art. 12 (description of substantive requirement of what companies must do). In Canada, companies are required to act in compliance with ten enumerated principles pertaining to data privacy. *See* Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.).

To me, your question seems to be about the effects of all this on the digital economy, is that right?

AUDIENCE QUESTION: Yeah. I imagine the opt-out framework may have a pretty massive impact on the digital economy. In fact, I just want to hear more of your thoughts on that.

JUSTIN HUGHES: Okay.

FELIX WU: Let me start by noting that it is a common assumption that the data websites collect on people is the driver of the advertising, but that is not necessarily the case—or at least it is a contested factual question as to how much of the value of the advertising actually depends on having these data versus how much of the advertising dollars would still get spent regardless and therefore support the web services even in the absence of the use of that private data. There are some studies[77] that report that the gap in value between targeted and contextual advertising is far smaller than is generally assumed ("contextual" meaning relative to whatever the user is looking at[78] rather than more targeted advertising based on the user's past history[79]).

If that's the case, that will mean that we still have lots of advertising dollars; we will still have lots of advertising supported web services. It's true, we may have a little less, but not in a way that necessarily is as catastrophic as some people might think.

JUSTIN HUGHES: I should add that the CCPA has very extensive provisions—that our panelists might want to comment on—providing that a person who opts out must be provided equal services, but eventually can be charged a differential based on the value of the data that they are withholding from being sold. I've seen some very low estimates about that—$0.06 per person or $0.12 per person—but that is something that the Attorney General's regulations are intended to address also. Do you have comments about that concern? I think, Margot, you might have had some comments on that.

---

77. *See* Charlotte Otremba, *How Contextual Targeting Puts Privacy First While Closing the Engagement Gap*, BIDTELLECT (Feb. 2020), https://bidtellect.com/2020/02/how-contextual-targeting-puts-privacy-first-while-closing-the-engagement-gap/.

78. Ana Gotter, *Contextual Advertising: What It Is and Why It Matters*, DISRUPTIVE ADVERT. (Jan. 15, 2018), https://www.disruptiveadvertising.com/ppc/contextual-advertising/.

79. *The Power of Targeted Ads*, IDG ADVERT.: BLOG, https://idgadvertising.com/the-power-of-targeted-ads/ (last visited Oct. 4, 2020); *see also* Hiltzik, *supra* note 36 (concluding that "[t]argeted advertising is a major source of pollution of the online experience" and that polls showing that Americans like targeted advertising "generally are sponsored by the advertising industry").

MARGOT KAMINSKI: Yeah. We were talking about this earlier and I think that we have differing views on this—more optimistic versus more pessimistic.

JUSTIN HUGHES: Let's hear them.

MARGOT KAMINSKI: Yeah. I'm excited about the charge-me-money-if-you're-going-to-give-me-my-privacy option not because I believe that your information is your property, to be really clear, but more because I think that identifying the economic value of personal information is a good idea. I think it is a good idea because it starts to make visible the data economy in a way that is necessary for other kinds of law. There's been, for example, a longstanding conflict over what counts as privacy harm. I think there is one court case where the court says that the "Mount Kilimanjaro" of privacy cases is *standing*, in other words convincingly saying "I was actually injured."[80]

Well, if you have a whole bunch of companies who are saying, "Give up your privacy or pay us this amount of money," you're forcing companies to start to actually place dollar amounts on your privacy and that thinking can be transferable to other parts of laws. That's my sneakily optimistic version of this.

Plus one to what Professor Wu just said about contextual advertising versus targeted advertising—this is not science as much as companies pretend it is. We don't actually know if targeted advertising works better.

The one thing I'd say on the impact on the digital economy—we haven't talked about this yet—but the bigger concern here, I think, is actually competition. As much as I'd like to go after the data brokers, the law is really going after the data brokers and not after the big platforms. In some ways, Facebook and Google and the other primary platforms might actually make out better, because we may be killing the third-party advertising industry. If the platforms stop working with third parties who now face higher regulatory costs and just internalize behavioral advertising by doing it all themselves, then the monopoly or anti-competitive concerns will go way up. That, I don't think, is an intended consequence of the legislation.

JUSTIN HUGHES: Mr. Snow?

80. *In re* Google, Inc. Priv. Pol'y Litig., No. C-12-01382-PSG, 2013 WL 6248499, at *4 (N.D. Cal. Dec. 3, 2013); *see also* Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL L. REV. 439, 449–50 (2017) (discussing the *Google Privacy Policy* case).

JAKE SNOW: I do think that a path forward for allowing ad-supported businesses is what Professor Kaminski and Professor Wu have mentioned which is that, if somebody exercises their opt-out rights, they will get contextual ads. If they don't opt out, then they would get more personalized, targeted ads. Contextual ads have been the way that advertising-supported businesses have worked for a long time—television and newspapers were all supported by contextual ads. There's no reason why that model can't still work.

With respect to the notion of discrimination or requiring that people pay more for their privacy rights under the CCPA, I think that's the wrong path to go down. One reason is that it inherently creates a barrier to privacy for people who don't have the means to pay for the right to have—for the privilege of having—privacy. Privacy shouldn't be a luxury good. It is in the Universal Declaration of Human Rights.[81] It is an inalienable right under the California Constitution.[82] Those rights are not something that should be bought and sold and they're not something people should be required to pay for.

I do think that it's important to recognize that the value of people's information is not just related to how much money they have. Being rich doesn't necessarily make people's information more valuable. In fact, people's information is valuable not when they are rich, but when they are vulnerable. If you look at the ranking of the most valuable adwords on Google, the top one is mesothelioma lawyer and if you look down the 100 Top Adwords, you see property damage, personal injury, addiction, car accidents.[83]

These are people who are looking to the internet in a time of desperation and they need help. They are not wealthy. They are going to the internet to find help with a desperate need, and *that* is the information that's most valuable to an advertising platform, the urgent needs of people who are struggling. That's another reason why we shouldn't be charging people more for the privilege of having their

81. Universal Declaration of Human Rights, *supra* note 44, art. 12 ("No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.").

82. CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

83. Chris Lake, *The Most Expensive 100 Google Adwords Keywords in the US*, SEARCH ENGINE WATCH (May 31, 2016), https://www.searchenginewatch.com/2016/05/31/the-most-expensive-100-google-adwords-keywords-in-the-us/.

information protected. We'll further disproportionately harm the most vulnerable among us.

JUSTIN HUGHES: Another question? Yes, ma'am—in front.

AUDIENCE QUESTION: Yes. You mentioned that the CCPA does not apply to certain businesses. And also how will this law affect law firms? To what extent do they have to meet the CCPA standards?

JUSTIN HUGHES: The question is a practical one. Does CCPA apply to law firms and also very quickly, what are the thresholds for the law's application?

MARGOT KAMINSKI: I don't have the thresholds memorized. It depends on how big you are and how many California residents' personal information you are processing.[84] There are three categories. Some of them are more oriented towards business size—depending on revenue—and others are more oriented towards sheer number of processing.

JUSTIN HUGHES: Jake, do you have the numbers memorized?

JAKE SNOW: No, but I have a computer.

FELIX WU: I have the full numbers here. There's annual gross revenue in excess of $25 million *or* the personal information of 50,000 or more consumers, households, *or* devices or derives 50 percent of its annual revenues from selling personal information.[85] Now, of those three, $25 million is quite a lot, but the information of 50,000 consumers is a very easy threshold to reach. Why? Because of the broad definition of personal information. Every time you track an individual on your website, that is another person's personal information that you now have. You track 50,000 people on your website—50,000 Californians just to be clear because that's who's defined as a consumer under the law—you track 50,000 Californians on your website and you will trigger the law.

JAKE SNOW: That's something like 137 per day, and so you don't need very much tracking to get there.

JUSTIN HUGHES: Another question? Yes, ma'am—in the middle.

---

84. *See* CAL. CIV. CODE § 1798.140(c)(1) (Deering 2020).

85. *Id.* (A business must satisfy "one or more of the following thresholds: (A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185. (B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices. (C) Derives 50 percent or more of its annual revenues from selling consumers' personal information").

AUDIENCE QUESTION: I have a question. Can you tell me about any provisions on appropriate safeguards to protect against data breaches? I was wondering if you could speak a little on that.

JUSTIN HUGHES: The question is whether the CCPA includes any data security requirements on those holding personal information.

JAKE SNOW: The one place where there is a private right of action in the CCPA is for data breach. I will say that the elements of a data breach claim are pretty narrow under the CCPA, so it is not going to apply any time you have a breach; it requires an exfiltration, theft, or disclosure that is unauthorized and a result of a failure to maintain reasonable security practices with respect to a different definition of personal information than applies to the rest of the statute.[86]

That different definition is what we would normally think of as highly sensitive personal information—names, email addresses associated with social security numbers, other ID numbers, biometrics, things like that. All that means that the data breach cause of action which is available is fairly narrow and the definition of personal information is much narrower there as well. As a result, there's a more limited litigation risk for companies, but there is some.

JUSTIN HUGHES: So biometric information is definitely is personal information under the CCPA?

MARGOT KAMINSKI: Yeah, it's on the list.

FELIX WU: It explicitly says so.

JAKE SNOW: It's in the primary definition list of CCPA[87] and it's also in the list in the definition for the data breach.[88]

MARGOT KAMINSKI: I will just say by way of background that the data security provisions of the CCPA have been attracting a lot of attention in part because that's where the class action attorneys are going to have fun, but California has had a data breach law since 2003.

---

86. *Id.* § 1798.150(a)(1) ("(a)(1) Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following: (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. (B) Injunctive or declaratory relief. (C) Any other relief the court deems proper.").

87. *Id.* § 1798.140(o)(1)(E) (definition of personal information includes biometric information).

88. *See id.* § 1798.150(a)(1) (including biometric data under personal information, "as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5").

This is actually one place where we've seen the most ratcheting up of state-by-state legislation in the last couple of years. States have gone from having in place laws where a company has to inform consumers that their data have been breached to laws with actual substantive requirements of what a company has to do in order to protect data. States are moving from transparency obligations to what I was talking about earlier: substantive obligations for the company.

One of the big focuses in these sorts of provisions is what the heck does "reasonable" security practices mean, but I will leave that to Professor Wu to start to spell that out. [*Laughter*]

FELIX WU: Oh, I'm not sure that I can exactly spell that out. The one point I want to make with respect to biometrics though is that even though biometric information is in the definition of personal information in the CCPA, the coverage of biometrics in California is far short of what it is, for example, in Illinois, because in Illinois you need prior written consent in order to collect biometrics,[89] whereas under the California law, you're given the same rights as all the rest of the things that count as personal information and there is no requirement of prior written consent for the collection of personal information generally under the CCPA. In that sense, the coverage of biometrics currently in the California law is short of what it is in Illinois, which is currently the leading source of biometrics protection.

JUSTIN HUGHES: Professor Wu is thinking of a class action against Facebook under the Illinois law that was filed under diversity jurisdiction in federal court in Northern California. And for which the Ninth Circuit recently upheld for class certification, correct?

FELIX WU: Right. In which Facebook recently settled for $500 million.[90]

JUSTIN HUGHES: Ouch. Okay. I would like to go just until 7:20 PM. Any other questions from the audience? Yes, sir.

---

89. 740 ILL. COMP. STAT. 14/15(b) (2020).

90. Natasha Singer & Mike Isaac, *Facebook to Pay $550 Million to Settle Facial Recognition Suit*, N.Y. TIMES (Jan. 29, 2020), https://www.nytimes.com/2020/01/29/technology/facebook-privacy-lawsuit-earnings.html. Although Facebook agreed to settle this lawsuit for $550 million, the court rejected the settlement and only later approved a revised settlement in which Facebook is to pay $650 million to settle the class action. Siladitya Ray, *Facebook Gets Preliminary Approval to Settle Facial Recognition Lawsuit*, FORBES (Aug. 20, 2020, 9:30 AM), https://www.forbes.com/sites/siladityaray/2020/08/20/facebook-gets-preliminary-approval-to-settle-facial-recognition-lawsuit/?sh=49c140924f73.

AUDIENCE QUESTION: Continuing with the biometric data we were just talking about, there is a recent article that came out about a company in Silicon Valley called Clearview.[91] They're using a facial recognition app that now they released to several law enforcement agencies. The way that they developed the app is that they scraped Facebook—basically every single website that posts images—and so the app is 99% accurate. Given that they would clearly fall over the 50,000 persons threshold, Clearview would be subject to the CCPA. If I submit a deletion request to that company, do you think that the deletion would also apply to data held under law enforcement agency control or are they exempt?

MARGOT KAMINSKI: I'm going to let Jake answer this but I want to point out that Clearview's 99% accuracy claim[92] is based in part on policy trolling that Jake did to Congress. Watching this back and forth has been amazing.

JAKE SNOW: Don't believe their accuracy claims. For background, in 2018, as part of the work that we did at the ACLU surrounding facial recognition, we took 25,000 public mugshots, loaded them into Amazon Rekognition[93] and then searched in that database for every current member of Congress—all 535 members of Congress. We found that twenty-eight members of Congress in 2018 falsely matched with mugshots. Those twenty-eight false positives were disproportionately people of color; six members of the Congressional black caucus falsely matched. As a result of that, members of Congress sent letters to Amazon saying there's a real civil-rights concern with bias and accuracy with your surveillance tool,[94] i.e., what the hell is going on?

---

91. Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (last updated Feb. 10, 2020). Clearview AI is headquartered in New York.

92. Donie O'Sullivan, *This Man Says He's Stockpiling Billions of Our Photos*, CNN (Feb. 10, 2020, 9:18 AM), https://www.cnn.com/2020/02/10/tech/clearview-ai-ceo-hoan-ton-that/index.html.

93. *What Is Amazon Rekognition?*, AMAZON WEB SERVS., https://docs.aws.amazon.com/rekognition/latest/dg/what-is.html (last visited Oct. 4, 2020). The controversy surrounding this technology has prompted Amazon to suspend its marketing to law enforcement. Sam Dean, *Amazon Pauses Police Use of Its Facial Recognition Software*, L.A. TIMES (June 10, 2020, 4:59 PM), https://www.latimes.com/business/technology/story/2020-06-10/amazon-police-facial-recognition-software-rekognition.

94. Davey Alba, *Bipartisan Lawmakers Want to Talk to Amazon About Its Facial Recognition Tech*, BUZZFEED NEWS (July 26, 2018, 1:37 PM), https://www.buzzfeednews.com/article/daveya

Clearview said they used the ACLU's methodology, which they did not. What Clearview did is they took their tool, which has the images from the sources you identified, and then they searched in that tool for members of Congress. All members of Congress were in their database because they have public photos on the internet and their software apparently correctly identified them. To me, that is not a valid test of the accuracy of their tool and says nothing about whether it is accurate in real-world conditions. Nor is it similar at all to our work except that they used members of Congress.

Imitation is the most sincere form of flattery, but this is flattery that I can do without. If they want the ACLU's stamp of approval, they should shut it all down and turn off their servers and get out of the surveillance business.

JUSTIN HUGHES: Yes, every member of Congress has a well-constructed, well-lit photo but the question was, if you send a request to Clearview and say delete my biometrics and Clearview behaves, what happens to the datasets held by the law enforcement agencies?

MARGOT KAMINSKI: Just an important caveat, deletion applies to businesses with whom you have a direct consumer relationship.[95] Clearview is not Facebook. You don't have an account at Clearview by which you're a consumer. So, my understanding is that you don't have a deletion right. The bigger question is whether you have an access right to be able to actually see the information—because that does apply to third parties. I'll leave the law enforcement exception to Jake.

JAKE SNOW: With respect to the deletion right, I agree. The statutory language is "collected from consumers,"[96] so I think you wouldn't necessarily have that right. With respect to the access rights, if you go to the Clearview website, they actually require—at least they did a couple of weeks ago—that you send them an image of your government ID in an email in order to exercise your access right. I

lba/congressmen-mismatched-to-mugshots-by-amazon-tech-demand (last updated July 27, 2018, 4:19 PM). The ACLU demonstrated similar results with members of the California legislature. Anita Chabria, *Facial Recognition Software Mistook 1 in 5 California Lawmakers for Criminals, Says ACLU*, L.A. TIMES (Aug. 13, 2019, 5:00 AM), https://www.latimes.com/california/story/2019-08-12/facial-recognition-software-mistook-1-in-5-california-lawmakers-for-criminals-says-aclu.

95. *See* CAL. CIV. CODE § 1798.105 (Deering 2020).

96. *Id.* § 1798.105(a) ("A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.").

don't know about you but I'm not super excited about sending an image of my government ID in an email to a company that's building a massive dystopian surveillance network for law enforcement.

This speaks to the chilling effects of what Clearview is doing and how what they are doing stands in the way of people exercising their access rights. With respect to the law enforcement exception, it's a fair question and I don't know the answer. Clearview has said—or I should say suggested— that they are selling to authoritarian regimes overseas and also that they have private security contracts potentially as well. For those customers, the law-enforcement exception under the CCPA would not apply.[97]

JUSTIN HUGHES: Let me ask you a quick question. The law provides that you can go in twice a year and request your information and the law also provides you can request the companies with which you have a relationship to delete your information. How often can you ask them to delete your information, because I'm wondering if it is kind of like cleaning the gutters on a house. Do you have to keep going every six months and say, "Delete my information?" Is that the system that's been set up by the CCPA?

FELIX WU: I think so.

MARGOT KAMINSKI: Yeah, I think so. This is why we should not rely only on individual rights. Individuals don't have the time, capacity, or often the sophistication to police companies this way. We need to put affirmative obligations on companies even if consumers don't invoke their rights.

JUSTIN HUGHES: So if you really were stringent about wanting people not to collect your information, not only would you have to visit a hundred websites, but you would have to visit a hundred websites every six months.

MARGOT KAMINSKI: Yeah. I think the interesting question to Jake is, if the global opt-out option that's being considered in regulations that you are following in far more detail than I have been, is that something that once you flag yourself for global opt-out, would that get rid of this regularly-cleaning-the-gutters problem?

JAKE SNOW: The global opt-out applies to sale and, for that, I think the idea is that you would opt out globally and forget it; you wouldn't

97. *Id.* § 1798.145(a)(3) (providing an exception to "[c]ooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law").

have to do it again—it would not, for example, turn itself off every six months and force you to figure out your settings and turn it back on. With respect to deletion, there's nothing in the draft regulations for a global ongoing deletion request or something like that.

JUSTIN HUGHES: Let me ask each of our panelists to handle one last question. The last question is, concerning the CCPA what is the issue that the courts will have to figure out *first* or the issue that they will have to figure out that is *most important* and how should they figure it out? I think Professor Wu has to start.

FELIX WU: I think the first thing that's going to arise is the question of "sale." I think the scope of what counts as a sale is probably going to be the most pressing issue, because transactions for valuable consideration is a really broad idea and could cover lots of possible activities. Since that's the one thing that you can specifically tell companies not to do, it is the easiest place in the CCPA to detect a possible violation—as opposed to you accessing your information or something along those lines. What I mean is, you put in a request to access your information and how are you going to know when they don't give you some piece of something that's buried somewhere?

It will be really hard for you to know if they didn't give you all the information they have, whereas if you tell them not to sell your information and then they still engage in some sort of transaction which they say is not a sale, we are more likely to become aware of that. So, I think that's the thing that's going to come up first. As for how you resolve it, it will depend on exactly how it comes up, but I think that Jake is right that the statute is written very broadly. Any transaction for value will do and, accordingly, I think courts should interpret the provision broadly.

JUSTIN HUGHES: You think the question of what things count as valuable consideration under the statute will have to be litigated first?

FELIX WU: Correct.

JUSTIN HUGHES: Okay. Professor Kaminski?

MARGOT KAMINSKI: They call it the *First* Amendment for a reason. The challenges are coming and in short, my view is 95 percent of the CCPA is constitutional.

FELIX WU: You're not saying which 5 percent is unconstitutional?

JAKE SNOW: I agree that it's the First Amendment and I think Dormant Commerce Clause for good measure. And just to add to Professor Kaminski's comments, the Attorney General's office lacks

the resources to actually do comprehensive enforcement. You have like ten or fifteen attorneys and they are trying to stand up an enforcement program for all of California.

I think that the AG's office will start by finding companies who are effectively scofflaws, who have done essentially nothing to comply. They don't have the links on the website. They're not responding to access requests. They're blowing deadlines. I think there are going to be some companies who do that, who decided to take their chances with an under-resourced Attorney General's office. If somebody makes that choice, then I think the Attorney General might make an example of them. Those scofflaws—and I would say this as somebody who litigated cases against scofflaws for the Federal Trade Commission—love the First Amendment argument. So I think they'll bring it up. Basically, the First Amendment will come up in a case against an entity that may have few other valid defenses.

JUSTIN HUGHES: Your answer was both constitutional but it was also political—that is, the Attorney General's office wants to show enforcement, so they will go after the low hanging fruit, and take them out. All right. With that, I'd like to thank our panelists. Please, let's thank our panelists. I think they'll stay around a bit and answer questions, so if you want to come down, please do.